FRA:s överdirektör Charlotta Gustafsson: FRA:s roll i Sveriges cybersäkerhetsarbete

(anförande vid Försvarsutskottets öppna utfrågning rörande cybersäkerhet, den 17 april 2018)

”Jag heter Charlotta Gustafsson och är överdirektör på FRA. Jag vill tacka för möjligheten att få beskriva för er vad FRA arbetar med i detta ämne.

Under mina tio minuter tänkte jag först beskriva FRA:s roll inom cybersäkerhetsarbetet. Sedan kommer jag att berätta om vår verksamhet på området.

Redan inledningsvis skulle jag vilja ringa in vilket område vi arbetar med – det är fientliga aktiviteter som kommer från statliga eller statsunderstödda aktörer. Det är framför allt detta som utgör hotet mot Sverige och våra viktiga samhällsfunktioner.

Även om FRA bidrar till att skydda de viktigaste funktionerna hos vårt samhälle, och dessutom bara hanterar de hot som kommer från statsaktörer – så har vi tillräckligt att göra: Vi ser ett mycket stort antal angrepp från utländska statsaktörer. Utländska statsaktörer visar en utomordentlig målmedvetenhet vad gäller att systematiskt hacka sig in i våra viktigaste system. Och då ser vi på FRA ändå inte allt.

Varför gör då vissa stater detta? Syftena varierar, men domineras av vilja att komma åt information. Man vill ha kvalificerad teknik och sådant utvecklingsarbete som kostat mycket tid och pengar. Detta kan ofta ha rent kommersiella syften.

Vissa aktörer är exempelvis intresserade av vapensystem. Man vill också genom kunskap om svensk försvarsförmåga utveckla sitt militära uppträdande.

Även överväganden som finns inom politik och statsledning hör till det som utländska statsaktörer vill ha information om.

Som ni hör är det framför allt klassiskt spionage vi talar om – men som genom nätet numera är så oerhört mycket lättare, billigare och riskfriare än med äldre metoder. Detta är numera knappast några nyheter.

En annan fullt tänkbar strävan är att genom skadlig kod kunna sabotera vårt samhälle, så att vi exempelvis inför en militärt skärpt situation ska mista sådana funktioner som vi behöver för att kommunicera, handla mat och värma våra bostäder.

Vi har ju här redan hört beskrivas vikten av ett gott och systematiskt informationssäkerhetsarbete. Man ska ha genomtänkta system, där skyddet dimensionerats efter de risker man ser. Att förbättra informationssäkerheten i hela samhället är väldigt viktigt.

Men när det är sagt – för de utländska aktörer som jag just beskrivit, finns inga inbrottsäkra miljöer. Enheter som är uppkopplade till internet går att hacka sig in i, det är bara en fråga om tid, kompetens och resurser.

Och statsaktörer har alla tre sakerna: De har tid. De har kompetens. Och de har resurser.

Bara genom att själv ha samma typ av kompetens och resurser kan man bygga ett skydd som kan upptäcka de mest kvalificerade angreppen. Det har vi byggt upp på FRA, under ett antal år. Vår förmåga inom cybersäkerhet är idag väl utvecklad, och utvecklas löpande.

En fördel som vi har på FRA är vår traditionella verksamhet, nämligen att utgöra Sveriges signalunderrättelsetjänst. En stor del av den verksamheten sker numera i det globala nätet. Vi har stor kunskap om en del aktörers sätt att agera. Vi vet hur skadlig kod kan användas, och vi ser hur den används i praktiken. Det är kunskap som vi har får genom signalunderrättelseverksamheten. Idag är arbetet med signalspaning mot

omvärlden och att skydda Sverige mot cyberangrepp två sidor av samma mynt.

Dessa uppdrag är inte samma sak, det vill jag betona. De bygger på olika uppdrag och har delvis olika lagstöd. Men de stärker varandra sett till vår kompetens på båda områdena och stärker vår förmåga att fullgöra båda uppdragen.

Signalspaningsförmågan ger en unik bild av utländska angripare och deras angrepsmetoder. Förmågan gör att vi har kvalificerad kunskap som också kan användas i arbetet med att stärka Sveriges informationssäkerhet. Signalunderrättelseverksamheten och arbetet mot statsunderstödda IT-angrepp vinner båda mycket på att utföras inom samma organisation.

Sverige vinner på den kombinationen, jämfört med alternativen.

Cybersäkerhet ger inte full effekt om den bara utförs *åt* andra. Vårt enskilda arbete är viktigt, men det får bäst utväxling när det sker *med* andra. Genom oss fyra som representerar var sin myndighet ser ni idag hur staten fördelat uppgifter och kompetenser. Vi gör det inte som isolerade öar, utan har ett gott samarbete både systematiserat och mer informellt. Tillsammans bygger vi Sveriges cyberförsvar.

Vad gör vi då konkret på FRA, för att hantera den cybermiljö jag och andra idag beskrivit för er?

1. Från FRA:s sida bistår vi myndigheter och statliga bolag i deras informationssäkerhetsarbete. En rad myndigheter har genom åren fått sin IT-säkerhet analyserad. I det uppdrag vi får från dessa myndigheter ingår ofta att testa och försöka skaffa oss kontrollen över deras IT-system. Efter att vi avslutat säkerhetsgranskningen, brukar vi ha en mycket givande diskussion om hur IT-säkerheten på den aktuella myndigheten bäst kan utvecklas.

2. Statliga aktörer har resurser att utveckla *skräddarsydda* program för att tränga sig in i *utvalda* IT-system – då finns det i förväg ingen kännedom om dessa program. Inga antivirusprogram kommer att varna, hur uppdaterade de än må vara.

   Därför har FRA utvecklat en typ av tekniskt detekterings- och varningssystem som larmar om det känner av vad som kan vara ny och tidigare okänd skadlig kod. Information om angreppet skickas tillbaka till FRA för analys. Vi kallar det för TDV och det är i drift hos ett antal myndigheter. Det ersätter inte sedvanliga skydd, men är ett viktigt komplement.

3. FRA lämnar stöd till samhällsviktiga funktioner i användandet av säkra kommunikationer. Ansvaret för att krypton utvecklas och håller nödvändig kvalitet åligger Försvarsmakten. Vi på FRA har kontakterna med de civila verksamheter som använder krypton, ser till att personalen utbildas och att de uppdaterar sina system.

4. Ingen har missat debatten om outsourcing av IT-tjänster och hur detta kan göras mer eller mindre smart. Från FRA:s sida har vi publicerat en öppen rekommendationsskrift för den som överväger att låta underleverantörer hantera IT-driften. Om man följer våra rekommendationer kommer man att göra de viktiga överväganden som avgör om outsourcing är en bra idé, eller om det är en inbjudan till intrång och förlust av information till obehöriga.

   Den konkreta händelsen bakom dessa rekommendationer var ett angrepp som fått namnet Cloud Hopper. Det var ett ganska väl konstruerat angrepp, och använde just tjänsteleverantörer inom IT för att vinna tillträde till deras kunder. Systematiskt och bit för bit, kunde angriparna plocka ut information. FRA spelade en ledande roll när Cloud Hopper upptäcktes. Vi kunde också identifiera angriparen som låg bakom. Cloud Hopper visade sig ha varit verktyget för intrång på många platser i världen.

5. För ett år sedan gav regeringen FRA och Säkerhetspolisen ett uppdrag som motiverades just av angrepp såsom Cloud Hopper. Vi skulle inleda ett fördjupat samarbete kring de mest skyddsvärda verksamheterna i vårt samhälle, och hur de bör skyddas mot de allvarligaste hoten. Vi tycker att det är bra att ytterligare fördjupa samarbetet mellan oss på FRA som ju har signalspaning och cybersäkerhet som uppdrag, och Säkerhetspolisen som är Sveriges säkerhetstjänst. Nyligen har regeringen sett till att också Försvarsmakten är med i detta arbete.

   Att vi samarbetar i dessa frågor är inte nytt. Exempelvis har vi samlats inom något vi kallar NSIT, nationell samverkan mot allvarliga IT-hot. Vi samutnyttjar där FRA:s, Försvarsmaktens och Säkerhetspolisens mest specialiserade kompetenser och arbetar i konkreta projekt. Som alltid,

arbetar vi inom ramen för respektive myndighets uppdrag och befogenheter.

6. Regeringen har ju gett Försvarsmakten uppdraget att utveckla och förstärka det svenska cyberförsvaret. Det ska enligt direktiven ske i nära samverkan med FRA. En väsentlig del i detta arbete är frågan om svensk kapacitet till aktiva förmågor i cybermiljön. En sådan kapacitet vore en viktig och naturlig del av ett framtida svenskt cyberförsvar.

Som ni hör genomförs det mesta av FRA:s verksamhet inom cybersäkerhet i nära samverkan med andra. Det samarbetet och vår egen kombination av uppdrag inom både cybersäkerhet och underrättelser fungerar väl.

Därmed har jag gått igenom de viktigaste delarna av FRA:s verksamhet och ser fram emot att om en stund och tillsammans med mina kolleger från de övriga myndigheterna få svara på utskottets frågor. Tack.”