InfoSäkutredningen

Delrapport 1 om signalskydd

STATENS OFFENTLIGA UTREDNINGAR

SOU 2003:27

Missiv

Till statsrådet och chefen för Försvarsdepartementet

Genom beslut den 11 juli 2002 (dir. 2002:103) bemyndigade regeringen chefen för Försvarsdepartementet att tillkalla en särskild utredare med uppdrag att bedöma behovet av signalskydd i samhällsviktig verksamhet samt att lämna förslag till organisatorisk placering, lokalisering, uppgifter, ledning och samordning av signalskyddstjänsten.

Genom tilläggsdirektiv beslutade den 20 februari 2003, utökades utredningens uppdrag. Den särskilde utredaren fick utöver det ursprungliga uppdraget i uppgift att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas, hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet bör utformas i framtiden samt hur OECD:s riktlinjer om nät- och informationssäkerhet kan genomföras i Sverige. Utredaren skall dessutom följa myndigheternas uppbyggnad av de verksamheter som regeringen aviserade i propositionen Samhällets säkerhet och beredskap angående informationssäkerheten i samhället (prop. 2001/02:158).

Med stöd av regeringens bemyndigande kallade chefen för Försvarsdepartementet f.d. riksdagsledamoten Anders Svärd till särskild utredare (Regeringsbeslut 2002:1743/CIV, Protokoll Fö 2002:1744/EPS).

Till sakkunniga utsågs den 15 januari 2003, med början den 2 oktober 2002, kansliråd Ulf Johansson och ämnessakkunnig Richard Oehme och till experter ämnessakkunnig Helena Lindberg, chefsjurist Elisabeth Lager, avdelningschef John Daniels, avdelningsdirektör Arne Jonsson och avdelningsdirektör Kristina Starkerud. Departementsrådet Michael Mohr utsågs, också med början den 2 oktober 2002, till huvudsekreterare. Josefin Grennert förordnades som sekreterare den 1 december 2002.

Som referensgrupp i arbetet har fungerat en informell grupp inom Regeringskansliet som utbyter information om informationssäkerhetsfrågor. Gruppen består av representanter från Justitiedepartementet, Utrikesdepartementet, Försvarsdepartementet, Finansdepartementet och Näringsdepartementet

Utredningen har antagit namnet InfoSäkutredningen.

Utredningen har genomfört besök och intervjuer för att kartlägga, skapa överblick och definiera problem inom signalskyddsområdet. Kontakter med företrädare för näringslivet har också tagits. Inför avlämnandet av denna rapport har även ett seminarium genomförts med deltagande av berörda departement, myndigheter och organisationer.

Stockholm 28 februari 2003

Anders Svärd

/Michael Mohr

Josefin Grennert

Innehåll

1 Uppdraget 5

1.1 Bakgrund 5
1.1.1 De ursprungliga direktiven 7
1.1.2 Tilläggsdirektiven 8

1.2 Arbetets uppläggning och genomförande 9

2 Vad är signalskydd? 11

2.1 Begreppet signalskydd 11

2.2 Historik 12

3 Dagens signalskyddsverksamhet 15

3.1 Signalskydd inom totalförsvaret 15
3.1.1 Nyckelproduktion 15
3.1.2 Nyckeldistribution 16
3.1.3 Kontrollverksamhet 16
3.1.4 Kompetensförsörjning 17
3.1.5 Materielanskaffning och finansiering 19

3.2 Övrig signalskyddsverksamhet i samhället 20

3.3 Internationellt 21

4 Behov av signalskydd idag och i framtiden 23

4.1 Allmänt ... 23
4.2 Totalförsvarsbegreppets inverkan ... 23
4.3 Nationellt ... 25
4.4 EU ... 27
4.5 Internationellt ... 28

5 Säkerhetsskydd ... 31

5.1 Nya behov ... 31
5.1.1 Signalskydd – en del av säkerhetsskyddet ... 32
5.1.2 Närmare om säkerhetsskyddslagen m.m. ... 33

6 Signalskydd och informationssäkerhet ... 37

7 Utredningens överväganden ... 39

Akronymlista ... 41

Kommittédirektiv ... 43

Tilläggsdirektiv ... 49

1 Uppdraget

1.1 Bakgrund

I takt med att samhället har blivit allt mer beroende av olika informationssystem har vikten av att förbereda sig för IT-relaterade hot av olika slag ökat. Regeringen har närmare beskrivit hotbilden för attacker mot eller via informationssystem i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 104 f). Där konstateras att en av svårigheterna med hanteringen av de IT-relaterade hoten är att urskilja vem aktören är, eftersom ingen absolut åtskillnad mellan olika typer av aktörer kan göras. Detta faktum gör det särskilt svårt att skydda sig eftersom säkerhetsåtgärderna måste anpassas till samtliga typer av aktörer. Ytterligare en försvårande faktor är att de IT-relaterade hoten är geografiskt obundna. Den som vill göra intrång i eller på annat sätt manipulera ett informationssystem i Sverige kan befinna sig var som helst i världen.

Behovet av att skydda information i form av meddelanden och trafik eller elektroniskt lagrad information ökar i dagens samhälle i takt med att myndigheter och företag digitaliserar sina arbetsprocesser och därmed sin information. Även information som idag inte omfattas av signalskydd kan vara skyddsvärd. Exempel på sådan skyddsvärd information kan vara uppgifter

som gäller känslig infrastruktur, ekonomi och personliga förhållanden.

Utvecklingen av signalskyddssystem sker idag till största delen inom Försvarsmakten, utifrån de krav som behovet av att kunna hantera information som omfattas av sekretess till skydd för rikets säkerhet ställer. Utvecklingen av IT-säkerhetslösningar i samhället i övrigt styrs allt mer av behovet av att skydda information som inte omfattas av sekretess till skydd för rikets säkerhet. På grund av detta delade behov är det rimligt att signalskyddstjänsten utvecklas till att även kunna hantera andra kryptografiska skyddsbehov än de som utvecklas för skydd av rikets säkerhet och att en bedömning av hela samhällets skyddsförmåga görs.

Idag leds signalskyddstjänsten av en funktion inom Försvarsmakten (MUST ITSA). För att tillse att de civila behoven av signalskydd prioriteras i tillräcklig utsträckning bör frågan om var signalskyddstjänsten på nationell nivå skall organiseras och lokaliseras övervägas.

Regeringen angav i propositionen Ett informationssamhälle för alla (prop. 1999/2000:86) att den välkomnar en bred användning av kryptografi. I enlighet med detta bör det övervägas om det finns behov av en rådgivande funktion i kryptografifrågor i Sverige. Det finns ett behov av att undersöka i vad mån signalskyddstjänsten kan utgöra ett sådant rådgivande organ i samhället.

Det statliga behovet av att kunna hantera signalskyddsutrustning och kryptonycklar även i internationella sammanhang ökar i takt med ökande samarbete med andra stater och internationella organisationer. Det bör övervägas om signalskyddstjänsten kan bistå i den utvecklingen.

I det följande redogörs kortfattat för direktiven samt tilläggsdirektiven.

1.1.1 De ursprungliga direktiven

Utredningen skall, mot bakgrund av utvecklingen på informationssäkerhetsområdet, göra en bedömning av behovet av signalskydd i samhällsviktig verksamhet samt lämna förslag på hur signalskyddsverksamheten skall utformas. Utifrån det bedömda behovet skall utredningen ge förslag på organisatorisk placering av signalskyddstjänsten, dess lokalisering, uppgifter, ledning och samordning av densamma.

I utredningens direktiv anges att särskild uppmärksamhet bör ägnas följande frågor:

- Hur bör signalskyddsverksamheten utformas så att den kan komma till nytta inom fler samhällssektorer?
- Vilka samhällsektorer har störst behov av signalskydd och vilka krav ställer de?
- Vem skall vara ansvarig för signalskyddet och hur skall detta vara organiserat?
- Vilka uppgifter skall signalskyddstjänsten ha och hur skall ledning och samordning ske?
- Hur säkerställs att det framtida behovet av kompetens inom det kryptografiska området kan tillgodoses?
- Hur säkerställs samordning med andra länders signalskyddsorganisationer på ett förtroendefullt och säkerhetsmässigt trovärdigt sätt?

- Hur åstadkoms en nationell distributionsfunktion för signalskyddsmateriel och signalskyddsnycklar för det internationella samarbetet?

En delrapport om signalskyddstjänsten skall lämnas senast den 28 februari 2003.

I direktiven aviseras regeringens avsikt att i tilläggsdirektiv utöka utredningens uppdrag till att även omfatta frågor om informationssäkerhet i stort samt att genomföra den utvärdering som regeringen beskrivit i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158). Regeringen uttryckte sin avsikt att återkomma under hösten med tilläggsdirektiven.

En slutrapportering av uppdraget skall lämnas senast den 6 maj 2005.

1.1.2 Tilläggsdirektiven

Den 20 februari 2003 beslutade regeringen om tilläggsdirektiv för utredningen. Utredningen skall, utöver de ursprungliga uppgifterna, lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas, hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsarbetet skall utformas samt hur OECD:s riktlinjer om nät- och informationssäkerhet kan genomföras i Sverige. Utredningen skall dessutom följa myndigheternas uppbyggnad av de verksamheter som regeringen anmälde i propositionen Samhällets säkerhet och beredskap angående informationssäkerheten i samhället (prop. 2001/02:158, kap. 17). I propositionen anmälde regeringen sin avsikt att genomföra en utvärdering av organisatoriska och övriga konsekvenser av propositionens förslag.

1.2 Arbetets uppläggning och genomförande

Utredningen har varit i kontakt med berörda myndigheter och organisationer i syfte att inhämta underlag till diskussion om och bedömning av nuvarande ordning. Besök har gjorts vid Försvarets radioanstalt (FRA), Militära underrättelse- och säkerhetstjänsten (MUST), Krisberedskapsmyndigheten, (KBM), Totalförsvarets signalskyddssamordning (TSA), Säkerhetspolisen (Säpo), Totalförsvarets forskningsinstitut (FOI), Totalförsvarets signalskyddsskola (TSS) och Försvarets materielverk (FMV). Övriga organisationer som har besökts är Näringslivets säkerhetsdelegation (NSD), Svenska Bankföreningen och Ericsson. Utöver dessa besök har utredningen deltagit i totalförsvarets centrala signalskyddsmöte, den 4-5 december 2002 i Göteborg.

Arbetet har genomförts i nära samarbete med Försvarsmakten, Försvarets radioanstalt, Rikspolisstyrelsen (Säpo) och Krisberedskapsmyndigheten.

2 Vad är signalskydd?

2.1 Begreppet signalskydd

I ett alltmer utvecklat informationssamhälle används tele- och informationssystem för i stort sett all samhällsverksamhet. Obehöriga aktörer kan av olika skäl, genom aktiva och passiva åtgärder, försöka skaffa sig tillgång till den information som förmedlas i systemen. Termen signalskydd har visserligen sina rötter i den avlyssning genom signalspaning som ständigt pågår mot telekommunikations- och informationssystem som en väsentlig del av främmande makts underrättelsetjänst, men signalskydd är också ett relevant begrepp för behovet av att skydda information i bred mening, till exempel transaktioner i finansiella system eller uppgifter som rör personliga förhållanden.

Riskerna med att försöka skaffa sig tillgång till information i olika system är många gånger relativt små, och kan samtidigt ge mycket bra resultat. De olika aktörer som kan vilja skaffa sig tillgång till information omfattar allt från stater till enskilda. Så till exempel bedrivs signalspaning av andra stater för att på strategisk, operativ och taktisk nivå få insyn i verksamhet och inhämta underrättelser genom att upptäcka, avlyssna och kartlägga data- och telekommunikationer och informationssystem. Sådan signalspaning kan ske från eget territorium, andra länders territorium, internationellt vatten och

luftrum samt från rymden. I andra sammanhang kan avlyssning eller manipulering av information utgöra ett led i brottslig verksamhet.

Signalskydd är åtgärder som syftar till att förhindra obehörig insyn i och påverkan av tele- och radiokommunikationer. Signalskydd omfattar också användning av kryptografiska funktioner i informationssystem. Kryptografiska funktioner används för att uppnå sekretess, det vill säga att endast den som är behörig ska kunna läsa eller förändra data. Vidare syftar användningen till att garantera autentisering och identifiering, vilket innebär att data inte ska kunna förvanskas obemärkt respektive att en avsändare kan bevisa sig vara den han eller hon utger sig för. Ett fjärde syfte med kryptografiska funktioner är oavvislighet. Ingen skall kunna utföra en handling, till exempel en elektronisk betalning, och sedan påstå sig inte ha utfört den. Kryptografiska funktioner kan även användas i specifika syften, såsom till exempel vid elektroniska val, för att garantera anonymitet, verifierbarhet, att ingen röstar mer än en gång och så vidare. Genom att använda signalskydd skyddar vi oss mot obehörig insyn och manipulering eller förvanskning av information.

Exempel på signalskyddsåtgärder är kryptering, täckning, omskrivning, radiotystnad, bandspridning, val av sambandsmedel, användning av digitala signaturer för säker verifiering av elektroniska dokument samt identifiering och autentisering av användare och information.

2.2 Historik

Inom den offentliga sektorn har signalskyddsverksamheten vuxit fram främst som ett resultat av de militära behoven och inom ramen för totalförsvarsverksamheten. Det militära försvarets behov av signalskydd har i sig motiverat relativt omfattande statliga satsningar, och efterhand som behoven av samordning

mellan det militära och det civila försvaret uppmärksammats, har en särskild struktur och organisation vuxit fram.

Före 1959 sköttes Försvarsmaktens signalskyddstjänst inom varje försvarsgren utan någon nämnvärd samverkan. Inom det som idag kallas totalförsvarets civila del förekom endast begränsad signalskyddsverksamhet. Det militära och det civila försvaret använde sig av olika system för att skydda sin signalering, varför säker kommunikation mellan de båda delarna av försvaret var problematisk.

För att verka för en gemensam struktur infördes 1959 en för totalförsvaret gemensam signalskyddstjänst, Statens Signalskyddsnämnd (SN), under dåvarande Inrikesdepartementet. Beredande och verkställande organ var signalskyddsbyrån (Byrå K). På grund av ökande effektivitetskrav lades senare SN ned och Byrå K blev 1968 Totalförsvarets signalskyddsavdelning (TSA) i Försvarsstabens Sektion 1. Utbildningsorganet, Statens Signalskyddsnämnds skola (SNS), bytte namn till Totalförsvarets Signalskyddsskola (TSS) och inordnades under Stabs- och sambandsskolan (StabSbS). Efter omorganiseringen leddes signalskyddstjänsten av Överbefälhavaren. Detta gav Försvarsmakten en stor roll i det civila försvarets signalskydd.

Inom Försvarsmakten har chefen för Militära underrättelse- och säkerhetstjänsten (MUST) idag ansvaret för samtliga uppgifter inom området (regelverk, utveckling, driftstöd och kontroll). Signalskyddsärendena för totalförsvaret, det vill säga Försvarsmakten, Försvarsmakten närstående myndigheter och de civila myndigheter som ingår, bereds och verkställs av TSA. TSA ingår organisatoriskt i IT-säkerhetsavdelningen (ITSA) vid MUST i Högkvarteret (HKV). TSA har ansvaret för signalskyddsärenden inom hela totalförsvaret men Krisberedskapsmyndigheten (KBM) samordnar signalskyddstjänsten inom totalförsvarets civila del. KBM

anskaffar signalskyddsmateriel för områdesvis civil ledning samt för samverkan mellan civila myndigheter genom att beställa från Försvarets materielverk (FMV). KBM anlitar Försvarsmakten S1 (Upplands Regemente)/TSS för utbildning av signalskyddspersonal vid de civila myndigheterna.

FMV har förutom upphandlingsansvar för signalskyddsmateriel även uppgift att samordna signalskyddsverksamheten vid försvarsindustrin.

Inom övrig offentlig verksamhet och i kommersiella sammanhang har signalskydd använts relativt sparsamt. Först när utvecklingen av olika informationssystem lett till såväl ökat beroende som mer påtagliga hot har behoven av skydd uppmärksammats. Inom kommersiell verksamhet har det i första hand handlat om en ökad användning av kryptosystem, där syftet har varit att skydda information om företagens finansiella läge eller affärsstrategiska överväganden. Alltmer har det också kommit att handla om forskning och utveckling, som i många högteknologiska företag betraktas som den viktigaste tillgången. Att en allt större del av handeln med varor och tjänster bedrivs via till exempel Internet bidrar också till ett ökat behov av olika former av kryptering.

3 Dagens signalskyddsverksamhet

3.1 Signalskydd inom totalförsvaret

Prioriterade uppgifter inom ramen för den signalskyddsverksamhet som bedrivs av Försvarsmakten TSA, är att utveckla och godkänna kryptosystem för kryptering av hemliga uppgifter (13 § 2:a stycket i Säkerhetsskyddsförordningen (1996:633) stadgar att hemliga uppgifter får krypteras endast med kryptosystem som har godkänts av Försvarsmakten), tillhandahålla kryptografisk funktion för riktighet, autentisering, och oavvislighet, nyckelförsörjning för alla system i drift samt att utarbeta regelverket för signalskyddstjänsten. Det ses som viktigt att verksamheten bedrivs i direkt närhet av utvecklingen av komplexa informations- och kommunikationssystem, då kryptofunktioner ofta är en del av dessa. Samtliga uppgifter ställer krav på välutbildad och behörig personal.

3.1.1 Nyckelproduktion

Kryptonycklar är en viktig del av den kryptologiska funktionen i signalskyddssystemen. Nycklarna produceras nästan uteslutande av TSA för användning på olika myndigheter inom ramen för totalförsvarsverksamheten. TSA ansvarar också för att utveckla de datorprogram som genererar nycklar. Medier som används för

kryptonycklarna är papper i form av tryckta streckkoder, hålkort samt smarta kort och andra datamedier. Tillverkning är en känslig process med hög sekretess som förutsättning för att signalskyddssystemen skall fungera som de är avsedda att göra. Att varje nyckel i sig är en hemlig handling ställer stora krav på noggrannhet i alla led. TSA har ansvaret för att arbetet bedrivs på ett korrekt sätt och har utvecklat ett system för kontroll inom sin produktionsenhet.

3.1.2 Nyckeldistribution

Distributionen av kryptonycklar sker idag i huvudsak genom postbefordran. TSA distribuerar producerade nycklar till ett antal centrala myndigheter samt internt inom Försvarsmakten. KBM får nycklar för den civila delen av totalförsvaret för vidare distribution av dessa till myndigheter på regional och lokal nivå. Eftersom innehållet i dessa försändelser är hemligt är det viktigt att kontrollera att de verkligen når rätt mottagare. KBM anser att distributionen av kryptonycklar sker enligt säkra rutiner och med högt ställda krav på säkerhet i samtliga led. Det är viktigt att upprätthålla säkerhetsskyddet till dess att nycklarna upphört att gälla och förstörts.

3.1.3 Kontrollverksamhet

3.1.3.1 Signalkontroll

Signalkontrollverksamheten inom TSA syftar främst till att kontrollera att de signalskyddssystem som är i drift används på ett riktigt sätt och att de ger det skydd de är avsedda att ge. Kontroll sker också av den klartexttrafik som förekommer i samband med olika övningar och materielförsök. Den insamlade trafiken analyseras för att få reda på om det har förekommit

något som röjer den kontrollerade verksamheten. Den kontrollverksamhet som bedrivs av TSA är helt inriktad på trafik inom totalförsvaret. Den enhet som idag finns inom TSA utgör en liten, och därför känslig, resurs. Uppgifterna är stora och resurserna begränsade, trots att enheten endast utnyttjas inom totalförsvaret. Gruppen används idag i huvudsak inom Försvarsmakten samt vid olika former av materielförsök, vilka man gör på uppdrag av FMV.

3.1.3.2 Administrativ kontroll

TSA genomför också en administrativ kontroll av signalskyddsverksamheten vid de olika myndigheter som har en signalskyddsorganisation. Vid dessa kontroller undersöks att myndigheten följer det regelverk i form av föreskrifter, instruktioner och allmänna råd som är utgivet av TSA. Kontrollerna skall också ses som ett led i att utbilda och informera myndigheterna om förändringar och nyheter. Avsikten är att felaktig hantering av signalskyddsmateriel, kryptonycklar och totalförsvarets aktiva kort (TAK) skall upptäckas och kunna rättas till.

3.1.4 Kompetensförsörjning

3.1.4.1 TSS

Totalförsvarets signalskyddsskola (TSS) är en del av Försvarsmakten Upplands Regemente, S1. Skolan har till uppgift att samordna signalskyddsutbildningen inom totalförsvaret. Detta sker genom att man anordnar utbildning för systemoperatörer och personal för administration av kryptonycklar och användare, tidigare benämnda kryptörer, på

olika typer av signalskyddssystem. TSS bedriver också utbildning som ger behörighet att arbeta som signalskyddschef. Verksamheten omfattar även utbildning av signalskyddslärare som sedan sköter utbildningen lokalt, till exempel inom eget förband. Utbildningen bedrivs dels vid TSS lokaler i Enköping och dels genom att lärare genomför utbildning vid myndigheterna. Försvarsmakten bedriver också utbildning inom signalskydd vid I 19/Signalbataljon, Försvarsmaktens Halmstadskolor, Örlogsskolorna i Berga och Karlskrona.

Försvarsmakten finansierar elever från Försvarsmakten och Försvarsmakten närstående myndigheter (FMV, FOI, KBV, FHS, FRA och FortV) som genomgår signalskyddsutbildning vid TSS, och KBM står för kostnaderna för de civila eleverna vid TSS.

3.1.4.2 Kryptologer

Hörnstenar i signalskyddet är förmågan att utveckla kryptografiska funktioner och att granska implementeringen av dem i systemlösningar och andra typer av produkter som använder kryptografi. Förmågan är beroende av tillgången på kvalificerade kryptologer – ett yrke som kräver lång högskoleutbildning inom matematik och teknik. Nödvändig erfarenhetsuppbyggnad och specialisering sker inom statsförvaltningen genom arbete vid FRA och TSA. Antalet personer som söker sig till denna typ av arbeten är få i ett litet land som Sverige.

För att säkerställa rätt matematisk kompetens och hög förmåga, har den så kallade kryptologpoolen etablerats. FRA organiserar denna resurs, som utgör ett nationellt kompetenscentrum för kryptologi. Poolen har bland annat till uppgift att säkerställa en hög kryptologisk kompetens samt att tillse att det finns ett fruktbart informationsutbyte mellan verksamhetsområdena forcering och kryptoutveckling, samtidigt som dessa båda

verksamhetsområden medvetet hålls organisatoriskt skilda åt - kryptoutvecklingen sker inom TSA och forceringsverksamheten bedrivs av FRA. Denna ordning anses vara ett effektivt och avgörande tillvägagångssätt för att skapa god och aktad förmåga inom kryptografi. Detta ses som en av de viktigaste orsakerna till att Sverige är framstående inom såväl forceringsverksamhet som utveckling av krypto. Kunskap om forcering är grundläggande för konstruerandet av skydd. Kunskapen utnyttjas inom kryptologpoolen men skulle även kunna användas inom andra delar av samhället.

Personal från FRA tjänstgör vid MUST/TSA för kryptografiskt utvecklingsarbete inom totalförsvaret. Personalen gör även oberoende bedömningar av vissa andra svenska kryptosystem. FRA och Försvarsmakten stödjer dessutom Regeringskansliet och Rikspolisstyrelsen i kryptofrågor.

3.1.5 Materielanskaffning och finansiering

Det finns en mängd kryptosystem att tillgå som COTS (kommersiellt tillgängliga system). För vissa behov, till exempel militära, anses det dock krävas särskilt kvalificerade system. Sådana system måste utvecklas alternativt anpassas till kravspecifikationen för att fastställda säkerhetskrav skall uppfyllas. Utveckling av totalförsvarsgemensamma, fristående kryptoprodukter sker genom att Försvarsmakten ger FMV i uppdrag att lägga ut tillverkningen på företag som kan realisera beställningen utifrån den av TSA uppställda målsättningen. TSA granskar och godkänner upphandling av utvecklingsuppdraget. För funktionsspecifika kryptosystem, till exempel för JAS 39 Gripen, ingår framtagandet i utvecklingsprojektet. Beställningen går via FMV på samma sätt som för övriga kryptoprodukter.

Försvarsmakten ansvarar i huvudsak för finansieringen av TSA:s verksamhet och för att utveckla nya signalskyddssystem. Krigsförbandsledningen (KRI) finansierar materielsystem,

utveckling och framtagning av kryptoprodukter, för totalförsvaret.

Anskaffning av kryptosystem för totalförvarets behov sker i dag genom att Försvarsmakten, och i enstaka fall KBM, ger FMV uppdrag att upphandla. Upphandlingen sker sedan i nära samarbete mellan FMV och TSA. Under de senaste åren har antalet lämpliga leverantörer minskat avsevärt. Idag utnyttjas fyra till fem svenska företag för tillverkning och utveckling av de signalskyddssystem som nyanskaffas men även företag utanför Sverige anlitas.

Försvarsmakten finansierar idag anskaffning av signalskyddsutrustning för den militära delen av totalförsvaret och KBM finansierar i huvudsak anskaffning för den civila delen. Försvarsmakten närstående myndigheter finansierar sin egen anskaffning om det inte i författning eller i avtal med Försvarsmakten framgår annat.

3.2 Övrig signalskyddsverksamhet i samhället

Inom kommersiell verksamhet har det utvecklats en användning av kryptografi som inte är relaterad till totalförsvaret eller samhällsviktig verksamhet. Syftet med skyddet är kommersiellt snarare än försvarsrelaterat. För många företag är information, till exempel om forskning och utveckling, den viktigaste tillgången. Uppgifter om det finansiella läget eller affärsstrategiska överväganden, såsom upphandling, är känslig information som andra företag eller underrättelseorganisationer kan vara intresserade av. Skyddsbehoven utanför den offentliga sektorn växer i takt med att verksamheter blir allt mer informationsbaserade. Att en allt större del av handeln med varor och tjänster bedrivs via till exempel Internet bidrar också till ett ökat behov av olika former av kryptering.

Exempel på verksamheter som kräver kryptografiskt skydd är banktjänster via Internet, där kunden använder sig av någon form av digital signatur för att koppla upp sig mot banken över Internet. Ett annat användningsområde är e-handel där det kan vara önskvärt att inte kontokortsnummer skickas i klartext. I mobiltelefoni används också kryptering i stor utsträckning.

Många företag skyddar idag sin datakommunikation med hjälp av kryptografiska metoder. Företag kan också kräva att data som lagras på hårddisk krypteras, åtminstone på bärbara PC som används utanför den skyddade företagsmiljön.

Ett flertal metoder för kryptering och digitala signaturer används i kommersiella sammanhang. En del av dessa har tagits fram inom universitetsvärlden, vissa av privata företag och andra av, eller i samarbete med, samma myndigheter som bistår totalförsvaret. En del stora företag har särskilda avdelningar inom företaget för framtagning av krypto. Standardisering av kommersiellt framtagna system är en viktig del av arbetet för att de skall få stor spridning. I denna verksamhet deltar ett flertal olika aktörer.

3.3 Internationellt

Historiskt sett har Sverige endast i begränsad omfattning deltagit i olika internationella signalskydds- och informationssäkerhetssamarbeten. Det viktigaste skälet för detta har varit att signalskyddsarbetet i de mest framträdande länderna har varit förbehållet Nato-kretsen. Sedan ett antal år tillbaka deltar Sverige dock mer aktivt i olika internationella samarbeten där signalskydd finns med som en viktig komponent i det övergripande informationssäkerhetsarbetet.

Det finns idag ingen organisation formellt utpekad som ”National Communications Security Authority” (NCSA), det vill säga den organisation i landet som ansvarar för

signalskyddsfrågor, eller ”National Distribution Authority” (NDA), den organisation som är behörig att distribuera kryptonycklar. Försvarsmakten har anhållit om att få dessa roller. I avvaktan på beslut anser Försvarsmakten att de i praktiken fingerar som NCSA och NDA. Man menar att det idag inte finns någon annan organisation som har tillräcklig, adekvat kompetens för att komma i fråga. Funktionerna får allt större relevans i takt med att Sverige ökar sitt internationella samarbete och det anses därför viktigt att formellt klargöra den nationella rollfördelningen.

4 Behov av signalskydd idag och i framtiden

4.1 Allmänt

Signalskydd och kryptografiska funktioner används i allt större omfattning i samhället. Det finns en stor vilja och ett stort behov av att skydda information från obehörig insyn och påverkan. Det är viktigt att tillse att signalskyddet är organiserat på ett sådant sätt att samhällets behov av stöd inom området tillgodoses i enlighet med olika verksamheters varierade behov av skyddsnivåer.

4.2 Totalförsvarsbegreppets inverkan

Som framgått av beskrivningen av dagens verksamhet, har signalskyddet i stor utsträckning varit en verksamhet inom ramen för totalförsvaret.

Av lagen (1992:1403) om totalförsvar och höjd beredskap framgår att: ”Totalförsvar är verksamhet som behövs för att förbereda Sverige för krig. För att stärka landets försvarsförmåga kan beredskapen höjas. Höjd beredskap är antingen skärpt beredskap eller högsta beredskap. Under högsta beredskap är totalförsvar all samhällsverksamhet som då skall bedrivas”.

Enligt 1992 års försvarsbeslut utgjordes totalförsvaret av en militär och en civil del. Medan Försvarsmaktens främsta uppgift var att möta väpnat angrepp, ”varifrån det än kommer” var den civila delen av totalförsvarets uppgifter: ”att värna civilbefolkningen mot verkningarna av krigshandlingar och under kriser och i krig trygga en livsnödvändig försörjning; att under kriser och i krig stödja Försvarsmakten; samt att, för fullföljandet av dessa uppgifter, under kriser och i krig upprätthålla de viktigaste samhällsfunktionerna”.

I 1996 års försvarsbeslut slogs fast att ett vidgat säkerhetsbegrepp, som rymmer icke-militära hot och risker vid sidan av väpnade anfall, skulle styra totalförsvarets uppgifter och att en helhetssyn måste prägla synen på det militära och civila försvarets uppgifter i krig och fred. Totalförsvaret betraktades som ett uttryck för att försvaret av grundläggande samhällsvärden är en nationell angelägenhet som förutsätter hela samhällets stöd och insatser. Vidare angavs att totalförsvarets resurser också skulle utformas för att kunna användas vid internationella fredsfrämjande och humanitära insatser samt för att kunna stärka samhällets förmåga att förebygga och hantera svåra nationella påfrestningar i fred.

Däremot gjordes ingen förändring i själva definitionen av begreppet totalförsvar eller rörande kopplingen av begreppet till yttre hot och krigsförhållanden. Den organisatoriska, administrativa och legala uppdelningen mellan hot i fred och hot i krig, och principerna för finansiering av beredskapsåtgärder, kvarstod i allt väsentligt.

Insikten om att samhällets säkerhet och den vidgade hotbilden krävde en än mer genomgripande förändring ledde fram till att Sårbarhets- och säkerhetsutredningen (SOU 2001:41) tillsattes i juni 1999. Uppdraget var att utveckla formerna för att på ett effektivt sätt kunna möta ett bredare spektrum av hot och risker.

De förslag som Sårbarhets- och säkerhetsutredningen presenterade innebar ett nytt nationellt krishanteringssystem där alla typer av hot inom ramen för ett vidgat säkerhetsbegrepp skulle ingå. Begreppet totalförsvar skulle finnas kvar men ingå som en del i det övergripande systemet.

Regeringen tog fasta på många av Sårbarhets- och säkerhetsutredningens förslag i den proposition, Samhällets säkerhet och beredskap (2001/02:158), som överlämnades till riksdagen i mars 2002. Regeringens proposition, och riksdagens beslut med anledning av propositionen, innebär att totalförsvarskonceptet anses vara för snävt och ett hinder för en effektiv samhällsberedskap mot olika typer av hot och risker. Totalförsvarsbegreppet lever kvar, men som en del i ett större sammanhang. Sammantaget finns därför all anledning att även för signalskyddets del betrakta begreppet totalförsvar som ett kriterium bland flera.

I enlighet med statsmakternas beslut bör behoven av signalskydd därmed värderas utifrån ett bredare perspektiv, där såväl totalförsvarsaspekter som så kallade svåra påfrestningar på samhället i fred och de risker som är förknippade med den ordinarie verksamheten måste beaktas. Kraven på en tillräcklig signalskyddsförmåga bör ses som ett ansvar som varje myndighet eller organisation måste beakta i sin ordinarie verksamhet.

4.3 Nationellt

Dagens organisation för att leda signalskyddsverksamheten inom den statliga sektorn hålls samman i en organisation. Utgångspunkt för denna är totalförsvarets behov vilka framgår av avsnittet ovan. Verksamheten leds av Försvarsmakten, där Krigsförbandsledningen (KRI) har det generella ansvaret för

prioritering av utveckling och anskaffning samt medel för detta. TSA deltar i prioriteringen avseende totalförsvarsgemensam utveckling. Vid funktionsspecifik utveckling, till exempel för en specifik myndighets räkning, är det i regel den aktuella myndigheten som leder och ansvarar för arbetet. Rätten att bestämma om användning av de medel som tilldelas för utveckling av totalförsvarsgemensam signalskyddsmateriel tillkommer sålunda idag inte enbart signalskyddstjänstens ledning utan är ett ansvar för myndigheten Försvarsmakten. Vid överväganden om Försvarsmaktens budget sker inte något samråd med civila myndigheter när det gäller utvecklingen av totalförsvarsgemensam signalskyddsmateriel. Det kan därmed anses föreligga en risk för att civila behov inte tillgodoses i tillräcklig omfattning.

Försvarsmakten är idag den största kravställaren och kunden av system där signalskydd ingår. Utöver Försvarsmakten kommer även Regeringskansliet (RK), Rikspolisstyrelsen (RPS), KBM, med flera, även fortsättningsvis att behöva avancerade signalskyddslösningar.

I takt med att myndigheter och företag i allt större utsträckning digitaliserar sina arbetsprocesser och därmed sin information, har behovet av att skydda även sådan information som inte är totalförsvarsanknuten ökat på senare år. Behovet av skydd av sådan information ligger dock i regel inte på samma höga nivå som traditionellt har varit fallet för försvarsanknuten verksamhet. Exempel på samhällsviktiga system som främst bedöms ha behov av att utöka skyddet av sin information med hjälp av signalskydd är samhällsviktig infrastruktur, till exempel telekommunikation, el- och vattenförsörjning, sjukvård, rättsväsendet samt offentliga finans- och uppbördssystem.

Det ingår inte i nuvarande signalskyddsorganisations uppgifter att utveckla signalskyddssystem för de behov av signalskydd som ligger utanför totalförsvarets behov.

En växande infrastruktur av datanätverk, såsom Internet, LAN (Local Area Network) och WAN (Wide Area Network), en allt större användning av IT-baserade informationssystem har bidragit till att många länder har anpassat sin signalspaningsförmåga för att även kunna inhämta underrättelser ur dessa. Omfattande satsningar sker också i omvärlden för att kunna öka tillgången till signalspaningsinformation via den nya informationstekniken. Detta ställer följaktligen nya krav på signalskyddet. För att signalskyddsåtgärder i dagens komplexa system skall ge avsedd skyddseffekt måste de oftast kompletteras med övriga IT-säkerhetsåtgärder.

4.4 EU

Samarbetet inom EU syftar till att uppnå kvalificerad informationssäkerhet för alla medlemsstater. Det ankommer på Sverige, liksom på andra länder, att aktivt bidraga till att säkra EU:s informationssystem. Generellt följer Sverige utvecklingen inom EU avseende informationssäkerhet. En övergripande målsättning för Sverige bör vara att bidraga till att finna praktiska lösningar för hur man kan garantera säkra kommunikationer inom EU:s institutioner samt mellan dessa och medlemsländerna, inklusive säkra datorsystem.

4.5 Internationellt

Utredningen har av tidsskäl inte genomfört någon tillräckligt omfattande studie av internationell verksamhet eller initiativ inom signalskyddsområdet i andra länder för att kunna beskriva nuläge och framtida behov på ett heltäckande sätt. Frågan om hur man internationellt har löst frågor kring signalskydd, och i ett bredare perspektiv informationssäkerheten, blir en uppgift för nästa fas i utredningsarbetet.

Det kan dock konstateras att den förändrade omvärldssituationen och kanske främst internationaliseringen, innebär för signalskyddstjänsten att de svenska system som idag utvecklas även skall kunna användas utanför landets gränser. Svenska militära förband tilldelas system för säkert informationsutbyte med militära förband från andra stater. Arbetet med att producera och hantera kryptonycklar kräver säkra rutiner och personal med mycket högt säkerhetstänkande. Inom Nato finns mycket strikta rutiner som blivit normgivande för Nato-ländernas regelverk. För Sveriges internationella samverkan ställs, bland annat av förtroendeskäl, krav på att hålla en minst lika hög nivå. Informationsägare och ansvariga för de system som används måste känna ett orubbligt förtroende för verksamheten och för dess personal. Det måste i Sverige finnas en betrodd part med uppgift att administrera kryptomateriel och -nycklar för våra nationella system samt för de system från andra stater som används inom landet.

Idag finns stora, och växande, behov av skyddade förbindelser med utlandet, såväl bi- som multilateralt. Det kan gälla skydd av information om såväl politiska frågor (till exempel EU, Nato, FN), som frågor relaterade till bekämpning av organiserad, gränsöverskridande brottslighet men också behov föranledda av företagens internationalisering. Det ställs krav på internationell kompatibilitet, vilket kräver ett ökat samarbete med utlandet för att utveckla lösningar. Det kräver också ökade insatser för att ta fram system som inte till andra släpper signalskyddshemligheter

av betydelse för vår egen säkerhet. Bedömningar av kryptografiska funktioner och signalskyddssystem blir allt viktigare. Vi måste hålla en hög kompetensnivå för att kunna samarbeta med de mest kvalificerade europeiska länderna.

När det gäller internationellt samarbete inom signalskydds- och informationssäkerhetsområdet måste man beakta att de flesta länder inte samarbetar på ett djupare plan då man riskerar att blotta svagheter i de egna systemen. Detta hindrar dock inte att det finns en hel del frågor som det är okontroversiellt att samarbeta kring, till exempel CERT-funktioner, elektroniska signaturer, utbyte av rutiner, med mera. Inom mindre grupperingar och bilaterala samarbeten finns det en mängd olika frågeställningar med vilka Sverige nu och i framtiden kan arbeta gemensamt med andra länder.

5 Säkerhetsskydd

5.1 Nya behov

De signalskyddssystem som idag används är framtagna för att garantera skydd av uppgifter i upp till 50 år. En övervägande del av de uppgifter som idag behöver ges ett skydd har ett skyddsvärde under betydligt kortare tid. I många fall rör det sig om dagar, ibland upp till några år. I den verksamhet som bedrivs i samhället idag finns det enbart behov av att skydda uppgifter på den högsta säkerhetsnivån i en liten del av verksamheten. Detta bör beaktas vid utveckling av nya system. Det är sannolikt mer kostnadseffektivt att använda lägre skyddsnivåer som komplement till dagens system som är framtagna för att skydda uppgifter som är hemliga med hänsyn till rikets säkerhet.

Om signalskyddsbegreppet utökas till att gälla även annan känslig och skyddsvärd information som inte med nödvändighet omfattas av sekretess, vidgas kretsen av användare. Det finns i Sverige ett stort behov av att kunna kommunicera skyddsvärd information inom och mellan myndigheter, kommuner, landsting och andra offentliga organ. Landets kommuner, till exempel, hanterar känslig information som berör viktiga frågor för samhället, såsom vattenförsörjning, avloppshantering och lokal elkraftförsörjning. Uppgifter om svagheter i dessa system samt konsekvenser av bortfall av systemen framkommer i sårbarhetsutredningar som kommunen sedan vidarerapporterar.

Uppgifter av denna typ bör skyddas från obehörig insyn och påverkan vid lagring och vid kommunikation. Skyddet bör ligga på den nivå som erfordras för den aktuella uppgiften.

I takt med att Sverige ökar sitt internationella samarbete uppfattas diskrepansen mellan svenska och internationella skyddsnivåer som alltmer problematisk. Erfarenheter av Sveriges internationella samarbeten har visat på ett behov av fungerande rutiner. När det gäller kommunikation mellan Sverige och EU:s institutioner och av EU-information inom Sverige, finns det dessutom en rättslig förpliktelse av att kunna överföra och hantera denna på ett trovärdigt och tillförlitligt sätt. Överföringen och hanteringen måste ske i enlighet med ministerrådets säkerhetsbestämmelser (2001/264/EGT, EGT L 101/1 11.5.2001). Rådets säkerhetsbestämmelser, som medlemsstaterna således är skyldiga att följa, kräver av medlemsstaterna att lämpliga åtgärder vidtas för hantering av sekretessbelagda EU-uppgifter. EU graderar sina uppgifter i fyra sekretessgrader: TRÈS SECRET UE, SECRET UE, CONFIDENTIEL UE och RESTREINT UE. Graderna motsvarar det som i andra internationella sammanhang benämns TOP SECRET, SECRET, CONFIDENTIAL och RESTRICTED.

5.1.1 Signalskydd – en del av säkerhetsskyddet

Signalskyddsverksamheten inriktas idag nästan uteslutande mot skydd av uppgifter som är hemliga med hänsyn till rikets säkerhet. Detta är bland annat en konsekvens av att de svenska säkerhetsskyddsbestämmelserna i princip endast tar sikte på sådana uppgifter som omfattas av sekretess och som rör rikets säkerhet. Se närmare härom i säkerhetsskyddslagen (1996:627) med tillhörande förordning samt verkställighetsföreskrifter utfärdade av Försvarsmakten respektive Rikspolisstyrelsen. I många samhällsviktiga informations- och ledningsstödssystem hanteras dock uppgifter som är känsliga och skyddsvärda, men

som inte kan anses omfattas av bestämmelserna om säkerhetsskydd. För sådana känsliga och skyddsvärda uppgifter finns det idag inte några krav på hur skyddet skall utformas. Detta kan medföra att uppgifter som i sig måste anses känsliga eller skyddsvärda ges ett bristfälligt skydd, vilket kan få allvarliga konsekvenser för verksamheten och i förlängningen för viktiga funktioner i samhället.

5.1.2 Närmare om säkerhetsskyddslagen m.m.

Bestämmelser om skydd för hemlig information finns således i säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). Lagens och förordningens tillämpningsområden är verksamhet hos staten, kommunerna och landstingen samt för aktiebolag, handelsbolag, föreningar och stiftelser över vilka staten, kommuner eller landsting utövar ett rättsligt bestämmande inflytande. Därutöver gäller lagen också för enskilda om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism.

Med säkerhetsskydd avses skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet, skydd i andra fall av uppgifter som omfattas av sekretess enligt sekretesslagen och som rör rikets säkerhet samt skydd mot terrorism (6 §). Säkerhetsskyddet skall bland annat förebygga att uppgifter som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (informationssäkerhet). I förordningen och tillämpningsföreskrifterna avses med ”hemlig uppgift” följaktligen bara sådana uppgifter som omfattas av sekretesslagen och som samtidigt rör rikets säkerhet. Säkerhetsskyddslagen gäller således bara en mindre del av alla uppgifter som omfattas av sekretess (är hemliga) enligt sekretesslagen och den gäller inte heller för uppgifter som är skyddsvärda av andra skäl än till följd av sekretess enligt sekretesslagen.

Av 39–47 §§ säkerhetsskyddsförordningen framgår vilka myndigheter som har ett tillsynsansvar enligt lagen respektive rätt att meddela föreskrifter om verkställigheten av densamma. Säkerhetsskyddet skall kontrolleras av Försvarsmakten när det gäller Fortifikationsverket samt de myndigheter som hör till Försvarsdepartementet utom Kustbevakningen, Krisberedskapsmyndigheten, Statens Räddningsverk och Styrelsen för Psykologiskt försvar, samt Rikspolisstyrelsen när det gäller Kustbevakningen, Krisberedskapsmyndigheten, Statens Räddningsverk, Styrelsen för Psykologiskt försvar och övriga myndigheter utom Justitiekanslern.

Sammantaget kan man förledas att tro att säkerhetsskyddssystemet tillförsäkrar samhället ett fullgott skydd. Den praktiska erfarenheten sägs visa att så inte är fallet. Många av de brister och fel som identifieras i samhällsviktiga system kan utnyttjas inte bara för att hota sådana intressen som säkerhetsskyddsbestämmelserna tar sikte på. Bristerna kan till exempel också utnyttjas för att begå brottsliga gärningar av olika slag. Som ett praktiskt exempel kan nämnas bristen på skydd för elektroniska transfereringssystem. Samtliga större myndigheter sköter till exempel idag sina in- och utbetalningar helt på elektronisk väg.

Ett centralt konstaterande baserat på ovanstående resonemang är att säkerhetsskyddslagen och säkerhetsskyddsförordningen endast reglerar det som är hemligt med hänsyn till rikets säkerhet. Ett växande behov finns dock avseende skydd av annan information, det vill säga sådan som inte omfattas av de nuvarande bestämmelserna och rutinerna för informationssäkerhetsskydd. Det är utredningens uppfattning att den kompetens och de rutiner som utvecklats inom signalskyddsverksamheten bör kunna komma samhället till godo i större utsträckning än vad dagens bestämmelser ger utrymme för. En tänkbar lösning är att utvidga säkerhetsskyddslagens tillämpningsområde till att inte bara omfatta det som är hemligt

med hänsyn till rikets säkerhet. En annan modell kan vara att regeringen föreskriver hanteringsrutiner för skyddsvärd information hos statliga myndigheter I båda fallen måste dock noggrant övervägas vad som skall inrymmas i begreppet ”skyddsvärd information”.

6 Signalskydd och informationssäkerhet

Traditionellt har IT-säkerhet och signalskyddsverksamhet konceptuellt hanterats som två parallella verksamheter. Tidigare utgjordes kryptofunktionen av en separat kryptoapparat som krypterade informationen innan den nådde mottagaren. Idag är kryptofunktionen ofta integrerad i en komplett systemlösning som hanterar informationen och denna överförs krypterad utan mellansteg. De kryptografiska funktionerna blir genom teknisk utveckling en allt mer integrerad del av systemutveckling och därmed av säkerheten i informationssystem. Krypto utgör inte längre enbart en garant för kommunikationssäkerhet utan är en del av den sammantagna informationssäkerheten. Det anses därför att kryptologisk kompetens måste finnas med vid utvecklandet av IT-säkerhetslösningar. Det är av vikt att utvecklingen av kryptografiska funktioner sker så nära utvecklingen av övrigt informationsskydd som möjligt. I takt med att informationssäkerhet och signalskydd på detta sätt integreras i allt större utsträckning, bör möjligheterna att sammanföra dessa i en gemensam funktion eller att på annat sätt samordna verksamheten, övervägas. En tanke som har förts fram är att föreskriftsrätt för samtliga myndigheter, samt i vissa fall även för samhällsviktiga företag, i sammanhanget bör övervägas.

De tekniska aspekterna är i sammanhanget viktiga att beakta, eftersom de utgör själva grunden till problematiken, men andra komponenter, såsom utbildning, information och regelverk får inte glömmas bort. Exempelvis är kunskap att korrekt implementera en kryptografisk funktion i mjukvaran i en

systemlösning avgörande för skyddet. En kryptografisk funktion som till exempel är godkänd för Windows NT kan inte utan vidare användas i Windows XP utan att ny granskning måste genomföras och nytt godkännande ges.

7 Utredningens överväganden

Utredningen har i sitt arbete konstaterat att signalskydd är en integrerad del av informationssäkerheten. Den tekniska utvecklingen inom detta område bidrar också till att integrera kryptografiska funktioner i informationssäkerhetsprodukter. Som konstateras i rapporten var signalskyddstjänst tidigare en egen disciplin som hanterades i stor utsträckning skilt från kommunikationen av informationen. Idag är signalskyddet integrerat i IT- och kommunikationsutrustningen. Utredningen anser av detta skäl att det inte är lämpligt att lägga några förslag inom signalskyddsområdet innan övriga delar av informationssäkerhetsområdet har belysts. I det fortsatta arbetet kommer utredningen att väga in signalskyddsfrågorna som en del av informationssäkerhetsområdet.

Utredningen har i sitt arbete konstaterat att det finns ett behov av signalskydd även utanför det som lagstiftningsmässigt definieras som totalförsvaret. De resurser och den kompetens som genom anslag finansieras inom ramen för totalförsvaret skulle kunna användas även i andra samhällsverksamheter. Så görs i vissa fall redan idag. Detta skall vägas mot möjligheterna att tillgodose behoven med kommersiellt tillgängliga system (COTS). Aktuella områden skulle kunna vara såväl statlig verksamhet utanför totalförsvaret som privat sektor med kommersiella behov. Utredningen utgår fortsättningsvis från att det finns ett behov och intresse av samarbete mellan den verksamhet som bedrivs inom totalförsvaret och den inom privat eller kommersiell verksamhet, som motiverar vidare utredning av

samverkansmöjligheter. Det finns därmed också ett behov av att se över gränsdragningar i lagstiftningen, ansvarsförhållanden, organisation, etc.

Utredningen utgår ifrån att en svensk anpassning till internationella normer, vad avser signalskydd och hantering av skyddsvärd information, är eftersträvansvärd. Utredningen har identifierat några handlingsalternativ under avsnitt 4. Genom dessa skulle man även kunna omhänderta frågan om anpassning till internationella normer. En framkomlig väg synes t.ex. vara att utvidga säkerhetsskyddslagens tillämpningsområde till att omfatta även annan skyddsvärd information än den som är hemlig med hänsyn till rikets säkerhet. I det sammanhanget skulle skyddsvärd information t.ex. kunna definieras såsom av EU eller annan internationell organisation angiven skyddsvärd information. Därutöver skulle till exempel annan skyddsvärd information i samhällsviktig verksamhet kunna omfattas. Med en sådan ordning skulle en större krets av de organ som hanterar skyddsvärd information kunna omfattas av tillämpningsföreskrifter eftersom lagens tillämpningsområde även omfattar kommuner, landsting och vissa andra enskilda rättssubjekt. Ett mindre långtgående alternativ kan vara att regeringen föreskriver att särskilda signalskyddsrutiner med mera, skall tillämpas hos de statliga myndigheterna. Inom ramen för denna första delrapport har det dock inte varit möjligt att närmare analysera frågeställningen. Utredningen är också medveten om att frågan för närvarande bereds inom Regeringskansliet. Eftersom det är angelägna frågor har dock utredningen känt sig förpliktad att särskilt belysa dem och lyfta fram dem, till det gagn det må ha för den fortsatta beredningen.

Akronymlista

CERT	Computer Emergency Response Team
CIV	Enheten för det civila försvaret (Fö)
COTS	Commercial off-the-shelf
EU	Europeiska Unionen
EPS	Enheten för ekonomi, personal och samordning
FHS	Försvarshögskolan
FMV	Försvarets materielverk
FN	Förenta Nationerna
FOI	Totalförsvarets forskningsinstitut
FortV	Fortifikationsverket
FRA	Försvarets radioanstalt
Fö	Försvarsdepartementet
HKV	Högkvarteret
IT	Informationsteknik
ITSA	Informationssäkerhetsavdelningen
JAS	Jakt Attack Spaning
KBM	Krisberedskapsmyndigheten
KBV	Kustbevakningen
KRI	Krigsförbandsledningen
LAN	Local Area Network
MUST	Militära underrättelse- och säkerhetstjänsten
NATO	North Atlantic Treaty Organisation
NCSA	National Communications Security Authority
NDA	National Distribution Authority
NSD	Näringslivets säkerhetsdelegation
OECD	Organisation on Economic Cooperation and Development
PC	Personal computer
RK	Regeringskansliet
RPS	Rikspolisstyrelsen
SN	Statens Signalskyddsnämnd
SNS	Statens Signalskyddsnämnds skola
SOU	Statens offentliga utredningar
StabSbS	Stabs- och sambandsskolan
SÄPO	Säkerhetspolisen
TAK	Totalförsvarets aktiva kort
TSA	Totalförsvarets signalskyddsavdelning
TSS	Totalförsvarets signalskyddsskola
WAN	Wide Area Network

Kommittédirektiv
Dir. 2002:103

Angående vissa frågor om informationssäkerheten i samhället

Beslut vid regeringssammanträde den 11 juli 2002.

Sammanfattning av uppdraget

En utredare skall lämna förslag på hur signalskyddsverksamheten i samhället skall utformas. I uppdraget ingår att bedöma behovet av signalskydd i samhällsviktig verksamhet samt att lämna förslag till organisatorisk placering, lokalisering, uppgifter, ledning och samordning av signalskyddstjänsten.

Den särskilda utredaren kommer också att få i uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas och till hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet bör utformas i framtiden. Utredaren planeras också få uppdraget att genomföra den utvärdering som regeringen aviserat i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158).

Regeringen avser att återkomma under hösten med tilläggsdirektiv när det gäller dessa uppdrag.

Inledning

I takt med att samhället har blivit allt mer beroende av olika informationssystem har vikten av att förbereda sig för hot av olika slag ökat. Regeringen har närmare beskrivit hotbilden för attacker via informationssystem i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 104 f). Där konstateras att en av svårigheterna med hanteringen av de IT relaterade hoten är att urskilja vem aktören är, eftersom ingen absolut åtskillnad mellan olika typer av aktörer kan göras. Detta faktum gör att det är särskilt svårt att skydda sig eftersom säkerhetsåtgärderna måste anpassas till samtliga typer av aktörer. Ytterligare en försvårande faktor är att de IT-relaterade hoten är geografiskt gränslösa. Den som vill göra intrång i eller på annat sätt manipulera ett informationssystem i Sverige kan befinna sig var som helst i världen.

Signalskyddsverksamheten

Att skydda information som utväxlas i form av meddelanden och trafik eller information som lagras elektroniskt får allt större betydelse i dagens samhälle. Det gäller inte bara för sådan information som omfattas av bestämmelserna om sekretess i sekretesslagen (1980:100), utan också för andra uppgifter som hanteras i informationssystem av olika slag i samhället. Exempel på sådan skyddsvärd information kan vara uppgifter som gäller känslig infrastruktur, ekonomi och personlig integritet.

Utvecklingen av dagens signalskyddssystem sker till största delen inom Försvarsmakten utifrån de krav som behovet av att kunna hantera information som omfattas av sekretess till skydd för rikets säkerhet ställer. Utvecklingen av IT-säkerhetslösningar

i samhället i övrigt styrs allt mer av behovet av att skydda information som inte omfattas av sekretess till skydd för rikets säkerhet. En utveckling av signalskyddstjänsten till att även kunna hantera andra kryptografiska skyddsbehov än de som utvecklas för totalförsvarsändamål och en bedömning av hela samhällets skyddsförmåga är därför påkallad.

Signalskyddstjänsten leds idag av en funktion inom Försvarsmakten (MUST/TSA). Att signalskyddstjänstens ledning organisatoriskt har denna placering kan innebära en risk för att de civila behoven inte prioriteras tillräckligt. Frågan om var signalskyddstjänsten på nationell nivå skall organiseras och lokaliseras bör därför övervägas.

I propositionen Ett informationssamhälle för alla (prop. 1999/2000:86) angav regeringen att den välkomnar en bred användning av kryptografi. Mot denna bakgrund bör det eventuellt finnas en rådgivande funktion i kryptografifrågor i Sverige. Därför finns behov av att undersöka i vad mån signalskyddstjänsten kan utgöra ett sådant rådgivande organ i samhället.

Det ökade samarbetet med andra stater och internationella organisationer medför vidare ett ökat statligt behov av att kunna hantera signalskyddsutrustning och kryptonycklar även i internationella sammanhang. Det bör övervägas om signalskyddstjänsten kan bistå i den utvecklingen.

Arbetet med informationssäkerhet inom offentlig sektor

Regeringen har i propositionerna Fortsatt förnyelse av totalförsvaret (prop. 2001/02:10, bet. 2001/02:FöU02, rskr. 2001/02:91) och Samhällets säkerhet och beredskap (prop. 2001/02:158, bet. 2001/02:FöU10, rskr 2001/02:261) redovisat sin strategi och förslag till åtgärder för att stärka informationssäkerheten i samhället och skyddet av de samhällsviktiga systemen. I propositionen Samhällets säkerhet och beredskap vidgades åtgärderna från att endast omfatta IT-

säkerhet till att täcka hela informationssäkerhetsområdet. Det tidigare använda mer oprecisa begreppet "informationsoperationer" utmönstrades därmed ur terminologin.

Regeringen har angett att målet bör vara att man skall upprätthålla en så hög informationssäkerhet i hela samhället att störningar i samhällsviktig verksamhet kan förhindras eller hanteras. Strategin för att uppnå detta mål liksom för övrig krishantering i samhället utgår från ansvarsprincipen, likhetsprincipen och närhetsprincipen.

Som ett första steg i en samlad strategi i informationssäkerhetsarbetet har fyra myndigheter fr.o.m. andra halvåret 2002 fått nya uppgifter. Dessa myndigheter är Krisberedskapsmyndigheten, Post- och telestyrelsen, Försvarets radioanstalt och Försvarets materielverk.

Detta första steg skall utvärderas efter två år som regeringen förutskickat i propositionen Samhällets säkerhet och beredskap.

Med anledning av att det finns många företag som är verksamma inom informationssäkerhetsområdet finns det dock skäl att ytterligare överväga vilken verksamhet staten skall bedriva inom detta område. Härvid skall beaktas att konkurrensen på den öppna marknaden inte får påverkas negativt.

Regeringen finner att de bästa förutsättningarna för ett gott beslutsunderlag kan skapas genom att utvecklingen inom informationssäkerhetsområdet följs.

Internationell verksamhet

Genom att hoten mot informationssystemen inte bara är en svensk angelägenhet, utan är av global natur, krävs internationell samverkan. Sådan samverkan bedrivs på flera olika områden, bl.a. inom EU. Olika myndigheter medverkar vidare i internationell samverkan som i regel har informationsutbyte som syfte. För att Sverige skall få genomslag i sitt agerande på den internationella

arenan bör det finnas en övergripande inriktning. Inriktningen bör också knyta an till och vara anpassad till respektive myndighets ansvarsområde.

Uppdraget

Den särskilda utredaren skall bedöma behovet av signalskydd i samhällsviktig verksamhet och lämna förslag på hur signalskyddsverksamheten i samhället skall utformas. Utredaren skall mot bakgrund av utvecklingen inom informationssäkerhetsområdet föreslå hur signalskyddstjänsten i Sverige skall vara organiserad. Utredaren skall också belysa hur signalskyddsutbildningen skall organiseras och var den skall lokaliseras.

Följande frågor bör besvaras.

- Hur bör signalskyddsverksamheten utvecklas så att den kan komma till nytta inom fler samhällssektorer?

- Vilka samhällssektorer har störst behov av signalskydd och vilka krav ställer de?

- Vem skall vara ansvarig för signalskyddet och hur skall detta vara organiserat?

- Vilka uppgifter skall signalskyddstjänsten ha och hur skall ledning och samordning ske?

- Hur säkerställs att det framtida behovet av kompetens inom det kryptografiska området kan tillgodoses?

- Hur säkerställs samordning med andra länders signalskyddsorganisationer på ett förtroendefullt och säkerhetsmässigt trovärdigt sätt?

- Hur åstadkoms en nationell distributionsfunktion för signalskyddsmateriel och signalskyddsnycklar för det internationella samarbetet?

Utredaren kommer att få i uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas och hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet skall utformas i framtiden. I detta arbete skall gränsdragningsfrågor särskilt beaktas gentemot den översyn av de rättsliga aspekterna, inklusive de internationella, på området för informationssäkerhet som Justitiedepartementet avser att genomföra (jfr. prop. 2001/2002:158).

Utredaren planeras också få uppdraget att genomföra den ovan nämnda utvärderingen.

Direktiv angående dessa två senare uppdrag avser regeringen att återkomma med under hösten 2002 som tilläggsdirektiv.

Samråd och avrapportering

Utredaren skall bedriva arbetet i nära samarbete med Försvarsmakten, Försvarets radioanstalt, Rikspolisstyrelsen och Krisberedskapsmyndigheten.

Inom Regeringskansliet finns en informell grupp bestående av representanter från Justitiedepartementet, Utrikesdepartementet, Försvarsdepartementet och Näringsdepartementet som utbyter information i dessa frågor. Denna grupp bör utredaren använda som referensgrupp i arbetet. Även andra kontakter bör tas.

Utredaren skall lämna delrapport om signalskyddstjänsten senast den 28 februari 2003.

Utredaren skall lämna slutrapport senast den 6 maj 2005.

(Försvarsdepartementet)

Tilläggsdirektiv

Kommittédirektiv
Dir.
2003:29

Tilläggsdirektiv till utredningen angående vissa frågor om informationssäkerheten i samhället (Fö 2002:06)

Beslut vid regeringssammanträde den 20 februari 2003

Sammanfattning av uppdraget

Utredningen angående vissa frågor om informationssäkerheten i samhället skall lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas samt hur Sveriges engagemang i det internationella arbetet inom informations säkerhetsområdet skall utformas. I propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 105) anmälde regeringen sin avsikt att göra en utvärdering av de bedömningar som regeringen gjorde inom informationssäkerhetsområdet. Utredaren skall följa myndigheternas uppbyggnad av den informationssäkerhetsverksamhet som regeringen har givit

myndigheterna i uppgift enligt propositionen. Utredaren skall vidare lämna förslag till hur OECD:s riktlinjer om nät- och informationssäkerhet kan genomföras.

Bakgrund

Med stöd av regeringens bemyndigande den 11 juli 2002 (dir. 2002:103) tillkallade chefen för Försvarsdepartementet en särskild utredare med uppdrag att föreslå hur signalskyddsverksamheten i samhället skall utformas. Utredaren skall enligt direktiven lämna en delrapport avseende detta uppdrag den 28 februari 2003. Regeringen angav i direktiven att den avsåg att återkomma med tilläggsdirektiv angående uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas och till hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet bör utformas i framtiden.

OECD (Organisation for Economic Co-operation and Development) antog den 25 juli 2002 en rekommendation om nya riktlinjer för nät- och informationssäkerhet (OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security). Riktlinjerna syftar till att stödja utvecklingen av en säkerhetskultur i samhället genom att främja säkerhetstänkande vid utveckling och användning av nät och informationssystem. Riktlinjerna innehåller mål och principer för utvecklingen av nya nät och informationssystem.

Uppdraget

En utvecklad svensk informationssäkerhetsstrategi

Utredaren skall i det fortsatta arbetet, utöver det tidigare lämnade uppdraget, även lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas. Den i

prop. 2001/02:158 s. 103 redovisade strategin för informationssäkerhetsarbetet skall utgöra grunden.

Utredaren skall göra jämförelser med hur andra länder har hanterat informationssäkerhetsfrågan när det gäller strategi, organisation och andra förhållanden som kan vara relevanta.

I sitt arbete skall utredaren beakta OECD:s riktlinjer för nät- och informationssäkerhet och lämna förslag till hur riktlinjerna kan genomföras i utredarens förslag.

Följande frågor skall besvaras.

- Hur bör den nationella strategin för informationssäkerhet vidareutvecklas?
- Hur säkerställs att den nationella strategin för informationssäkerhet möter de krav som ställs via det multinationella samarbete Sverige deltar i, främst EU?
- Utifrån en nationell strategi behöver den nuvarande samordningen av Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet förändras?
- Inom vilka delar av informationssäkerhetsområdet bör staten ha ett särskilt ansvar?
- Hur skall informationssäkerhetsarbetet finansieras?

Utvärdering förutskickad i prop. 2001/02:158

I propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 105) redovisade regeringen att de nya uppgifterna på informationssäkerhetsområdet skulle fördelas på de myndigheter som redan hade närliggande verksamhet. Regeringen anmälde också att man hade för avsikt att göra en utvärdering av denna fördelning av uppgifterna inom informationssäkerhetsområdet. Regeringen uteslöt inte att det skulle kunna finnas andra organisatoriska lösningar eller andra verksamheter inom informationssäkerhetsområdet som skulle kunna behövas ses över.

Som en förberedelse inför denna utvärdering skall utredaren skapa sig en god uppfattning av det ändamålsenliga i propositionens bedömningar att dela upp de nya uppgifterna

genom att följa uppbyggnaden av verksamheten inom informationssäkerhetsområdet vid Krisberedskapsmyndigheten, Försvarets radioanstalt, Förvarets materielverk och Post- och telestyrelsen, inklusive den sistnämnda myndighetens uppdrag att inrätta en rikscentral för IT-incidentrapportering. Regeringen avser att återkomma till frågan om utvärderingen.

Författningsfrågor

Om utredaren finner att det finns ett behov av att föreslå författningsändringar skall utredaren lämna lagtekniskt genomarbetade förslag vid varje rapporteringstillfälle.

I detta arbete skall gränsdragningsfrågor särskilt beaktas gentemot den översyn av de rättsliga aspekterna, inklusive de internationella, på området för informationssäkerhet som Justitiedepartementet avser att låta genomföra (jfr. prop. 2001/02:158 s. 106).

I den mån det uppkommer frågor som rör behandling av personuppgifter skall de bestämmelser om skydd för den personliga integriteten vid behandling av sådana uppgifter som bl.a. finns i personuppgiftslagen (1998:204) och EG-direktivet om personuppgifter (95/46/EG) beaktas.

Utredningsarbetet

I sitt arbete skall utredningen ta hänsyn till OECD:s riktlinjer för nät- och informationssäkerhet.

Utredningen skall bedriva arbetet i nära samarbete med Rikspolisstyrelsen, Säkerhetspolisen, Datainspektionen, Statskontoret, Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk, Krisberedskapsmyndigheten, Totalförsvarets forskningsinstitut och Post- och telestyrelsen. Utredningen skall också ta de kontakter som behövs med viktiga IT-användare och andra intressenter, både inom den offentliga

sektorn och i näringslivet, för att få en bild av vilka roller de spelar i informationssäkerhetsarbetet, deras behov och önskemål.

Utredningen skall utöver det som angavs i direktiven (2002:103) om att slutrapport skall lämnas senast 6 maj 2005 också lämna en delrapport angående uppdragen i detta tilläggsdirektiv senast den 1 mars 2004.

(Försvarsdepartementet)