Lokalisering av Sveriges IT-incidentcentrum (Sitic)

Delrapport från Informationssäkerhetsutredningen
FÖ 2009:04

Missiv

Till statsrådet och chefen för Försvarsdepartementet

Genom beslut den 19 november 2009 (dir. 2009:110) bemyndigade regeringen chefen för Försvarsdepartementet att tillkalla en särskild utredare med uppdrag att utreda formerna och konsekvenserna av att flytta ansvaret för dels Sveriges IT-incidentcentrum (Sitic) från Post- och telestyrelsen (PTS) dels Sveriges certifieringsorgan för IT-säkerhet (CSEC) från Försvarets materielverk (FMV). Utredaren ska undersöka vilken myndighet av Försvarets radioanstalt (FRA) och Myndigheten för samhällsskydd och beredskap (MSB) som bedöms bäst lämpad att vara ansvarig utifrån de behov och målsättningar som regeringen angett när det gäller bl.a. att samla informationssäkerhetsfrågorna.

Med stöd av regeringens bemyndigande kallade chefen för Försvarsdepartementet departementsrådet Jan Hyllander till

särskild utredare (regeringsbeslut 2009:04, protokoll Fö 2009:2455/EPS).

Ett beslut om tilläggsdirektiv fattades av regeringen den 14 januari 2010 om förlängd utredningstid som innebar att uppdraget ska slutredovisas den 1 april 2010 istället för den 22 januari 2010. Dock ska en delrapport om formerna och konsekvenserna av att flytta Sitic från PTS lämnas till regeringen den 1 februari 2010.

Departementssekreterarna Ingolf Berg och Linda Ericson har varit sakkunnig respektive expert i utredningen. Avdelningschef Magnus Hjort och analytiker Andreas Wedner (förordnad fr.o.m. den 7 december 2009, entledigad den 1 februari 2010) har varit sekreterare i utredningen.

Utredningen, som har tagit namnet Informationssäkerhetsutredningen överlämnar härmed delrapporten Lokalisering av Sveriges IT-incidentcentrum.

Stockholm 1 februari 2010

Jan Hyllander

/Magnus Hjort
Andreas Wedner

Innehåll

1 Sammanfattning

Regeringens uppdrag är att utreda formerna för och konsekvenserna av att flytta Sitic från PTS till antingen MSB eller FRA. Utredaren ska undersöka vilken av de två myndigheterna som bedöms bäst lämpad att vara ansvarig utifrån de behov och målsättningar som regeringen angett när det gäller bland annat att samla informationssäkerhetsfrågorna.

Utredaren föreslår att personalen och verksamheten vid Sitic inordnas i MSB. Formellt torde detta kunna ske den 1 januari 2011. De lokaler som är förberedda för Sitic då PTS under våren 2010 flyttar till Valhallavägen kan dock behöva disponeras under en övergångsperiod under 2011. Utredaren vill betona att denna övergångsperiod bör vara så kort som möjligt då de synergieffekter som redovisats kräver en samlokalisering med relevanta verksamheter vid MSB.

Utredaren föreslår vidare att PTS nuvarande uppgifter enligt 6 § i myndighetens instruktion gällande Sitics verksamhet i sin helhet överförs till MSB. I förordningen (2008:1002) med instruktion för MSB bör därför en motsvarande bestämmelse föras in samtidigt som nuvarande 6 § i PTS instruktionsförordning ska upphävas. Ändringen bör träda i kraft den 1 januari 2011.

Utredarens bedömning är att förslaget att inordna verksamheten vid Sitic i MSB skulle få positiva konsekvenser både för arbetet med informationssäkerhet samt för arbetet med samhällets krisberedskap i stort och alltså gagna både det arbete som Sitic och MSB utför idag. Genom att placera Sitic vid MSB åstadkoms en mer samlad lösning av ansvaret för informations-

säkerhet på central myndighetsnivå. Det skapas också möjligheter att bättre integrera informationssäkerhetsarbetet i arbetet med samhällets krisberedskap, t.ex. arbetet med risk- och sårbarhetsanalyser.

2 Inledning

2.1 Utredarens uppdrag

Regeringen beslutade den 19 november 2009 att tillsätta en utredning med uppgift att utreda formerna för och konsekvenserna av att flytta ansvaret för Sitic från PTS samt CSEC från FMV. Verksamheterna ska antingen inordnas i MSB eller FRA. Utredaren ska undersöka vilken av de två myndigheterna som bedöms bäst lämpad att vara ansvarig utifrån de behov och målsättningar som regeringen angett när det gäller bland annat att samla informationssäkerhetsfrågorna. Utredaren ska slutligen föreslå en myndighet som ska vara signatär för de internationella organen CCRA och SOGIS-MRA vilket bl.a. innebär att underteckna fördrag.

Ansvaret för informationssäkerhet på nationell nivå är uppdelat på ett flertal myndigheter, bl.a. MSB, PTS inkl. Sitic och FRA vilket innebär att ansvaret är splittrat. Detta betyder att styrningen och samordningen av arbetet försvåras och att resurser riskerar att inte nyttjas på ett optimalt sätt. Regeringen anser därför att ansvaret för informationssäkerhet bör samlas. Utredaren ska mot denna bakgrund:

- utreda och redovisa konsekvenserna av en överföring av Sitics verksamhet till MSB eller FRA,
- utreda och redovisa formerna för och konsekvenserna av en överföring av CSEC:s verksamhet till antingen MSB eller

FRA med beaktande av gällande regler kring teknisk kontroll och principen om kontrollordningar i öppna system,

- utreda och ange vilken av myndigheterna MSB eller FRA som är bäst lämpad att vara ansvarig för CSEC och Sitic,
- föreslå en myndighet som ska vara signatär för både CCRA och SOGIS-MRA,
- redovisa kostnader och intäkter för respektive verksamheter som skall flyttas och föreslå en lämplig finansiering,
- redovisa eventuella rationaliseringar som kan uppstå i samband med samordningen, varvid engångskostnader som t.ex. kan uppstå i samband med flyttning, anpassning av nya eller avveckling av befintliga lokaler ska anges särskilt,
- lämna förslag till författningsändringar till följd av utredningens förslag samt
- redovisa en tidsplan för ändrade ansvarsförhållanden och gemensam signatär.

Utredaren ska, utöver de verksamhetsmässiga och ekonomiska konsekvenserna även redovisa de personella konsekvenserna av sitt förslag. Utredaren ska kontinuerligt informera Regeringskansliet om arbetets bedrivande. Utredaren ska beakta bl.a. det fortsatta arbetet med anledning av Stödutredningens rapport Ett användbart och tillgängligt försvar - Stödet till Försvarsmakten (Fö 2009:A), det arbete som Delegationen för e-förvaltning (2009:19) genomför samt Infosäkutredningens delrapport och betänkanden (SOU 2004:32, 2005:42, 2005:71).

Ett beslut om tilläggsdirektiv fattades av regeringen den 14 januari 2010 (Fö 2009:04) om förlängd utredningstid som innebär att uppdraget ska slutredovisas den 1 april 2010. Dock ska en delrapport om formerna för och konsekvenserna av att flytta Sitic från PTS lämnas till regeringen den 1 februari 2010.

2.2 Arbetsform

Utredaren har tagit del av tidigare utredningar och propositioner, samt underlag från myndigheter. Vidare har samtal förts med företrädare för närmast berörda myndigheter samt med företrädare för Svenska bankföreningen, IT- & Telekomföretagen samt Svenskt näringsliv.

2.3 Tidigare utredningar

2.3.1 Sårbarhets- och säkerhetsutredningen

Sårbarhets- och säkerhetsutredningen (SOU 2001:41) tillsattes i syfte att lämna förslag till principer för att åstadkomma en förbättrad helhetssyn avseende planeringen för civilt försvar och beredskapen mot svåra påfrestningar på samhället i fred. Enligt utredningen var ansvaret för informationssäkerhet i Sverige splittrat och det saknades ett sammanhållande system för att hantera allvarliga IT-hot. Med utgångspunkt från bl.a. internationella erfarenheter föreslog utredningen att följande funktioner skulle inrättas:

- Ett tvärsektoriellt samordningsorgan för IT-säkerhet och skydd mot informationsoperationer med placering i Regeringskansliet,
- en funktion för IT-incidenthantering med PTS som chefsmyndighet,
- en funktion för teknikkompetens inom IT-säkerhet med FRA som chefsmyndighet,
- ett svenskt system för evaluering och certifiering med placering vid FMV.

Utredningen föreslog vidare att den tänkta planeringsmyndigheten (sedermera KBM) borde ges ett sammanhållande ansvar för samhällets IT-säkerhet och även kunna ha kapacitet att bedriva omvärldsanalys inom områdena IT-säkerhet och informationsoperationer.

2.3.2 Infosäkutredningen

Regeringen beslutade den 11 juli 2002 att utreda behovet av signalskydd i samhällsviktig verksamhet. Utredningen tog namnet Infosäkutredningen. Den 20 februari 2003 utökades uppdraget genom ett tilläggsdirektiv där utredningen bland annat fick i uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet borde utvecklas samt hur Sveriges engagemang i det internationella arbetet på informationssäkerhetsområdet skulle utformas.

En delrapport om signalskydd (SOU 2003:27) lämnades till regeringen den 28 februari 2003. Delrapporten Informationssäkerhet i Sverige och internationellt – en översikt, lämnades till regeringen den 1 april 2004 (SOU 2004:32). Ytterligare ett delbetänkande lämnades i maj 2005 (Säker information. Förslag till informationssäkerhetspolitik SOU 2005:42). Infosäkutredningens slutbetänkande överlämnades till regeringen i september 2005 (SOU 2005:71) med förslag på organisatoriska förändringar inom informationssäkerhetsområdet.

Infosäkutredningen konstaterade att rapporteringen av IT-incidenter till Sitic varit mer begränsad än vad som förväntats, bl.a. beroende på att verksamheten varit relativt okänd och att sekretessfrågan varit oklar.[1] Infosäkutredningen såg klara fördelar med att ge signalunderrättelsetjänsten en mer aktiv roll i bekämpandet av IT-relaterade hot genom dess unika möjlighet att kartlägga och identifiera illasinnade aktörer.

[1] SOU 2005:71, s.104.

Utredningen konstaterade att PTS/Sitic genomförde tekniska analyser vars resultat publicerades brett i syfte att kunna informera samhällets organisationer om nya problem som kunde störa IT-system. Rättsväsendet genomförde tekniska analyser i syfte att säkra bevis. FRA genomförde teknisk analys i syfte att kunna stödja individuella organisationers arbete med informationssäkerhet.

I betänkande Informationssäkerhetspolitik – organisatoriska konsekvenser (SOU 2005:71) framfördes att informationssäkerhetsarbetet bör organiseras så att kraftsamling kan ske till administrativa (exempelvis omvärldsanalys och publikationer) respektive tekniska (exempelvis utveckling av teknik för aktiv IT-kontroll) frågeställningar. Av detta drog utredningen slutsatsen att gemensamma behov och tvärsektoriella frågeställningar bör samlas under en myndighet för administrativa funktioner respektive en myndighet för tekniska funktioner.

2.3.3 Utredningen om översyn av Försvarets radioanstalt

I mars 2003 presenterade Utredningen om översyn av Försvarets radioanstalt sitt betänkande (SOU 2003:30). Utredningen betonade att den betraktade informationssäkerhetsområdet som en betydelsefull uppgift för FRA i framtiden. Enligt utredningen borde den teknik som FRA använder för att följa och inhämta information kunna användas för att skydda Sverige och svenska intressen mot attacker mot IT-systemen. Genom signalspaningsinsatser mot global kommunikation till och från Sverige skulle FRA kunna upptäcka attacker mot svenska informationssystem oberoende av var en aktör befann sig. Enligt utredningen borde FRA i framtiden kunna bistå myndigheter och andra aktörer med bl.a. underrättelser som skulle kunna läggas till grund för skydd mot IT-relaterade hot mot systemen.

2.3.4 Utredningen om en myndighet för säkerhet och beredskap

Utredningen om en myndighet för säkerhet och beredskap betonade i sitt betänkande Alltid redo (SOU 2007:31) signalunderrättelsetjänstens stora betydelse för att stärka den svenska informationssäkerheten. Utredningen föreslog därför att informationssäkerhetsansvaret vid dåvarande Krisberedskapsmyndigheten (KBM) skulle överföras till FRA. Detta skulle medföra vissa effektiviseringsvinster genom att samla både det administrativa och det tekniska informationssäkerhetsarbetet under en och samma myndighet. Genom signalunderrättelsetjänsten skulle kunskap också genereras om brister i olika informationssystem vilket skulle gagna säkerheten i svenska system. Utredningen menade även att det internationella samarbetet skulle gynnas av en sådan lösning då Sverige i och med detta endast skulle få en kontaktpunkt utåt. Utredningens förslag kom dock inte att genomföras utan informationssäkerhetsfrågorna fördes över från KBM till den nya myndigheten MSB då denna bildades i januari 2009.

2.3.5 Uppdrag till MSB angående samhällets samlade förmåga att förebygga och hantera IT-incidenter

Den 29 oktober 2009 fick MSB i uppdrag av regeringen (Fö2009/2162/SSK) att lämna förslag på åtgärder för att förebygga och hantera IT-incidenter. Uppdraget slutfördes genom en skriftlig rapport i januari 2010. MSB föreslår i rapporten att ett nationellt operativt samverkanscenter för informationssäkerhet inrättas och placeras vid MSB. Uppgiften för detta samverkanscenter bör enligt MSB vara att stödja samhällets förebyggande informationssäkerhetsarbete och att samordna hanteringen av allvarliga IT-incidenter. Vid samverkanscentret ska experter från både offentlig och privat sektor vid behov kunna arbeta. Centret ska enligt MSB:s förslag

vara en integrerad del av krishanteringssystemet och ha en nära koppling till den lägesbildsfunktion som finns vid myndigheten. Enligt MSB bör en verksamhet med uppgifter av liknande slag som Sitic integreras i samverkanscentret. MSB betonar i rapporten även vikten av en tydlig nationell struktur för privatoffentlig samverkan inom informationssäkerhetsområdet.[2]

[2] Åtgärder för att förbättra samhällets samlade förmåga att förebygga och hantera IT-incidenter. MSB 2010-01-13 (Dnr 2009-14471)

3 Utgångspunkter

3.1 Nuvarande myndighetsstruktur

Den nuvarande ansvarsfördelningen för informationssäkerhet på nationell nivå bygger i huvudsak på en struktur som inrättades i början av 2000-talet. Som en följd av de förslag som Sårbarhets- och säkerhetsutredningen lämnade (SOU 2001:41) och regeringens proposition Samhällets säkerhet och beredskap med påföljande riksdagsbeslut (prop. 2001/02:158, bet. 2001/02:FöU 10, rskr. 261) inrättades år 2002 KBM med ett sammanhållande myndighetsansvar för samhällets informationssäkerhet. Vid PTS inrättades en funktion med ansvar för att hantera uppgifter om IT-incidenter (Sitic). FRA fick ansvar för att tillhandahålla teknikkompetens inom informationssäkerhetsområdet och Försvarets materielverk fick i uppgift att bygga upp ett system för evaluering och certifiering av IT-säkerhetsprodukter. Från och med 2009 är de uppgifter som hanterades av KBM överförda till MSB.

Nedan redogörs för de arbetsuppgifter inom informationssäkerhetsområdet som idag vilar på PTS/Sitic, MSB och FRA. Det ansvar som vilar på andra myndigheter såsom Försvarets Materielverk, Försvarsmakten, Rikspolisstyrelsen och Säkerhetspolisen redovisas inte i detta sammanhang.

3.1.1 PTS/Sitic

PTS fick i maj 2002 regeringens uppdrag att inrätta en funktion för IT-incidentrapportering och sedan januari 2003 är Sitic i drift. Bakgrunden till att Sitic inrättades och placerades vid PTS finns i det förslag som år 1998 lämnades av regeringens arbetsgrupp om informationskrigsföring (AgIW) att en stats-CERT skulle inrättas under PTS. Förslaget bearbetades vidare av PTS och därefter av Sårbarhets- och säkerhetsutredningen.[3]

Sitic är en organisatorisk enhet inom nätsäkerhetsavdelningen vid PTS med för närvarande 13 personer. Av dessa utför personal motsvarande 3 årsarbetskrafter uppgifter som stöder myndighetens generella informationssäkerhetsarbete och robusthetsstärkande insatser för elektroniska kommunikationer, utanför den direkta IT-incidenthanteringen enligt PTS instruktion. Det gäller bl.a. insatser avseende Internetsäkerhet där PTS har ett särskilt regeringsuppdrag, Internet Governence och arbete med att höja medvetenhet och säkerhet för konsumenter och användare av elektroniska kommunikationer inom myndigheter, företag och organisationer.

Inom informationssäkerhetsområdet ansvarar PTS idag för att utveckla robustheten i de elektroniska kommunikationsnäten samt för att förhindra att system slås ut vid störningar. Myndigheten har sektorsansvar för elektroniska kommunikationer och förvaltar därigenom bl.a. lagen om elektronisk kommunikation (LEK) som PTS även har föreskriftsrätt för enligt lagen om elektronisk kommunikation.

PTS deltar i internationellt samarbete som berör informationssäkerhetsområdet, bl.a. via EU och Internationella teleunionen (ITU), EU:s IT-säkerhetsmyndighet Enisa, OECD, organisationer verksamma med Internets förvaltning etc. Inom EU är Sitic medlem av European Government CERT Group (EGC) där liknande nationella funktioner ingår. Ett annat samarbete som Sitic deltar i är Task Force Collaboration of

[3] Förutsättningar för att inrätta en särskild funktion för IT-incidentrapportering. PTS 28 november 2000 (Dnr 99-194489)

Security Incident Response Teams (TF-CSIRT) vilket betyder att Sitic är ackrediterade att ta del av organisationens hantering av incident- och sårbarhetsinformation. Sitic är även medlem i Forum of Incident Response and Security Teams (FIRST) som är en världsomspännande organisation som utgörs av incident-hanteringsfunktioner som gemensamt hanterar och förebygger incidenter på informationssäkerhetsområdet.

PTS budgeterade kostnader för Sitics verksamhet 2010 uppgår till totalt 18,3 mnkr.

Enligt instruktionen ska PTS svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Sitic ska vid inträffade IT-incidenter agera skyndsamt genom att sprida information samt vid behov medverka i samordning av åtgärder som krävs för att avhjälpa eller lindra effekter av det inträffade. Sitic ska vidare samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet, lämna råd och stöd avseende förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer i frågor om nätsäkerhet.

Sitic bedriver verksamhet dygnet runt och är Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder. Sitic bevakar endast trafikflöden i elektroniska kommunikations-nät, således inte innehållet i meddelanden och har ingen legal möjlighet att beordra nedstängning av kommunikationsnät. Motsvarande trafikövervakning utförs också av de större teleoperatörerna/ISP:er vid deras driftcentraler som en del i verksamheten. De har med andra ord egna CERT-funktioner avseende sin egen trafik.

Sitic strävar efter att öka IT-säkerhetsmedvetandet i Sverige genom att förmedla kunskap och fakta. Sitic utfärdar kontinuerligt varningar och råd om sårbarheter i våra IT-system. För detta bedrivs omvärldsbevakning rörande hot och säkerhets-problem på IT-området samt ett nära samarbete och informationsutbyte med liknande nationella och internationella organisationer. Sitic sammanställer varje vecka ett veckobrev

med de viktigaste nyheterna på IT-säkerhetsområdet. Sitic har även en tjänst som går ut med blixtmeddelanden vid allvarliga IT-händelser, som det går att kostnadsfritt ansluta sig till på Sitics webbplats. Sitic handhar systemen Honeynet, som detekterar och registrerar skadlig kod och intrångsförsök på Internet, och LISA som är ett system för insamling och analys av webbloggar. Sitic har även ett system som övervakar den svenska delen av Internet vilket möjliggörs genom ett samarbete med åtta svenska Internetoperatörer.

3.1.2 Myndigheten för samhällsskydd och beredskap

Myndigheten för samhällsskydd och beredskap (MSB) har ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning inte någon annan myndighet har ansvaret. Ansvaret avser åtgärder före, under och efter en olycka eller en kris. MSB ska vara pådrivande i arbetet med förebyggande och sårbarhetsreducerande åtgärder, utveckla och stödja samhällets beredskap mot olyckor och kriser, arbeta med samordning mellan berörda aktörer i samhället för att förebygga och hantera olyckor och kriser. MSB ska vidare bidra till att minska konsekvenser av olyckor och kriser, följa upp och utvärdera samhällets krisberedskapsarbete samt se till att utbildning och övningar kommer till stånd inom myndighetens ansvarsområde.

MSB har vidare enligt instruktionen (6 §) till uppgift att stödja och samordna arbetet med samhällets informationssäkerhet och har föreskriftsrätt inom samma område. MSB ska dessutom inom informationssäkerhetsområdet analysera och bedöma omvärldsutvecklingen samt rapportera till regeringen om förhållanden som kan resultera i behov av åtgärder inom olika nivåer och områden i samhället.

MSB ska kunna bistå med stödresurser i samband med allvarliga olyckor och kriser samt stödja samordningen av de berörda myndigheternas åtgärder vid en kris. I detta kan ingå att

stödja samordning av krishanteringsåtgärder, av information till allmänhet och media samt att samordna stödet till centrala, regionala och lokala organ i fråga om information och lägesbilder (7 §).

MSB har även till uppgift att samordna de civila myndigheternas arbete med säkra kryptografiska funktioner samt förvaltar den nationella handlingsplanen för samhällets informationssäkerhet.

3.1.3 Försvarets radioanstalt

Försvarets Radioanstalt (FRA) har till uppgift att på uppdrag av regeringen och de myndigheter som regeringen bestämmer bedriva signalspaning. Syftet är att kartlägga yttre militära hot och andra utländska förhållanden som kan påverka Sveriges säkerhet, till exempel internationell terrorism.

FRA ska enligt instruktionen ha hög teknisk kompetens inom informationssäkerhetsområdet och får efter begäran stödja sådana statliga myndigheter och statliga bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende.

FRA ska särskilt kunna stödja insatser vid nationella kriser med IT-inslag, medverka till identifieringen av inblandade aktörer vid IT-relaterade hot mot samhällsviktiga system, genomföra IT-säkerhetsanalyser och ge annat tekniskt stöd. FRA ska vidare samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet. FRA stödjer Säkerhetspolisen i tillsynen enligt säkerhetsskyddslagsstiftningen.

4 Analys av alternativen

4.1 Inledning

Enligt regeringens direktiv ska utredaren undersöka vilken av de två myndigheterna FRA och MSB som bedöms bäst lämpad att ansvara för verksamheten vid Sitic. Utgångspunkten ska vara de behov och målsättningar som regeringen angett när det gäller bland annat att samla informationssäkerhetsfrågorna. I detta kapitel redovisas därför en genomgång av hur regeringen behandlat informationssäkerhetsfrågorna i relevanta propositioner under 2000-talet, med tonvikt på de senaste åren. Därefter analyseras de två alternativens för- och nackdelar.

4.2 Regeringens bedömning i tidigare propositioner

I propositionen Samhällets säkerhet och beredskap (2001/02:158) presenterade regeringen år 2002 en övergripande strategi för informationssäkerhet i samhället och skydd av samhällsviktiga IT-beroende system. Regeringen gjorde här följande bedömning:

> Målet bör vara att upprätthålla en hög informationssäkerhet i hela samhället som innebär att man skall kunna förhindra eller hantera störningar i samhällsviktig verksamhet. Strategin för att uppnå detta mål bör liksom övrig krishantering i samhället utgå från

> ansvarsprincipen, likhetsprincipen och närhetsprincipen. Principiellt gäller att den som ansvarar för informationsbehandlingssystem även ansvarar för att systemet har den säkerhet som krävs för att systemet skall fungera tillfredsställande. En viktig roll för staten är därför att se till hela samhällets behov av informationssäkerhet och vidta de åtgärder som rimligen inte kan åvila den enskilda systemägaren. För att förhindra allvarliga informationsattacker mot Sverige bör underrättelse- och säkerhetstjänstens arbete förstärkas.

I propositionen Från IT-politik för samhället till politik för IT-samhället (prop. 2004/05:175) återupprepade regeringen grunddragen i den ovan redovisade strategin för informationssäkerhet. Regeringen gjorde även bedömningen att den viktigaste rollen för Sitic hittills varit omvärldsbevakning och informationsspridning men att få sårbarheter upptäckts genom rapporter till Sitic. Regeringen betonade också att det internationella CERT-samarbetet borde stärkas. I propositionen beskrevs även regeringens strategi för ett säkrare Internet i Sverige med målet att kunna säkerställa kritiska funktioner i Internets infrastruktur.

I mars 2006 presenterade regeringen propositionen Samverkan vid kris – för ett säkrare samhälle (prop. 2005/06:133). Regeringen framhöll här att den år 2002 fastställda strategin för informationssäkerhet borde utvecklas till att även omfatta att kunna upptäcka, ingripa mot och agera i samband med störningar i samhällsviktiga IT-system. I propositionen framhölls vikten av ett förbättrat integritetsskydd samt att en handlingsplan för informationssäkerhet borde utarbetas med utgångspunkt i en nationell strategi för informationssäkerhetsarbetet. Regeringen menade också att det var angeläget med en bred syn på informationssäkerheten i samhället. Ett allt för snävt perspektiv på teknikutveckling och hot borde undvikas och det sågs som viktigt att flera aktörer deltog i informationssäkerhetsarbetet och att formerna och ansvaret för detta klarlades.

I propositionen En anpassad försvarsunderrättelseverksamhet (prop. 2006/07:63) framhöll regeringen att det är angeläget att

de unika inhämtningsmetoder och det avancerade tekniska kunnande som finns inom de myndigheter som bedriver försvarsunderrättelseverksamhet också kan utnyttjas för att möta de IT-relaterade yttre hoten mot den svenska tekniska infrastrukturen, inte minst tele- och datasystemen. Enligt regeringens bedömning ökade antalet rapporter om såväl spridning av datavirus som mycket kvalificerade attacker utförda av t.ex. transnationella kriminella grupperingar eller främmande länders underrättelsetjänster. Ett flertal studier hade också visat hur sårbart samhället är från angrepp från mer kvalificerade aktörer. Regeringen anförde vidare:

> Dessa studier förstärker argumenteringen från t.ex. Informationssäkerhetsutredningen för att staten måste påta sig ett ytterligare ansvar på detta område, framförallt för att möta de IT-relaterade hot som är så allvarliga att de kan betecknas som yttre hot mot rikets säkerhet. Det viktigaste skyddet mot de kvalificerade IT-hoten är det förebyggande arbetet, t.ex. tekniska och administrativa säkerhetsarrangemang. Underrättelseverksamheten kan bidra till dessa, men har också kompetens att tidigt möta de kvalificerade IT-hoten. Samma teknik som används för signalspaning i det globala nätet för traditionell underrättelseinhämtning kan också användas för att skydda mot kvalificerade attacker via det globala nätet mot våra IT-system. En förutsättning för detta är att såväl eter- som trådburen trafik får följas, och att signalspaningens unika metoder kan användas. Sverige riskerar annars att utnyttjas av främmande stater och andra aktörer, som vill begagna våra informationssystem.

Regeringen betonade vidare att de senaste årens stora förändringar av den säkerhetspolitiska miljön och den tekniska utvecklingen medfört ett ökat behov av underrättelser. Regeringen framhöll i detta sammanhang signalspaningens allt viktigare roll i att upprätthålla informationssäkerheten i samhället och för att skydda kommunikation mot intrång från andra länder och aktörer.

I propositionen Stärkt krisberedskap för säkerhets skull (2007/08:92) föreslog regeringen att Krisberedskapsmyndigheten, Statens räddningsverk och Styrelsen för

psykologiskt försvar skulle läggas ned och att en ny myndighet (MSB) inrättades för frågor om samhällets krisberedskap och skydd mot olyckor. I anslutning till detta anförde regeringen att ”informationssäkerhetsfrågorna är sektorsövergripande varför de sammanfaller väl med det ansvar och de uppgifter i övrigt som den nya myndigheten bör få”. Med anledning av detta borde den nya myndigheten ta över KBM:s verksamhet inom området och uppdraget borde också förtydligas.

I 2009 års budgetproposition betonade regeringen att god informationssäkerhet är en förutsättning för att kunna förhindra och hantera störningar i samhällsviktig verksamhet och att MSB borde hålla samman och utveckla det nationella informationssäkerhetsarbetet. Regeringen behandlade också samhällets ökade beroende av Internet och elektronisk kommunikation vilket i sin tur kunde innebära en ökad sårbarhet för samhället. Enligt regeringen hade robusthets- och krishanteringsarbetet inom sektorn för elektronisk kommunikation byggts upp under flera år och vilade på samverkan och ömsesidigt förtroende mellan privata och offentliga aktörer.

Den 21 september 2009 lämnade regeringen budgetpropositionen för år 2010 (prop. 2009/10:1) till riksdagen. Regeringen anförde här bl.a. följande:

> Regeringen anser att ett ändamålsenligt arbete med informationssäkerhet på nationell och internationell nivå är av central betydelse för samhällsutvecklingen. Det är också viktigt att arbeta förebyggande, ha en operativ förmåga samt att ha förmågan att snabbt kunna återgå till normalläget. Det är också viktigt att detta arbete bedrivs på EU-nivå och internationellt. Regeringen anser att det är väsentligt att integrera informationssäkerhetsfrågorna och se dem som en naturlig del i bedömningen av samhällets förmåga, i arbetet med risk- och sårbarhetsanalyser och i beroendeanalyser. Med utgångspunkt från befintliga rekommendationer och gällande föreskrifter är det viktigt att se till att det finns stöd, vägledning och information för införande av godtagbar informationssäkerhet för såväl myndigheter som andra aktörer. Det är också viktigt att på nationell nivå verka för utbildning och medvetandehöjande åtgärder för att öka kompetensen inom

> området på alla nivåer i samhället, t.ex. genom att utbildning i informationssäkerhet ingår som en naturlig del i skolväsendet. Inom ramen för regeringens översyn för en effektiv myndighetsförvaltning finns anledning att även se över informationssäkerhetsfrågorna. Det finns ett behov av att samla resurserna för att skapa goda förutsättningar för att förebygga IT-incidenter liksom för att hantera dem när de inträffar. Rapporteringen av IT-incidenter som utgör hot mot eller medför allvarliga konsekvenser för samhällsviktig verksamhet och kritisk infrastruktur i samhället behöver förbättras.

Regeringen framhöll vidare att uppgiften att ”hålla samman det nationella informationssäkerhetsarbetet för samhällsviktiga verksamheter och tydliggöra olika aktörers ansvar inom området” blir viktig för MSB. Regeringen betonade också informationssäkerhetsfrågornas betydelse i den vardagliga IT-användningen. Fokus borde enligt regeringen ligga på det förebyggande arbetet och en höjd vardagssäkerhet för individer och små och medelstora företag som måste ha kunskap om vilka åtgärder som kan vidtas för den egna säkerheten.

4.3 För- och nackdelar med att placera Sitic vid MSB

MSB har ett brett uppdrag som sträcker sig från att bidra till att förebygga att olyckor och incidenter inträffar till att förbereda samhället på att hantera olyckor och kriser, ge stöd vid inträffade händelser och att löpande och i efterhand utvärdera och följa upp hantering och händelseförlopp. MSB har breda kontaktytor mot kommuner, landsting, företag, myndigheter, organisationer och enskilda. Genom Samfi[4] och Informationssäkerhetsrådet har MSB tillgång till nätverk för samverkan med både myndigheter och enskilda organisationer. Myndigheten har föreskriftsrätt när det gäller informationssäkerhetsarbetet hos statliga myndigheter.

[4] Samverkansrådet för informationssäkerhet

På flera sätt liknar MSB:s uppdrag att samverka, samordna och ge stöd före, under och efter en kris det uppdrag PTS har att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. MSB:s uppdrag om samordning och stöd vid olyckor och kriser kan sägas ha en parallell i PTS uppdrag att agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt vid behov medverka i samordning av åtgärder som krävs för att avhjälpa eller lindra effekter av det inträffade. Omvärldsbevakning inom informationssäkerhetsområdet är en uppgift för båda myndigheterna.

Även om de två myndigheternas uppdrag kan beskrivas i liknande termer (stöd, förebyggande, information, omvärldsbevakning etc.) så framstår dock Sitics arbete som mer tekniskt inriktat med t.ex. analys av och information om sårbarheter i programvara medan MSB mer arbetar på policynivå. Verksamheterna framstår därför som kompletterande, snarare än överlappande.

Enligt utredarens bedömning skulle en överföring av Sitic till MSB därför ge synergieffekter som torde bidra till att utveckla och öka det stöd som centrala myndigheter idag kan ge till samhället. En placering av Sitic vid MSB skulle sannolikt också bidra till att stärka informationssäkerhetsfrågorna vid MSB som därmed kunde ges en tydligare roll av kärnverksamhet. Därtill skulle en inordning av Sitic i MSB kunna bidra till att ytterligare integrera informationssäkerhetsfrågorna dels i den samlade analys av samhällets krisberedskap som sker vid myndigheten, dels i de risk- och sårbarhetsanalyser som statliga myndigheter ska göra enligt den så kallade krisberedskapsförordningen. Tidigare har bland annat Riksrevisionen lyft fram att det finns ett utvecklingsbehov inom detta område. Utredaren delar den bedömningen. Sitics verksamhet skulle dessutom kunna dra nytta av det breda kontaktnät bland kommuner, landsting, företag, myndigheter, organisationer och enskilda som MSB, tidigare KBM, har byggt upp under lång tid.

Verksamhetsmässigt finns således fördelar med att inordna den verksamhet som idag bedrivs vid Sitic med den verksamhet

som bedrivs vid MSB. För att synergieffekter ska kunna uppnås krävs dock att MSB förmår knyta ihop dels de olika delarna av myndighetens informationssäkerhetsarbete (förebyggande, operativt, strategiskt och lärande) inklusive Sitic-delen, dels denna verksamhet med andra relevanta verksamheter vid myndigheten såsom risk- och sårbarhetsanalyser, lägesbildsfunktion och krisinformation. I detta ligger också att skapa förutsättningar för tekniska lösningar som möjliggör informationsutbyte med högt ställda krav både på säkerhet och på funktionalitet.

En grundförutsättning för att uppnå synergieffekter är att Sitic inom rimlig tid kan samlokaliseras med relevanta delar av MSB (bl.a. informationssäkerhetsenheten, lägesbildsfunktionen och krisinformation.se), vilka idag är lokaliserade i Stockholm.

Den utredning som MSB lämnade till regeringen i mitten av januari 2010 innehåller många intressanta förslag för en mer sammanhållen struktur för att förebygga och hantera IT-incidenter. Utredaren finner det dock oklart huruvida MSB har förutsättningar att inom rimlig lösa frågan om samlokalisering.

4.4 För- och nackdelar med att placera Sitic vid FRA

FRA besitter hög teknisk kompetens och det informationssäkerhetsarbete som myndigheten idag utför som stöd till statliga myndigheter och bolag skulle mycket väl kunna förenas med den verksamhet som idag bedrivs vid Sitic. Enligt Infosäkutredningen finns den största gruppen disputerade matematiker utanför universitetsvärlden vid FRA. De tekniska analyser som idag genomförs dels vid Sitic, dels vid FRA kräver i viss utsträckning likartad kompetens. En överföring av verksamheten vid Sitic till FRA skulle kunna skapa en större kritisk massa av tekniker och analytiker vilket skulle stärka Sveriges förmåga att hantera framför allt mer kvalificerade IT-hot.

I samtal med utredaren har företrädare för FRA betonat sambandet och synergierna mellan signalunderrättelsetjänst och informationssäkerhetsarbete. Detta har även noterats av tidigare utredningar (se avsnitt 2.3.2 - 2.3.4) liksom av regeringen i propositionen En anpassad försvarsunderrättelseverksamhet (se avsnitt 4.2).

En placering vid FRA skulle också kunna kombineras med att ge myndigheten mandat att stödja aktörer som idag önskar stöd men inte kan få det med gällande regelverk, t.ex. kommuner, landsting och privata företag.

FRA har redovisat en förhållandevis klar idé om hur verksamheten vid Sitic skulle kunna integreras både organisatoriskt och fysiskt med nuvarande verksamhet vid FRA.

Ett problem vid en placering av Sitic vid FRA skulle kunna vara att förena den relativa öppenhet som kännetecknat arbetet vid Sitic i förhållande till den slutenhet som normalt kännetecknar en underrättelsemyndighet som FRA med dess krav på sekretess och källskydd. Det har också framförts både i den offentliga debatten och i samtal som utredaren haft med vissa företrädare för näringslivet att en placering vid FRA skulle kunna göra det svårare för Sitic att åstadkomma ett förtroendefullt samarbete med t.ex. privata aktörer. Med en placering av Sitic vid FRA kan det uppstå motsättningar vid inrapportering av incidenter då det ska värderas om det är skyddsintresset eller underrättelseintresset som bör väga tyngst. Det krävs en tydlig process för att hantera denna problematik.

Mot detta kan anföras att en förstärkning av informationssäkerhetsverksamheten vid FRA skulle kunna leda till ett mer öppet verkande FRA samt att det är svårt att bedöma huruvida en placering av Sitics verksamhet vid FRA verkligen skulle leda till minskad vilja till samverkan från det omgivande samhället. I utredarens samtal med näringslivet har också framkommit att det bland vissa privata aktörer kan ses som en fördel med en placering vid FRA på grund av myndighetens höga tekniska kompetens och rykte om att tidigt kunna identifiera och analysera tänkbara IT-hot.

5 Utredarens överväganden och förslag

5.1 Utredarens förslag

Utredarens förslag: Sitics personal och verksamheten vid Sitic inordnas i MSB. Formellt torde detta kunna ske den 1 januari 2011. De lokaler som är förberedda för Sitic då PTS under våren 2010 flyttar till Valhallavägen kan dock behöva disponeras under en övergångsperiod under 2011. Utredaren vill dock betona att denna övergångsperiod bör vara så kort som möjligt då de synergieffekter som redovisats ovan kräver en samlokalisering med relevanta verksamheter vid MSB i Stockholm.

Utredaren föreslår att 6 §, förordningen (2007:951) med instruktion för PTS som avser Sitics verksamhet upphävs och istället införs i förordningen (2008:1002) med instruktion för MSB. Ändringen bör träda i kraft den 1 januari 2011.

PTS budgeterade kostnader för Sitics verksamhet 2010 uppgår till totalt 18,3 mnkr. Sitic bör finansieras via MSB:s ordinarie anslag ur utgiftsområde 6, anslaget 2:7 för Myndigheten för samhällsskydd och beredskap. Utredaren föreslår därför att medel motsvarande Sitics nuvarande kostnader som för 2010 uppgår till 18,3 mnkr förs över från utgiftsområde 22, anslaget 2:1 Post- och telestyrelsens myndighetsanslag till MSB:s myndighetsanslag.

FRA har vid möte med utredaren framfört att det är en nackdel att myndigheten idag saknar mandat att ge stöd till icke-statliga aktörer t.ex. kommuner och landsting. Utredaren vill med anledning av detta framhålla att det kan finnas skäl för regeringen att, alldeles oavsett var Sitic placeras, överväga en ändring av FRA:s instruktion som skulle ge myndigheten möjlighet att stödja även andra organ än statliga myndigheter och bolag.

5.2 Skälen för utredarens förslag

Som framgått av redovisningen i kapitel 4 kan goda argument anföras för båda alternativen – FRA och MSB. Synergier skulle sannolikt uppstå oavsett om FRA eller MSB blev ny hemvist för verksamheten vid Sitic. Utredarens bedömning är att Sitic behöver placeras vid en myndighet med en stark och trovärdig ställning såväl bland myndigheter och andra offentliga aktörer som bland privata aktörer. Förtroendet för verksamheten är därmed en viktig aspekt då det gäller att väga de två alternativen mot varandra. Förtroendefrågan rymmer inom sig flera olika dimensioner såsom tekniskt kunnande, intern säkerhetskultur, förmåga att förmedla relevant information i rätt tid samt integritetsaspekter. Det är av största vikt att samarbetspartners både inom och utom landet, både offentliga och privata känner att en förtroendefull samverkan är möjlig.

Den mottagande myndigheten måste också ha tekniska och fysiska förutsättningar att ta emot verksamheten vid Sitic och dess idag 13 medarbetare. Under en kortare övergångsperiod kan det dock vara försvarbart att Sitic sitter kvar i de lokaler som verksamheten kommer att flytta till våren 2010.

Det har i flera sammanhang framförts att incident-rapporteringen till Sitic varit av mindre omfattning än vad som hade förväntats när verksamheten inleddes år 2003. Tänkbara orsaker till detta kan ha varit osäkerhet om Sitics möjlighet att sekretessbelägga rapporter som kommer in, att verksamheten

inte varit tillräckligt känd och att det bland vissa aktörer kan ha upplevts som oklart vad nyttan skulle vara med att rapportera en IT-incident till Sitic. Det tillägg till sekretesslagen (1980:100) som trädde i kraft den 1 juli 2004 bedöms visserligen ha givit ökade förutsättningar att skydda känslig information som rapporteras in. Det framstår dock som rimligt att i framtiden kunna öka andelen incidenter som rapporteras till Sitic. När det gäller att bedöma de två alternativen till ny hemvist för Sitic måste därför övervägas vilken av de två myndigheterna, FRA respektive MSB, som kan antas ha bäst förutsättningar att åstadkomma detta.

Som framgått av redovisningen i kapitel 4 betonade regeringen i budgetpropositionen för år 2010 informationssäkerhetsfrågornas betydelse i den vardagliga IT-användningen och att fokus borde ligga på det förebyggande arbetet och en höjd vardagssäkerhet. Regeringen framhöll också betydelsen av att integrera informationssäkerhetsfrågorna och se dem som en naturlig del i bedömningen av samhällets förmåga, i arbetet med risk- och sårbarhetsanalyser och i beroendeanalyser. Enligt utredarens bedömning blir det därför en nyckelfråga för den framtida Sitic-verksamhetens placering att den mottagande myndigheten har förmåga att arbeta både förebyggande och som ett stöd vid incidenthantering. Myndigheten måste kunna agera öppet och skapa ett förtroende genom att förmedla snabb och korrekt information till ett brett spektrum av målgrupper.

Av betydelse för utredarens bedömning är att den framtida placeringen av Sitic ses som en del i ett större sammanhang och att det gäller att bedöma vilket av de två alternativen som kan antas leda till de starkaste synergieffekterna och utvecklingsmöjligheterna för samhällets informationssäkerhet.

Utredarens bedömning är att både FRA och MSB i huvudsak åtnjuter ett högt förtroende bland flertalet tänkbara samarbetspartners. MSB:s styrka torde ligga i förtroendet för myndighetens öppna och breda samverkansmandat medan FRA i högre grad åtnjuter förtroende för myndighetens tekniska kunnande och möjlighet att ligga i den absoluta frontlinjen när det gäller att

identifiera IT-relaterade hot. Utredarens bedömning är att det synes enklare för MSB, med dess breda samverkansplattform och vana att agera öppet att hantera förtroendeproblematiken än för FRA. Med MSB:s öppna och breda samverkansplattform som bas skulle Sitic också sannolikt ha lättare att nå ut till det privata näringslivet.

Enligt utredarens bedömning torde FRA ha lättare att fysiskt integrera och samlokalisera Sitic med nuvarande verksamhet vid myndigheten. Detta gör att samhällets kostnader för att flytta verksamheten vid Sitic sannolikt blir något högre om alternativet MSB skulle väljas.

En placering vid MSB ger dock fördelen att Sitic placeras i en myndighet som arbetar med hela kedjan, från det förebyggande och förberedande, till det hanterande och lärande. Att placera Sitic vid MSB skulle även sannolikt bidra till att stärka informationssäkerhetsarbetets ställning inom MSB. Enligt utredarens bedömning är det vidare en fördel att kopplingen mellan informationssäkerhet och övriga delar av samhällets krisberedskap, bl.a. arbetet med risk- och sårbarhetsanalyser, stärks vilket skulle vara fallet om verksamheten vid Sitic inordnades i MSB.

Samtidigt kan argumenteras för att en placering vid FRA skulle bidra till att stärka informationssäkerhetsarbetet inom den myndigheten och därigenom stärka Sveriges skydd mot mer kvalificerade IT-attacker.

Frågan om vilken av de två myndigheterna som kan antas bäst lämpad att öka andelen incidenter som rapporteras in till Sitic är svår att besvara med säkerhet. FRA kännetecknas av mycket hög teknisk kompetens och en stark säkerhetskultur vilket skulle kunna tala för att vissa aktörer skulle vara mer benägna att rapportera in incidenter om Sitic var placerat vid FRA. För MSB talar att myndighetens många kanaler till det omgivande samhället kan skapa ett förtroende för myndigheten bland många små och medelstora företag, liksom bland kommuner och andra offentliga aktörer vilket skulle kunna leda till ökad vilja att rapportera incidenter.

Sammantaget är utredarens bedömning att argumenten i huvudsak talar för att verksamheten vid Sitic bör inordnas i MSB. Ett tungt vägande skäl är enligt utredaren möjligheten att skapa synergieffekter genom att tydligare knyta informationssäkerhetsfrågorna till MSB:s generella och sektorsövergripande arbete med samhällets krisberedskap. Vid MSB skulle verksamheten vid Sitic kunna knytas nära både den förebyggande informationssäkerhetsverksamheten och den lägesbildsfunktion som finns vid myndigheten och därmed bidra till att stärka både vardagssäkerhet och samhällets förmåga att förebygga och hantera mer allvarliga IT-hot. En överföring av verksamheten vid Sitic till MSB synes också ligga i linje med vad regeringen anfört som inriktning för informationssäkerhetsarbetet i ett flertal propositioner, inte minst 2010 års budgetproposition.

6 Konsekvenser

6.1 Generella konsekvenser

Utredarens bedömning är att förslaget att inordna verksamheten vid Sitic i MSB skulle få positiva konsekvenser både för arbetet med informationssäkerhet samt för arbetet med samhällets krisberedskap i stort och alltså gagna både det arbete som Sitic och MSB utför idag. Genom att placera Sitic vid MSB åstadkoms en mer samlad lösning av ansvaret för informationssäkerhet på central myndighetsnivå. Det skapas också möjligheter att bättre integrera informationssäkerhetsarbetet i arbetet med samhällets krisberedskap, t.ex. arbetet med risk- och sårbarhetsanalyser.

Några negativa konsekvenser för verksamheten vid Sitic ser utredaren idag inte under förutsättning att frågan om samlokalisering kan lösas inom rimlig tid. Utredaren förutsätter att nuvarande goda samarbete mellan de centrala myndigheter som har uppgifter och ansvar inom området informationssäkerhet fortsätter och utvecklas.

6.2 Personella konsekvenser

Bestämmelser om verksamhetsövergång finns i 6 b § lagen (1982:80) om anställningsskydd (LAS) och 28 § lagen om medbestämmande i arbetslivet (MBL). Enligt LAS (6 b §) övergår de enskilda anställningsavtalen vid verksamhetsövergång automatiskt till förvärvaren, som alltså blir ny arbetsgivare. För de anställda övergår också de rättigheter och skyldigheter på grund av anställningsavtal och de anställningsförhållanden som gäller vid tidpunkten för övergången på den nya arbetsgivaren. Anställda med tidsbegränsning överförs med tidsbegränsningen, den deltidsanställde går över i oförändrad omfattning etc.

Utredarens bedömning är att reglerna om verksamhetsövergång bör tillämpas för de 13 personer som arbetar vid PTS/Sitic som alltså bör erbjudas anställning vid MSB. Arbetstagare har dock möjlighet att välja att avstå från verksamhetsövergång och vara kvar vid PTS. Han eller hon riskerar då att bli uppsagd på grund av arbetsbrist. Arbetstagare som blir uppsagd på grund av arbetsbrist kan – om de uppfyller villkoren - omfattas av trygghetsavtalet. Den som tackat nej till verksamhetsövergång till anställning på samma verksamhetsort omfattas dock inte av trygghetsavtalet. Utredarens förslag avseende Sitic innebär att verksamheten överförs till MSB med placering i Stockholm. Personal vid Sitic som tackar nej till verksamhetsövergång till MSB (Stockholm) omfattas därmed inte av trygghetsavtalet.

Bilaga

Särskilt yttrande av sakkunnig Ingolf Berg

Arbetet med delbetänkandet har bedrivits under kort tid utan formella sammanträden i kommittén. Vid möten med PTS, FRA, MSB och RPS/SÄPO, med syfte att inhämta information och synpunkter i sakfrågan, har jag varit inbjuden. Därutöver har jag tagit del av ett utkast och lämnat synpunkter på detta, men ej slutprodukten.

Uppdraget är i denna del begränsat till att lämna förslag avseende nytt huvudmannaskap för Sitic och konsekvenser vid val mellan två alternativ, MSB eller FRA. Jag instämmer i utredarens förslag, som det redovisats i utkastet, av ny huvudman för Sitic (MSB), men inte avseende överföringen av personella och finansiella resurser från PTS (13 personer resp. 18,3 miljoner kronor).

I uppdraget ingår att utreda konsekvenser vid en överföring av Sitics verksamhet, redovisa kostnader och intäkter för den verksamhet som ska flyttas och att föreslå lämplig finansiering, Det ingår också att redovisa eventuella rationaliseringar som kan uppstå i samband med samordningen. Engångskostnader som t.ex. kan uppstå i samband med flyttning, anpassning av nya eller avveckling av befintliga lokaler ska anges särskilt. I det utkast till delbetänkande som jag tagit del av har detta inte redovisats. Uppgifterna nedan har tidigare tillställts utredaren och redovisas även i detta yttrande.

Sitic verksamhet finansieras idag inom ramen för PTS förvaltningsanslag, ingår i en avdelning för nätsäkerhet och styrs via § 6 i myndighetens instruktion (förordning 2007:951). Det ankommer på PTS ledning och styrelse att organisera verksamheten, fördela och prioritera resurser enligt sitt förvaltningsansvar. Detta har medfört att uppgifter som stöder PTS myndighetsuppgifter, utöver de som anges i nämnda § 6, också utförs inom ramen för Sitics organisatoriska uppbyggnad. Dessa resurser bör enligt min mening inte överföras.

Organisatoriskt har Sitic idag 12-13 årsarbetare, varav 3 årsarbeten enligt PTS utför uppgifter som stöder myndighetens generella informationssäkerhetsarbete och robusthetsstärkande insatser för elektroniska kommunikationer, utanför den direkta IT-incidenthanteringen enligt PTS instruktion. Det gäller bl.a. insatser avseende Internet-säkerhet där PTS har ett särskilt regeringsuppdrag, Internets förvaltning och arbete med att höja medvetenhet och säkerhet för konsumenter och användare av elektroniska kommunikationer inom myndigheter, företag och organisationer.

Kostnadsfördelning enligt 2010 års budget

Sitics totala organisatoriska kostnader 18,3 mnkr (föregående år 18,7 enl. budget)
- därav driftskostnader 11,8
- därav OH-kostnader 6,5

Fördelning av de organisatoriska driftskostnaderna

Sitics funktionella driftskostnader för att upprätthålla IT-incidenthanteringen enligt PTS instruktion 9,3 mnkr
Driftskostnader för PTS-verksamhet inom Sitics organisation som även fortsättningsvis måste bedrivas 2,5 mnkr, totalt 11,8 mnkr.

PTS budgeterade kostnader för den verksamhet som organisatoriskt ligger inom Sitic uppgår till totalt 18,3 mnkr, varav 11,8 utgör driftskostnader (löner, avskrivningar, resor, utbildning m.m.) och 6,5 mnkr overheadkostnader (OH) för att täcka lokalkostnader, gemensam administration och ledning m.m.

De direkta kostnaderna för Sitics funktionella IT-incidenthanteringsverksamhet som den uttrycks i instruktionen uppgår enligt myndigheten till 9.3 mnkr för verksamhetsåret 2010. Driftskostnader för PTS-relaterad verksamhet som organisatoriskt utförs inom Sitic organisation motsvarande tre årsarbetskrafter uppgår till 2,5 mnkr.

De framtida OH-kostnaderna är till viss del beroende av vem som blir ny huvudman och möjligheter till rationalisering. MSB och särskilt FRA har redan idag betydande personella resurser inom informationssäkerhetsområdet vilket torde medföra rationaliseringsmöjligheter. De totala kostnaderna hos en ny huvudman är slutligen också beroende på ambition och orientering av verksamheten.

Direkta finansiella konsekvenser vid ändrat huvudmannaskap

För verksamhetsåret 2011 tillkommer kostnader för direkt-avskrivning av PTS investeringar i särskild anpassning (bl.a. skalskydd) av den nya lokalen på Vallhallavägen, Stockholm som uppgår till 3,8 mnkr, kostnader för återställande av lokalen beräknas till 1 mnkr samt kontraktsenlig hyra under uppsägningstiden om lokalen inte övertas av den nya huvudmannen. Om lokalerna övertas behöver särskild anpassning ske avseende tillträde då dessa är lokaliserade på översta våningsplanet.

Sitics nya lokaler är på 357 kvm och deras andel av den gemensamma lokalytan uppgår till 105 kvm, dvs. totalt 462 kvm. Detta motsvarar 8,4 % av den totala lokalytan som är på 5 500

kvm. Kallhyran uppgår andelsmässigt till ca 1,1 och varmhyra till ca 1,5 mnkr/år.

Det bokförda värdet av främst datautrustning och system som ska överföras uppgår till ca 1 mnkr. Därtill kommer eventuella kostnader för personal som väljer att inte följa med i övergången (t.ex. kostnader för förlängd uppsägningstid, maximalt 12 månader enligt trygghetsavtalet). Det går inte att beräkna denna kostnad idag som i genomsnitt uppgår till 750 kkr/person för 12 månader enligt PTS uppskattning.

Sammanfattning

Det belopp som kan överföras från PTS torde uppgå till 9,3 miljoner kronor plus andel av gemensamma kostnaderna. Därutöver behöver PTS kompenseras för kostnader av engångskaraktär i samband med flyttningen. Finansierings-aspekterna måste hanteras i ett sammanhang, där preliminär avräkning sker initialt från det belopp som överförs och därefter slutavräkning när flytten är genomförd.