

ÅRSRAPPORT 2016

Ö K K S H
C W R S D
F D S W E
Ä Q D W W



Information viktigt i en osäker tid

Stadigt växande militär aktivitet i Östersjöregionen, tragiska terrorattacker i Europa, allvarliga cyberangrepp mot samhällsviktiga funktioner. Utvecklingen i omvärlden har gått i en riktning av tilltagande osäkerhet och svårförutsägbarhet. Detta har i sin tur ökat behovet av information och beslutsunderlag från FRA på det säkerhetspolitiska området.

FRA spelar i dag en viktig och alltmer efterfrågad roll för att rapportera om det som sker i omvärlden. Det är vår ena huvuduppgift.

Vår andra huvuduppgift, att vara statens resurs för teknisk informationssäkerhet, är betydelsefull för att skydda den mest skyddsvärda statliga verksamheten mot alltmer avancerade cyberangrepp.

Tillsammans med en osäker omvärld skapar den snabba teknikutvecklingen på IT-, krypto- och kommunikationsområdet fortsatta utmaningar för oss. Hur väl vi lyckas bygger på motiverade medarbetare med synnerligen hög kompetens och starkt engagemang.

Det ligger i sakens natur att vi för att lyckas med vårt uppdrag måste skydda våra mål och metoder med betydande sekretess. Samtidigt finns det i ett demokratiskt samhälle ett

självskrivet behov av att översiktligt kunna få information även om FRA:s verksamhet. Att möta detta behov är syftet med denna årsrapport.

I årets rapport går vi lite djupare in på utvecklingen inom IT-angrepp och behovet av att stärka det svenska cyberförsvaret. Också Sveriges digitala integritet – den digitala territorialgränsen – måste skyddas för att vi som lever här ska kunna känna oss trygga. För att lösa denna uppgift behöver vi såväl kunskap om angriparnas metoder som effektiva skyddsmekanismer.

Cyberförsvarsfrågorna ges i dag stor uppmärksamhet av regeringen. Ytterst innebär dessa frågor uppgifter för hela samhället – såväl offentliga som privata aktörer – och det är viktigt att våra samlade åtgärder både är effektiva och hänger ihop.

Överlag är nära samverkan mellan FRA och andra myndigheter en viktig förutsättning för bästa möjliga nytta för Sverige.

I denna årsrapport ger vi också en liten inblick i vilka vi är, vi som arbetar på FRA. Vanliga människor med unika arbetsuppgifter, för Sveriges säkerhet och integritet.

Dag Hartelius
Generaldirektör



Minskad förutsägbarhet i omvärlden

Den negativa trenden i den globala säkerhetspolitiska utvecklingen har fortsatt under 2016. På ett övergripande plan handlar det om grundläggande strukturer och principer för fredliga konfliktlösningar som nu upplevs hotade.

I en intervju inför Sveriges medlemskap i FN:s säkerhetsråd förklarade utrikesminister Margot Wallström att stämningen i rådet är den sämsta på länge.

Den grundbult – inte minst för små nationers säkerhet – som utgörs av respekt för folkrätten är fortsatt underminerad genom Rysslands annektering av Krim och dess medverkan i stridigheterna i östra Ukraina.

Flera länder, däribland Ryssland, har förklarat att de tänker lämna den internationella brottmålsdomstolen i Haag. Också icke-spridningsområdet har drabbats av bakslag. Bland annat har Ryssland slutat medverka i det globala partnerskapet mot spridning av massförstörelsevapen.

I Sveriges närområde fortsätter den militära aktiviteten att öka med tillförsel av förband och materiel. Totalförsvarets

forskningsinstitut (FOI) har konstaterat att Rysslands militära handlingsfrihet växer samtidigt som försvarsutgifternas andel av Rysslands BNP ökar.

Striderna i Syrien och norra Irak har fortsatt med hög intensitet, med ofattbart mänskligt lidande som följd. Flera överenskommelser om vapenvila i Syrien har även brutits.

Samtidigt har terrororganisationen Daesh tagit på sig attentaten i bland annat Bryssel och Nice som krävt över hundra människors liv. I sin årliga rapport om terrorism slår Europol fast att antalet gripna för terroristbrott ökat i EU-länderna samtidigt som Daesh bedöms ha utvecklat en strategi att angripa fler mål i bland annat Europa.

EU:s samordnare inom terrorism varnade i oktober för att ett par tusen personer med kunskap och förmåga att använda sprängmedel och möjligen kemiska vapen kan komma att återvända till Europa.

Säkerhetsläget i Mali, där Försvarsmakten deltar i en FN-operation, har beskrivits som ömtåligt av EU:s humanitära organisation ECHO. FN-soldater har

under året dödats i attacker vid ett flertal tillfällen.

Säkerhetspolisen pekar fortsatt på att det finns statliga aktörer som bedriver olaglig underrättelseverksamhet mot Sverige. Det är framför allt Rysslands agerande som oroar.

I sin årsrapport (2015) skriver Säkerhetspolisen att Ryssland har en avsikt att påverka det politiska beslutsfattandet och den allmänna opinionen och att Ryssland genom offentliga uttalanden försökt påverka debatten om Sveriges säkerhetspolitiska vägval.

Till mer spektakulära cyberangrepp som uppmärksammats under året hör överbelastningsattackerna mot domänserverföretaget Dyn, med omfattande kedjeeffekter i Sverige som följd, samt nätverksintrången mot det demokratiska partiet under presidentvalskampanjen i USA. I detta sammanhang har amerikanska myndigheter offentligt pekat ut Ryssland som ansvarigt.

Texten baserar sig på öppna källor och innehåller således information som återfunnits i öppna publikationer. Referatet ska därmed inte ses som en del av FRA:s underrättelserapportering.



Spaning mot utlandet och stärkt skydd

En förutsättning för en självständig svensk utrikes- och säkerhetspolitik är egen pålitlig information om omvärlden. Sverige måste även se till att landet har ett skydd mot att andra länder kommer åt skyddsvärd svensk information. FRA har en uppgift i båda dessa avseenden.

Genom att rapportera om utländska förhållanden och samtidigt stärka svensk informationssäkerhet bidrar FRA till att skydda Sverige och svenska intressen och till att stärka Sveriges roll internationellt.

FRA förser uppdragsgivarna med kvalificerad information om omvärlden genom signalspaning. Rapporteringen ger kunskap, djupare insikter och förvarning om händelser och förhållanden i utlandet som är viktiga för Sverige.

Det kan handla om information som bidrar till strategiska beslutsunderlag för regeringens utrikes- och säkerhetspolitik, men signalspaningen kan också varna för sådant som kan utgöra hot mot Sverige.

Den information som FRA förmedlar kan exempelvis röra sig om militär förmåga i andra länder, utvecklingen i krigs-

och konfliktregioner eller IT-angrepp i det globala nätet.

De som får ge FRA signalspaningsuppdrag är förutom regeringen Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella Operativa Avdelningen (NOA) inom Polismyndigheten. 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 Försvarsunderrättelsesdomstolen och att verksamheten löpande granskas av Statens inspektion för försvarsunderrättelseverksamheten (Siun).

Datainspektionen har dessutom under 2016 granskat behandlingen av person-

uppgifter inom FRA:s försvarsunderrättelseverksamhet.

Vid FRA finns också ett integritetsskyddsråd som följer hur integritetsfrågorna tas om hand inom FRA. Ledamöterna i rådet tillsätts av regeringen.

Utöver signalspaning handlar FRA:s uppdrag om att stärka informations säkerheten i svensk samhällsviktig verksamhet.

Vår spetskompetens inom teknisk informationssäkerhet används bland annat för att på uppdrag av myndigheter och statliga bolag identifiera sårbarheter och brister i deras IT-system. I detta arbete är den unika kunskap om angreppen i det globala nätet, som vi får genom signalspaning, en viktig förutsättning och framgångsfaktor.



Verksamhet 2016

Fortsatt hög militär aktivitet i närområdet

En stor del av FRA:s signalspaning handlar om att följa militär förmåga i Sveriges närområde – allt från truppförflyttningar och satsningar på nya vapensystem till främmande makts säkerhetspolitiska avsikter på längre sikt.

Intresset från våra uppdragsgivare för den säkerhetspolitiska utvecklingen i närområdet fortsätter att öka. Kraven på tidskritisk rapportering är i dag mer omfattande än på många år. Mot bakgrund av den ökade militära aktiviteten har FRA förstärkt närområdesbevakningen under 2016.

Flera länder har tillfört nya militära förmågor i Sveriges närområde. FRA har under året rapporterat om förändringar i den taktiska militära närvaron runt Östersjön. Vi följer löpande händelser och bidrar med bedömningar kring motiv bakom den förändrade utländska militära närvaron.

Vi har sett ett flertal exempel på faktisk ökning av främmande makts militära förmåga, men också identifierat händelser

som snarare utgör medvetna säkerhetspolitiska markeringar.

Mot bakgrund av den höga militära aktiviteten i närområdet har vi, genom bland annat flyg- och fartygsburen signalspaning, kunnat upprätthålla en fortsatt kvalificerad produktion till signalreferensbiblioteket (SRB). Informationen i SRB ger Försvarsmakten stöd att identifiera andra länders militära fartyg, flygplan och fordon.

Krig och konflikter med spridningsrisk

FRA följer utvecklingen i krig och konflikter, både nära Sverige och längre bort. Det kan gälla säkerhetspolitiska avsikter, maktbalans, militär förmåga eller centrala aktörer i konflikter och deras motiv.

Under 2016 har den oroliga situationen i delar av Mellanöstern, framför allt i Syrien, förvärrats med risk för ytterligare destabilisering av hela regionen som följd. Vår rapportering har bidragit till ett bättre svenskt kunskapsläge rörande centrala aktörers avsikter och agerande.

Generellt innebär krig och konflikter en tydlig risk för spridning av spänningen

till andra närliggande länder. Historien visar att lokala och regionala konflikter på avstånd kan utvecklas till internationella kriser, med konsekvenser även för Sverige och svensk säkerhet. Inte minst kan det gälla spridning av terrorism och hot mot svenska civila och militära insatser utomlands.

I skuggan av de krigs- och konfliktzoner som får stor massmedial uppmärksamhet finns andra skeenden och händelser som FRA följer på uppdrag av regeringen. Det kan handla om sådant som inte nödvändigtvis får samma uppmärksamhet men där ett gott underrättelseläge stärker Sveriges möjligheter att utforma och föra en oberoende utrikes- och säkerhetspolitik.

Internationell terrorism med kopplingar till Sverige

Säkerhetspolisen är FRA:s främsta uppdragsgivare rörande internationell terrorism. Uppdraget handlar dels om att följa internationella terrornätverk – finansiering, organisation, vapentillgång – dels om att identifiera eventuella kopplingar till Sverige.

Fortsättning på nästa uppslag ►



Vi ger underrättelsestöd till Säkerhetspolisen både löpande och i samband med särskilda händelser. Säkerhetspolisens höjning av terrorhotnivån i Sverige i november 2015 gav återverkningar för FRA inte bara under den tid som nivån var förhöjd. Produktionen av underrättelser till Säkerhetspolisen har under 2016 legat på en konstant högre nivå.

Rapportering från FRA har i vissa fall på ett avgörande sätt förbättrat Säkerhetspolisens underrättelseläge och i förlängningen lett till åtgärder som bidragit till att reducera allvarliga hot.

Komplexiteten i uppdraget och det ökade antalet ärenden med direkt koppling till Sverige under 2016 har lett till ett ansträngt läge för FRA inom området. Vi har fått göra vissa omprioriteringar under 2016 för att möta den ökade efterfrågan från Säkerhetspolisen på ett tillfredsställande sätt.

Stödet till Försvarsmaktens insatsverksamhet utvecklas

Vårt stöd till Försvarsmaktens insatsverksamhet kan gälla utrustning, specialkompetens eller underrättelser och kan ges både inför, under och efter en insats.

Typiska underrättelser i anslutning till

svensk militär insatsverksamhet utomlands handlar om hotbilden mot den svenska truppen och bedömningar av utvecklingen i det aktuella landet. Samarbetet med Försvarsmakten inom ramen för internationella insatser har utvecklats ytterligare under året.

Hybridhot synliga

Vid sidan av mer traditionella hot finns svårdefinierade hotbilder. Begrepp som hybridhot och påverkansoperationer används allt oftare. FRA har under 2016 sett exempel på tydliga försök från främmande makt till påverkan på beslutsprocesser, såväl internationellt som riktat mot Sverige.

Flera länder bedriver underrättelseverksamhet som riktas mot Sverige och svenska intressen. Den vanligaste formen av sådan underrättelseverksamhet utgörs i dag av avancerade IT-angrepp, även om också mer traditionella metoder förekommer. Det kan även gälla spionage som auktoritära regimer riktar mot flyktingar i Sverige.

FRA stödjer också Nationella Operativa Avdelningen (NOA) inom Polismyndigheten med underrättelser om viss grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen

samt ger stöd till exportkontroll gällande massförstörelsevapen.

IT-angrepp mot Sverige vanliga

FRA följer angreppen i det globala nätet via signalspaningen. Sverige angrips ständigt genom olika former av IT-angrepp och denna trend har förstärkts. Vanliga mål under 2016 i Sverige har varit forskning och utveckling, försvarsindustri, politiska organ och institutioner och myndigheter med samhällsviktiga uppdrag.

IT-säkerhetsanalyser bidrar till att stärka svensk informationssäkerhet

En viktig del av FRA:s verksamhet handlar om att lämna stöd till statliga myndigheter och statligt ägda bolag kring deras informationssäkerhet. FRA:s arbete på IT-säkerhetsområdet koncentrerar sig på de mest skyddsvärda verksamheterna i Sverige.

Arbetet sker bland annat genom IT-säkerhetsanalyser, där FRA:s experter på uppdrag av en myndighet eller ett statligt bolag identifierar brister och sårbarheter hos organisationens IT-system. Efterfrågan på FRA:s IT-säkerhetsanalyser har ökat under senare år, vilket sannolikt

Fortsättning på nästa uppslag ►



Maalbeek
Maelbeek



Police Politie

Bruxelles CAPITALE Ixelles Brussel HOOFDSTAD Elsene



Police Politie

Bruxelles CAPITALE Ixelles Brussel HOOFDSTAD



beror på den generellt växande medvetenheten om IT-angrepp.

Under 2016 har IT-säkerhetsanalyser gjorts hos ett tiotal statliga myndigheter och statligt ägda bolag. Även om det under analyserna ofta framkommer många sårbarheter kan FRA se en förbättring hos de organisationer där FRA genomfört återkommande IT-säkerhetsanalyser.

Stöd vid IT-incidenter

FRA har under året gett stöd till myndigheter och statliga bolag vid flera IT-incidenter. Stödet har handlat om identifiering av angrepp, återkoppling och råd till organisationen. FRA har genom detta arbete kunnat identifiera flera sårbarheter hos de drabbade organisationerna och på så sätt ökat deras möjligheter att göra systemen säkrare.

FRA hjälper andra myndigheter med säker kommunikation

För att svenska organisationer ska kunna samverka säkert med varandra krävs bland annat att alla använder samma kryptosystem. Inom ramen för informationssäkerhetsarbetet hjälper FRA andra myndigheter och organisationer med utrustning för säker kommunikation. FRA ansvarar för leverans av materiel, nycklar

och certifikat, användarstöd, utbildning och övning.

Nationell och internationell samverkan växer i betydelse

För att kunna möta dagens utmaningar behöver svenska myndigheter samarbeta effektivt. Samverkan mellan FRA och Försvarsmakten respektive Säkerhetspolisen är mycket nära och har fortsatt att fördjupas under 2016. Också med andra myndigheter såsom MSB, FOI och FMV är samarbetet viktigt. De särskilda samverkansformer som FRA har med Försvarsmakten och Säkerhetspolisen i form av Nationellt centrum för terrorhotbedömning (NCT) och Nationell samverkan till skydd mot allvarliga IT-hot (NSIT) har fortsatt att utvecklas. Tillammans gör vi Sverige säkrare.

Sverige delar säkerhetspolitiska utmaningar med andra länder. Många av de utländska företeelser som FRA följer är globala men har kopplingar till Sverige.

Detta gör att betydelsen också av internationell samverkan har ökat under de senaste åren. Exempel på områden där det internationella säkerhetssamarbetet vuxit i betydelse är internationell terrorism, bedömningar kring andra länders

militära förmåga samt skydd mot allvarliga IT-angrepp.

Under året har FRA genomfört informationstillfällen för riksdagens försvarsutskott och utrikesutskott.

Tekniksatsningar och rekryteringar

För att klara de ökade kraven från uppdragsgivarna mot bakgrund av omvärldsläget har FRA i och med 2015 års försvarsbeslut fått ökade anslag från regeringen för åren 2016–2020.

Vid sidan av omvärldsutvecklingen påverkas FRA:s förutsättningar för att utföra sitt uppdrag även av den mycket snabba teknikutvecklingen.

FRA har under året arbetat intensivt med rekrytering av rätt kompetenser och med tekniska investeringar för att säkerställa en fortsatt hög förmåga.



Sverige är utsatt för angrepp – varje dag

Stater och statsunderstödda organisationer bakom många angrepp

Även om IT-angrepp som utförs av organiserad brottslighet och enskilda individer kan vara väl så besvärliga råder det ingen tvekan om att andra staters underrättelsetjänster och statsunderstödda organisationer utgör det allvarligaste cyberhotet mot Sverige.

Flera länders underrättelsetjänster har ett intresse för Sverige och dessa använder sig alltmer av IT-angrepp för att inhämta informationen.

Utmärkande för utländska statliga kvalificerade aktörer är att de lägger ner stora resurser på personal och kompetens. De kan ta fram unika avancerade angreppsmetoder som inte alltid upptäcks av kommersiella skyddssystem. Genom stor uthållighet kan de under lång tid arbeta systematiskt med att hitta sårbarheter och utveckla skräddarsydd skadlig kod tills de kommer in i systemen.

Säkerheten är dock ofta så dålig i systemen att angriparen kan använda kända sårbarheter och angreppsverktyg och

på så sätt spara på de mer avancerade metoderna.

Kort sagt kan vi konstatera att om en kvalificerad angripare har bestämt sig för att ta sig in i ett givet system så lyckas man nästan alltid med det. Det är bara en fråga om tid.

Intressanta mål i Sverige

Genom signalspaning ser vi att IT-angrepp mot svenska myndigheter och företag pågår här och nu. Därför måste verksamheter som hanterar information som är intressant för främmande länders underrättelsetjänster utgå från att man blir utsatt. Även leverantörer till sådan verksamhet kan vara intressanta för en angripare, som en lättare väg till målet.

Följande information kan till exempel vara intressant för en främmande underrättelsetjänst:

- Försvarsförmåga och försvarsplanering
- Svenska säkerhetspolitiska avsikter
- Statshemligheter
- Industrihemligheter
- Forskningsresultat

Vi har även kunnat konstatera att statliga aktörer angriper kritisk infrastruktur i Sverige. Syftet kan exempelvis vara att allvarligt störa viktiga samhällsfunktioner vid en eventuell kris- eller krigssituation.

Två uppgifter inom cyberområdet

Genom signalspaningen följer FRA kvalificerade IT-angrepp som sker i det globala nätet. På så sätt får vi god kunskap kring vilka aktörer som står bakom, deras angreppssätt, mål och verktyg. Kunskapen om angreppen kan vi sedan omsätta till olika skyddsåtgärder när vi stödjer myndigheter och statliga bolag i deras informationssäkerhetsarbete.

Omvänt kan den kunskap vi får genom informationssäkerhetsuppdraget ge oss viktiga inslag för signalspaningen. Om vi till exempel ser ett större angrepp mot en myndighet eller ett statligt bolag kan vi försöka identifiera och spåra aktörerna genom signalspaning.



Olika angreppsmetoder för olika syften

De mest uppmärksammade angreppen är ofta sådana där den som ligger bakom har använt relativt enkla verktyg, såsom överbelastningsangrepp (även kallade DDoS). Sådana angrepp har traditionellt varit mindre relevanta för FRA, då de oftast inte kan knytas till de aktörer som vi följer, det vill säga stater och statsunderstödda organisationer.

Gränserna är dock inte längre lika aktörs-skarpa. I dag kan även enklare angreppssätt, som exempelvis DDoS-angrepp, användas av den här typen av aktörer som ett sätt att skapa allmän oro eller som ett led i mer eller mindre medveten hybridkrigföring.

Genom signalspaningen har FRA sett att de mer osynliga angreppen, med avancerad skadlig kod, påtagligt har ökat. Den här typen av angrepp sker regelmässigt av just stater eller statsunderstödda aktörer, som gör allt för att undvika upptäckt.

Grovt räknat handlar det om tiotusentals aktiviteter varje månad med skadlig kod som kan härledas till de statliga aktörer som FRA följer.

I den fortsatta analysen försöker vi på FRA identifiera vilka mål som angrips och få fram motivbilden bakom.

Det kan te sig som en omöjlig uppgift. Samtidigt underlättas analysen av vetenskapen att dessa aktörer är mycket målmedvetna och typiskt angriper vissa typer av mål som man kan förutse. Dessutom lär vi oss hela tiden mer om de metoder och verktyg som används.

Stater och statsunderstödda aktörer är bland annat väldigt skickliga på social engineering, som inte är ett ovanligt inslag inför ett angrepp. Social engineering handlar om att skapa legitimitet bakom en avsändare genom att skaffa sig goda kunskaper om målpersonens sociala liv och personliga preferenser. På detta sätt ökar sannolikheten att personen öppnar exempelvis ett e-postmeddelande med skadlig kod, eftersom det förefaller komma från personens privata nätverk och liknar tidigare kommunikationsmönster.

En annan oroväckande trend hos kvalificerade angripare är att placera avancerad skadlig kod i själva hårdvaran, exempel-

vis i en server, en dator eller en mobiltelefon. Angreppen kan då bli oerhört svåra att upptäcka. Det blir också svårare att bli av med skadlig kod, eftersom den kan finnas kvar även om de infekterade delarna av hårdvaran bytts ut.

Även vanliga privatpersoner som saknar koppling till skyddsvärd verksamhet kan bli föremål för angrepp. Det kan exempelvis ske genom att deras datorer används för att skapa ett nätverk av datorer som angriper ett mål någon helt annanstans. Det förekommer att svenska datorer används som ett mellanled i angrepp mot andra länder och vice versa.



Svårt att skydda sig mot allt

Vid sidan av signalspaningen stödjer FRA myndigheter och statligt ägda bolag med särskilt skyddsvärd verksamhet i deras arbete med informationssäkerhet.

Generellt kan vi konstatera att säkerheten hos myndigheter och statliga bolag inte är dimensionerad för den hotbild vi ser. När vi genomför säkerhetsgranskningar hos våra uppdragsgivare kan vi se att det med relativt enkla metoder och med kända angreppsverktyg går att ta över nätverken utan större problem. Ofta är det samma säkerhetsbrister som går igen hos många organisationer.

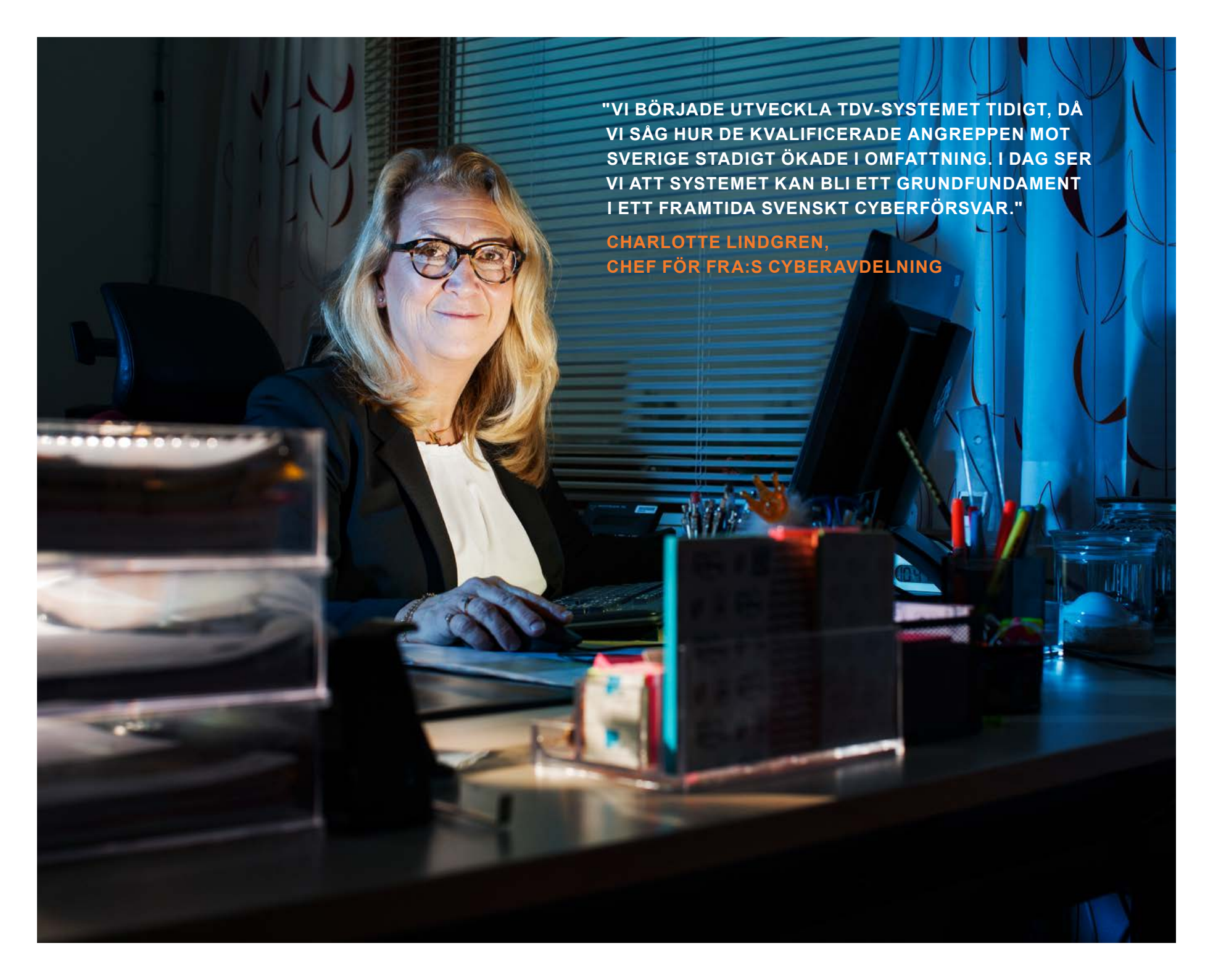
FRA har sedan början på 2000-talet genomfört ett hundratal säkerhetsgranskningar hos myndigheter och statliga bolag.

Här är de vanligaste bristerna vi ser:

- Otillräcklig kunskap om hotbilden
- Bristande förståelse hos ledningen för behov av åtgärder
- Outsourcing som skapar sårbarheter och försvagar informationssäkerhetskompetensen inom organisationen
- Bristande kravställning vid nya upphandlingar och avtal

Detta kan i sin tur leda till följande:

- Grundläggande svagheter i utformningen av nätverk
- Brister i intern dokumentation och regelverk kring informationssäkerhet
- Existerande säkerhetsfunktioner i system används inte
- Brister i separationen mellan system
- Onödigt breda administratörsrättigheter
- Bristande lösenordshantering
- Begränsad förmåga att hantera IT-incidenter

A woman with blonde hair and glasses, wearing a black blazer over a white top, sits at a desk in a dimly lit office. The desk is cluttered with various items, including a computer monitor, a keyboard, a mouse, and several pens. The background features a window with blinds and patterned curtains. The lighting is soft, highlighting the woman's face and the desk's surface.

"VI BÖRjade UTVECKLA TDV-SYSTEMET TIDIGT, DÅ
VI SÅG HUR DE KVALIFICERADE ANGREPPEN MOT
SVERIGE STADIGT ÖKADE I OMFATTNING. I DAG SER
VI ATT SYSTEMET KAN BLI ETT GRUNDFUNDAMENT
I ETT FRAMTIDA SVENSKT CYBERFÖRSVAR."

CHARLOTTE LINDGREN,
CHEF FÖR FRA:S CYBERAVDELNING

På väg mot ett svenskt cyberförsvar

Cyberangrepp innebär ett allvarligt hot mot Sveriges integritet, men det pågår många initiativ för att stärka den samlade svenska förmågan att stå emot angreppen. FRA samarbetar med andra myndigheter för att skapa ett sammanhållet svenskt cyberförsvar.

FRA:s bidrag i det nationella cyberförsvaret baseras främst på synergier mellan våra två uppdrag: signalspaning och teknisk informationssäkerhet.

Ett tydligt exempel på denna synergi är det tekniska detekterings- och varningssystem (TDV) som FRA har tagit fram på uppdrag av regeringen. Ett TDV-system kan jämföras med ett avancerat antivirusprogram.

Genom signaturer från signalspaning ska systemet upptäcka avancerade angrepp som kommersiella antivirusprogram inte kan hitta. Systemet är tänkt att användas av verksamheter som är mest kritiska ur ett nationellt säkerhetsperspektiv. Regeringen har gett FRA i uppdrag att fortsätta utvecklingen av TDV. Under 2016 har ytterligare ett antal verksamheter installerat systemet.

Vi samarbetar med Försvarmakten och Säkerhetspolisen i syfte att skapa ett sammanhållet nationellt system där den gemensamma kunskapen kan omvandlas till konkreta skyddsåtgärder, främst för de mest skyddsvärda verksamheterna i samhället.

Samarbetet sker framför allt inom ramen för Nationell samverkan till skydd mot allvarliga IT-hot (NSIT) som etablerades av FRA, Militära underrättelse- och säkerhetstjänsten (Must) och Säkerhetspolisen under 2012. Även Myndigheten för samhällsskydd och beredskap (MSB) medverkar till viss del. NSIT var initialt inriktad på gemensamma hotbildsanalyser men har i dag även börjat analysera skyddsåtgärder baserade på hotbilden.

Även om fokus i ett cyberförsvar ligger på de mest skyddsvärda verksamheterna är kopplingen till det nationella informationssäkerhetsarbetet i övrigt stark.

FRA lämnar därför också expert- och metodstöd i olika nationella och internationella samverkansgrupper, bland annat inom ramen för Samverkansgruppen för informationssäkerhet (Samfi).

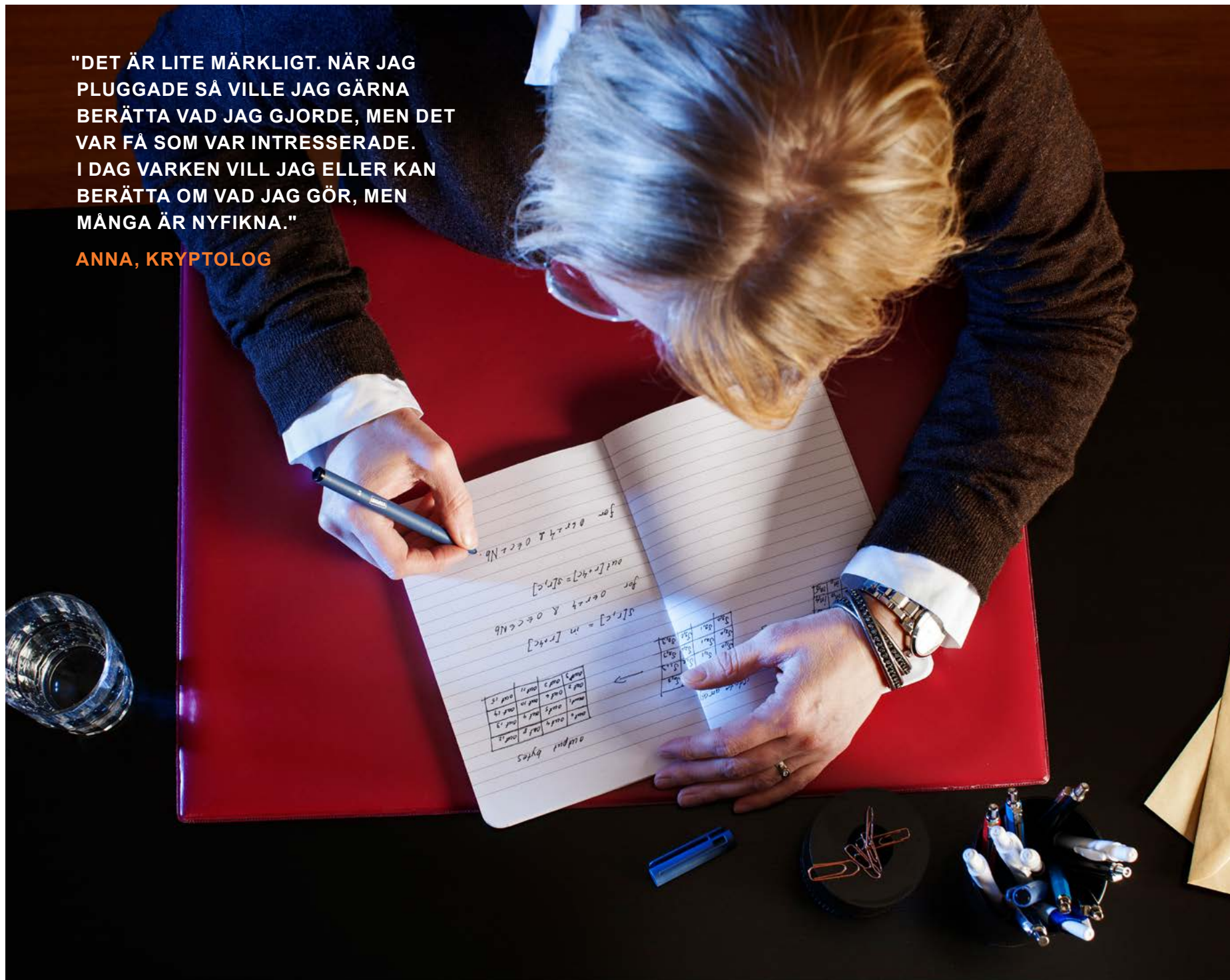
Vi ger också stöd till Försvarmakten i regeringens uppdrag att undersöka hur en svensk förmåga att utföra aktiva operationer i cybermiljön skulle kunna realiseras. Eftersom vi har kunskap kring cyberoperationer mot Sverige och djup teknisk kompetens inom informations-säkerhet kan flera förmågor från oss vara aktuella inom området.

CYBERFÖRSVAR: En nations samlade förmågor och åtgärder till skydd för dess kritiska cyberinfrastruktur som syftar till att säkerställa kritiska samhällsfunktioner samt förmågan att försvara sig mot kvalificerade angrepp.

(En definition som tagits fram gemensamt av Försvarmakten och FRA.)

"DET ÄR LITE MÄRKLIGT. NÄR JAG
PLUGGADE SÅ VILLE JAG GÄRNA
BERÄTTA VAD JAG GJORDE, MEN DET
VAR FÅ SOM VAR INTRESSERADE.
I DAG VARKEN VILL JAG ELLER KAN
BERÄTTA OM VAD JAG GÖR, MEN
MÅNGA ÄR NYFIKNA."

ANNA, KRYPTOLOG



Anna och hennes kollegor knäcker krypton

Möt Anna, 42, doktor i matematik. Hon är en av FRA:s många kryptologer och tycker att matte är det bästa som finns.

Vad har du för utbildning?

– Jag är matematiker från Stockholms universitet och doktorerade om Liealgebror.

Det får du nog förklara ...?

– All matematik handlar om logik och struktur. Man kan säga att en Liealgebra är en algebraisk struktur. Mitt arbete gick ut på att visa hur dessa kunde representeras eller beskrivas.

Hur kommer det sig att du blev intresserad av matte?

– Det blev jag först på högstadiet. Gångertabellerna på lågstadiet klarade jag väl med viss möda och det är inte matte för mig. Det är först med ekvationer som man börjar fatta vad matte handlar om och då är det ett fantastiskt ämne. Så vackert.

Hur hamnade du på FRA?

– Ja, det är en bra fråga ... Efter att jag doktorerat började jag fundera på om den akademiska karriären var något för mig och kollade runt vad som egentligen fanns för en mattenörd som jag. FRA var välkänd på matematiska institutionen. Jag

hade kompisar som hade börjat och det visade sig att FRA behövde fler kryptologer.

Vad gör en kryptolog på FRA?

– Det handlar ofta om att lösa väldigt svåra problem. Och att hitta det som sticker ut i materialet.

Varför är det så hemligt?

– Kryptofrågor har avgjort många krig eller åtminstone varit ett viktigt bidrag både strategiskt och operativt. Även i fredstid är det viktigt för ett land att ha kunskaper i krypto.

Hur är utvecklingen inom kryptologi?

– Det går sjukt snabbt. Kryptering blir mer och mer vanligt. Förr i tiden var det nästan så att om vi såg krypterad trafik visste vi att det sannolikt var något intressant. Så är det inte alls i dag.

Under andra världskriget knäckte Arne Beurling tyskarnas kod med papper och penna. Är det bara datorer som gäller i dag?

– Beräkningskraft är självklart väldigt

viktigt i dag, men någon måste ju tala om för datorn vad den ska räkna på.

Det finns mycket filmer om kryptologi, känner du igen dig?

– Jag gillade filmen om Turing. Den fångade verkligen mind-setet hos en kryptolog. Sen är det spännande att tänka att han faktiskt fick utveckla en dator för att lösa sitt problem.

Man ska vara förbannat envis. Vara beredd att slå huvudet i väggen och bara resa sig och försöka igen. Jag känner igen oss i det.

Hur hanterar du att nästan allt är hemligt?

– Det blir man van vid. Men jag tycker att det är lite jobbigt när jag inte kan berätta vart jag reser.

Kan du inte berätta något konkret som du och dina kollegor gjort?

– Inga detaljer, tyvärr. Men vi kryptologer har bidragit till avgörande pusselbitar inom viktiga frågor som har att göra med Sveriges säkerhet. För oss räcker det att veta att vi gjorde det.

Nt2Us\"c\\u0006\\u0005i0P*t2Uu\"c\\u0006\\u0005RKAN
01aC)z5^-\\u007fj\\b|,\\u001aC/z5^-D\\u0011\\u0019\\
0005i0P*t2Uu\"c\\u0006\\u0005RKANt2Up\"c\\u0003q\\
,\\u001aC/z5^-D\\u0011\\u0019\\u0018,\\u001aC*z5[Y
0005RKANt2Up\"c\\u0003q\\u001fp:]X\\u0004n;\", \"enc
\"function\": \"player\", \"md5\": \"2e6a9f3dd6428dd3f
001b[0m\", \"encoding\": \"none\"}
\"function\": \"ball\", \"md5\": \"2fa6bef65ccc43538519c
001b[0m\", \"encoding\": \"none\"}
\"function\": \"highscore\", \"md5\": \"492dafcc88e2a8fc9
EqUcyj/Y7V2bGQiuKfQPWUuYfhE0JoI2POEiSnsdYaBj4FIJj\\r
sq5wQ59ROBDc2HNAIFBhslf\\n3RQPyYHCyYy8lPaH0Y+6AfKdgZA
1ymWKTBQB9IzxoCF3eUw/+he2ZkKMEsWdwVuBl6TfcxJRmAdgyK
=\\n\", \"encoding\": \"rc4\"}
\"function\": \"score\", \"md5\": \"c552f8c17d8808e4
encoding\": \"none\"}
u001aF[\\fu4ZS\\\"c\\u0003p\\u001fp:]X\\u0004D
0\\u001aC*z5[Y\\t*b\\u000b\\u0000,i0
00Kz5^(\\u007fj\\r\\bZZ)XV\\u000
001\\by,\\u001aF[\\fu4ZS\\\"c\\u
|,\\u0011\\u0019\\u0018,\\u001aC
0005t003q\\u001fp:]X\\u0004n;\\
ANt2Up001fp:]X\\u0004D\\u0011\\u
0018,\\u000b\\u000b\\u0000,RKANt2U
001fp:]\\u0019\\u0018,\\u001aC
t*b\\u000b\\u0000\\s\"c\\u0006\\u0005i0
u0011\\u001aC)z5^-\\u007fj\\b|
KANt2Us\"c\\u0006\\u0005i0P*t2Uu
u001aC)z5^-\\u007fj\\b|,\\u001aC/z5^-D\\u0011\\u0019\\
u0005i0P*t2Uu\"c\\u0006\\u0005RKANt2Up\"c\\u0003q\\
,\\u001aC/z5^-D\\u0011\\u0019\\u0018,\\u001aC*z5[Y
0005RKANt2Up\"c\\u0003q\\u001fp:]X\\u0004n;\", \"enc
\"function\": \"player\", \"md5\": \"2e6a9f3dd6428dd3f
001b[0m\", \"encoding\": \"none\"}
\"function\": \"ball\", \"md5\": \"2fa6bef65ccc43538519c
001b[0m\", \"encoding\": \"none\"}
\"function\": \"highscore\", \"md5\": \"492dafcc88e2a8fc9
EqUcyj/Y7V2bGQiuKfQPWUuYfhE0JoI2POEiSnsdYaBj4FIJj\\r
sq5wQ59ROBDc2HNAIFBhslf\\n3RQPyYHCyYy8lPaH0Y+6AfKdgZA
1ymWKTBQB9IzxoCF3eUw/+he2ZkKMEsWdwVuBl6TfcxJRmAdgyK
=\\n\", \"encoding\": \"rc4\"}
\"function\": \"score\", \"md5\": \"c552f8c17d8808e4
encoding\": \"none\"}
u001aF[\\fu4ZS\\\"c\\u0003p\\u001fp:]X\\u0004D
0\\u001aC*z5[Y\\t*b\\u000b\\u0000,i0
00Kz5^(\\u007fj\\r\\bZZ)XV\\u000
001\\by,\\u001aF[\\fu4ZS\\\"c\\u
|,\\u0011\\u0019\\u0018,\\u001aC
0005t003q\\u001fp:]X\\u0004n;\\
ANt2Up001fp:]X\\u0004D\\u0011\\u
0018,\\u000b\\u000b\\u0000,RKANt2U
001fp:]\\u0019\\u0018,\\u001aC
t*b\\u000b\\u0000\\s\"c\\u0006\\u0005i0
u0011\\u001aC)z5^-\\u007fj\\b|
KANt2Us\"c\\u0006\\u0005i0P*t2Uu
u001aC)z5^-\\u007fj\\b|,\\u001aC/z5^-D\\u0011\\u0019\\
u0005i0P*t2Uu\"c\\u0006\\u0005RKANt2Up\"c\\u0003q\\
,\\u001aC/z5^-D\\u0011\\u0019\\u0018,\\u001aC*z5[Y
0005RKANt2Up\"c\\u0003q\\u001fp:]X\\u0004n;\", \"enc
\"function\": \"player\", \"md5\": \"2e6a9f3dd6428dd3f
001b[0m\", \"encoding\": \"none\"}
\"function\": \"ball\", \"md5\": \"2fa6bef65ccc43538519c
001b[0m\", \"encoding\": \"none\"}
\"function\": \"highscore\", \"md5\": \"492dafcc88e2a8fc9
EqUcyj/Y7V2bGQiuKfQPWUuYfhE0JoI2POEiSnsdYaBj4FIJj\\r
sq5wQ59ROBDc2HNAIFBhslf\\n3RQPyYHCyYy8lPaH0Y+6AfKdgZA
1ymWKTBQB9IzxoCF3eUw/+he2ZkKMEsWdwVuBl6TfcxJRmAdgyK
=\\n\", \"encoding\": \"rc4\"}
\"function\": \"score\", \"md5\": \"c552f8c17d8808e4
encoding\": \"none\"}

"MAN MÅSTE VARA EN LAG-
SPELARE. INGEN AV OSS KAN
LÄGGA PUSSLET SJÄLV MEN
TILLSAMMANS KAN VI GÖRA
RIKTIGT COOLA GREJER."

MATTIAS,
PRODUKTIONSLEDARE

Från bombflyg till virus på nätet

Mattias, 53, har arbetat på FRA sedan värnplikten. Han har följt de omvärldsförändringar som skett och varit en av pionjerna när FRA stått inför nya utmaningar. I dag följer han skadlig kod på internet.

Vad har du för utbildning?

– Ingen alls ...! Jag gjorde värnplikten på FRA och skulle plugga efteråt. Jag behövde en paus så jag frågade om jag kunde jobba här ett tag. Pausen har varat sen dess!

Vad fick du göra?

– Mitt första uppdrag var att följa det strategiska bombflyget i vårt närområde. Det var innan murens fall.

Blev det tomt när muren föll?

– Inte alls. Vi fortsatte att följa utvecklingen, även om förutsättningarna förändrats. Vid det laget började Försvarsmakten aktivt delta i många internationella insatser och jag fick kasta in mig i det.

Jag var med och byggde upp vårt stöd för Bosnieninsatsen. Det handlade ytterst om att bidra till säkerheten för svensk trupp. Sen jobbade jag länge med marin verksamhet i vårt närområde och följde det geomilitära pusslet på nära håll. Det är sånt vi ser efterverkningarna av i vissa av dagens konflikter.

Hur gick det konkret till?

– Genom vårt geografiska läge satt vi på första parkett och fick unik information om det som pågick. I dag är det här vardagsmat för oss. Då var vi bara några stycken som såg det nya mönstret.

Vad gör du i dag?

– I dag försöker jag framför allt att hålla jämna steg inom IT-hot. Det är inte lätt, det finns många stater som har stora resurser och som är mycket målmedvetna.

Jag var en av dem som tidigt såg att kommunikationen skulle flytta till internet. I dag finns de utländska företeelserna som vi följer sedan länge där.

Du har ofta fått göra nya saker?

– Absolut. Jag är nyfiken till min natur. Oavsett om det handlar om ny teknik eller en underrättelsefråga måste man nysta upp, dra och dra. Se hur allt vecklas upp och du börjar se det som händer. Om jag inte kommer åt något på ett sätt, provar jag ett annat. En aktör kanske dyker upp

nån annanstans och pusslet blir mer komplett. Det är lite av ett detektivarbete.

Vad ville du bli när du var barn?

– Jag hade inget särskilt drömyrke men redan i tidiga tonåren tyckte jag att världspolitik var jättespännande. Jag slukade litteratur om sånt så kanske fanns det tecken på var jag skulle hamna. Jag minns att bibliotekarien tyckte att jag var lite ung för boken om kinesisk diplomati i Sydostasien.

När jag tittar tillbaka ser jag att jag fått vara med och bygga nya förmågor när omvärlden och tekniken förändrats. Det är lite häftigt.

Vad är viktiga egenskaper för att jobba med det du gör?

– Man ska vara den visionära typen som ser bortom nästa kulle. Hinder är till för att röjas ur vägen. Vi pratar ofta om slitna uttryck som ”Thinking-Out-Of-The-Box” eller ”Pushing-Inside-The-Envelope”, men de stämmer verkligen.

A portrait of Gunnar Hellenius, a middle-aged man with short grey hair, wearing a dark blue suit, light blue shirt, and a patterned tie. He is standing in a server room, with dark server racks and perforated metal doors in the background. The lighting is dramatic, with blue light filtering through the perforations.

**"DET ÄR INTE ALLTID DEN NYASTE
TEKNIKEN SOM ÄR INTRESSANT UTAN
DET SKA VARA RÄTT TEKNIK."**

**GUNNAR HELLENIUS,
CHEF FÖR FRA:S TEKNIKAVDELNING**

Molnet och BigData – vardag för Gunnar

Gunnar Hellenius, 51, är ny chef för FRA:s tekniska avdelning. Här samsas det nya med det gamla inom teknik, och det gäller att hitta rätt teknik för rätt underrättelseområde.

Vad ser du för allmänna trender inom teknik?

– Det finns ett par tydliga trender på stark frammarsch. De jag direkt tänker på är Molnet, Internet of Things, Machine Learning och nya teknologier som Block Chain.

Vad betyder de här termerna?

– Molnet eller molntjänster kännetecknas av att resurser delas med andra, snabb skalbarhet, självbetjäning och flexibilitet för kunden. Internet of Things handlar helt enkelt om att allt blir uppkopplat, från bilen du kör till små prylar som hälsoband.

Machine Learning innebär förenklat att systemet kan lära sig självt och anpassa sig till ny information utan hjälp av människor, medan Block Chain handlar om nya sätt att göra transaktioner utan en massa mellanhänder.

Som paraply över allt finns digitaliseringen som gemensam nämnare. Den påverkar hela samhället.

Hur påverkar utvecklingen ditt uppdrag på FRA?

– Den utmaning vi kommer att leva med under en lång tid är att vi ska kunna hela spannet, från traditionell radio som används i något avlägset område där Försvarsmakten har en insats, till kommunikation på internet där aktörerna på olika sätt försöker gömma sig. Dessutom ska systemen drifas och förvaltas. En stabil och effektiv drift är ett måste i vår verksamhet.

Det är komplext men vår uppgift är att stödja verksamheten med rätt teknik. Det är inte alltid den nyaste tekniken som är intressant utan det ska vara rätt teknik utifrån de utländska underrättelsemålen.

Men det är klart att djupt kunnande i det digitala nätet i dag är en förutsättning för att klara vårt uppdrag och utvecklingen drivs av det som händer på internet.

Är det möjligt att hänga med i all teknik?

– Självklart inte. Mitt uppdrag handlar om att hitta bästa mixen över tid. Vår ut-

maning är den stora bredden som vi ska behärska med begränsade resurser.

Hur många tekniker har FRA?

Det är en uppgift som jag inte kan lämna ut. Det är sådant som en underrättelse-tjänst inte gärna berättar eftersom det ger en inisning om vår förmåga totalt sett. Men vi är en stor teknikorganisation med tyngdpunkt på utveckling.

Vilka egenskaper är viktiga hos en utvecklare?

– Intresse för verksamheten förstås, man ska ha ett driv att hjälpa till. Det är bra om man har stor bredd i botten och sedan en specialkompetens på ett programmeringsspråk som till exempel Java/C++ eller på Big Data-lösningar.

Du ska våga utmana dig själv och ha uthålligheten. Du måste också ha tillit till andra – du kommer inte att klara det själv och du måste ha alternativa planer om något går fel. Det är ett spännande jobb om man är intresserad av teknik!

**KUNSKAP OM UTLANDET –
FÖR SVERIGES SÄKERHET OCH INTEGRITET**