Årsrapport Säkerhetstjänst 2006

FÖRSVARSMAKTEN

Militära underrättelse- och säkerhetstjänsten MUST

Den militära säkerhetstjänstens omfattning

Säkerhetsunderrättelsetjänst

Följa hotutvecklingen och klarlägga den säkerhetshotande verksamhet som kan komma att riktas mot Försvarsmakten, främst i form av:

- Underrättelseverksamhet
- Kriminalitet
- Sabotage
- Subversion
- Terrorism

Säkerhetsskyddstjänst

Verka förebyggande och skydda (balans mellan IT-säkerhets-, signalskydds- och tillträdesskyddsåtgärder) hemliga uppgifter från att röjas, obehörigen förändras eller förstöras samt skydda materiel, anläggningar och personal mot sabotage, stöld och terrorism.

Delområden:

- Informationssäkerhet
- Tillträdesbegränsning
- Säkerhetsprövning
- Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)
- Internationella säkerhetsfrågor

IT-säkerhet och signalskyddstjänst

Följa riskutvecklingen och klarlägga säkerhetshotande verksamhet mot Försvarsmaktens informations- och kommunikationssystem.

Detektera, avbryta och återställa angrepp eller försök till angrepp på Försvarsmaktens informations- och kommunikationssystem. Detta syftar till att förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikationer, i detta ingår även användning av kryptografiska funktioner i informationssystem.

EN SVENSK TIGER®

ÅRSRAPPORT
SÄKERHETSTJÄNST
2006

Militära underrättelse- och säkerhetstjänsten MUST

FÖRSVARSMAKTEN

Omslagsbild

Foto: Digital Vsion

Fotografer

Sidan 7: Andreas Karlsson/FBB
Sidan 9: Björn Palmertz/FBB
Sidan 10: Andreas Karlsson/FBB
Sidan 13: Andreas Karlsson/FBB
Sidan 15: Andreas Karlsson/FBB
Sidan 17: Andreas Karlsson/FBB
Sidan 18: Andreas Karlsson/FBB
Sidan 20: Berga
Sidan 31: Johan Eckervad/FBB
Sidan 32: Andreas Karlsson/FBB
Sidan 33: Rickard Bergius/MUST SÄKK
Sidan 41: Peter Liander/FBB
Sidan 47: Therese Holmberg/FBB
Sidan 48: MUST SÄKK
Sidan 49: MUST SÄKK

Denna årsredovisning publiceras även på Försvarsmaktens hemsida på internet www.mil.se, sökord ”årsäk06”.

Omslaget är tryckt på Galerie 170 g och inlagan på Galerie 115 g.

Grafisk form: FMLOG AdmE ToD Grafiska ateljén.
Tryckeri: Davidsons Tryckeri AB, Växjö 2007.

ÅRSRAPPORT SÄKERHETSTJÄNST 2006

SÄKERHETSHOTANDE VERKSAMHET

SÄKERHETSSKYDD

SÄKERHETS- OCH SIGNALSKYDDSKONTROLLER 2006

SIGNALSKYDDSTJÄNST

ÅRSRAPPORT SÄKERHETSTJÄNST 2006

Säkerhetstjänst allmänt

Säkerhet handlar om kontroll

Säkerhet handlar om kontroll. I botten finns alltid ett skyddsvärde, ett objekt, det kan vara ett område, en byggnad, ett system, en informationsmängd eller en individ eller något annat som behöver skyddas. Runt det skyddsvärda objektet etablerar man sedan kontroll. Kontrollen kan bestå av fysiskt skydd, lås, väggar, säkerhetsskåp, de kan bestå av personal i form av vakter, det kan bestå i att kontrollera att bara personer som är prövade och bedömda som pålitliga och lojala får ta del av information. Ofta består kontrollen av en mängd samverkande funktioner och mekanismer, såväl fysiska, tekniska, administrativa som personella.

Beroende på skyddsvärdet hos objektet eller mängden tillgängliga resurser; eller gamla traditioner, sätts nivån på kontrollen runt objektet. Integritetsskäl påverkar också nivån på kontrollen. Kontrollen kan av naturliga skäl aldrig bli fullständig oavsett hur mycket resurser som sätts in. Däremot ökar kontrollen med mängden insatta åtgärder. Av integritetsskäl är det en vanlig tendens i säkerhetsarbetet att prioritera tekniska kontrollmetoder framför att noggrant undersöka personers pålitlighet och lojalitet.

När man förlorat kontrollen

En viktig dimension av kontrollen är strävan att få veta när man förlorar kontrollen, dvs att få larm eller indikation på att kontrollen runt objektet är komprometterad. Detta är naturligtvis i många fall svårt, speciellt avseende personers pålitlighet och lojalitet och också vad gäller sekretess-/ informationsförluster. I de fallen uppstår ju oftast inga spår förrän det är för sent. Trots detta måste man göra att allt för att säkerställa att man i de fall det är möjligt får indikationer, det kan vara larmsystem, logganalyser, löpande uppföljning av personalen, inventering av information, kontroller av säkerheten osv.

Att återfå kontrollen

Kontentan av ovanstående är att man vid vissa tillfällen kommer förlora kontrollen över sitt skyddsvärda objekt. Säkerhetsmekanismerna och säkerhetsorganisationen måste därmed ha en god förmåga att klarlägga, återställa, utreda och lagföra, med mera. Förmågan att återfå kontrollen måste vara lika god som förmågan till kontroll. Förmågan till att återfå kontrollen kommer i form av resurser för att utreda, återställa, exvis säkerhetsunderrättelseresurser, CERT, säkerhetsprövningsresurser för att utreda personfall, samt i form av planer och föreberedelser för att återfå kontrollen i händelse av incidenter.

Kontroll i IT-världen

Ett specialfall av att etablera kontroll över ett skyddsvärde är den kontroll som krävs för att skydda våra informationssystem och den information som är lagrad där. Dock föreligger samma grundläggande förutsättningar avseende kontroll enligt ovan även för IT-system. Det är egentligen ingen skillnad att skapa säkerhet i ett IT-system jämfört med att skapa säkerhet i ett hus. Man måste etablera kontroll och larmas om man förlorar den. På samma sätt som i ett hus måste man även se till att de behöriga användarna är pålitliga och lojala.

Organisation och ledning av den militära säkerhetstjänsten

Den militära säkerhetstjänstens uppgift är att tillvarata de säkerhetsintressen som främst berör Försvarsmakten och dess tillsynsområde enligt säkerhetsskyddslagstiftningen, (FRA, FMV, FORTV, FOI, Pliktverket, FHS och FortV).

Säkerhetsintressena omfattar eller kan hänföras till personal, materiel, information, anläggningar och verksamhet.

Med begreppet militär säkerhetstjänst avses såväl verksamheten som dess organisation. Den militära säkerhetstjänsten består av säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalskyddstjänst.

Den centrala ledningen av säkerhetstjänsten utövas av Säkerhetskontoret vid militära underrättelse- och säkerhetstjänsten, MUST. C MUST är Försvarsmaktens säkerhetsskyddschef, informationssäkerhetschef och chef för Totalförsvarets signalskyddstjänst.

Operativ chef i Högkvarteret leder säkerhetstjänsten i Utlandsstyrkan.

Operativ chef i Högkvarteret leder också den territoriella säkerhetstjänsten i Försvarsmakten med stöd av säkerhets- och samverkanssektioner i Malmö, Göteborg, Stockholm och Boden.

Varje myndighet inom Försvarsmaktens tillsynsområde har en egen säkerhetsorganisation. Dessa samverkar på många områden med Försvarsmaktens säkerhetsorganisation.

Omfattning

Militär säkerhetstjänst omfattar säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalskyddstjänst.

Säkerhetsunderrättelsetjänsten syftar till att bedöma säkerhetshot som riktas mot Försvarsmakten och dess intressen inom och utom landet. Bedömningen har sedan tjänat som underlag för beslut om skyddsåtgärder. Den säkerhetshotande verksamheten redovisas under kapitlet om säkerhetshotande verksamhet.

Säkerhetsskyddstjänsten syftar till hindra eller försvåra säkerhetshotande verksamhet samt förlust av skyddsvärd information.

Signalskyddstjänsten syftar till att förhindra obehörig insyn i och påverkan av totalförsvarets informations- och kommunikationssystem, samt övrig användning av kryptografiska funktioner i informationssystem.

Utöver detta tillkommer delprocesserna information/ utbildning och kontroller som skall ses som stöd och uppföljning av den militära säkerhetstjänsten.

Den militära säkerhetstjänsten är organiserad i 7 delprocesser:

- Ledning
- Information och utbildning
- Kontroller
- Säkerhetsoperationer
- Säkerhetsanalys
- Säkerhetsskydd
- Teknikutveckling

Världen förändras och globaliseras och säkerhetstjänsten försöker ligga långt fram vad gäller att utveckla den egna verksamheten. Kompetenser och metoder inom den millitära säkerhetstjänsten är och skall vara på en kvalitativt hög nivå. Våra motståndare är av världsklass och det sätter nivån på kraven på oss.

Ökade internationella insatser och internationalisering ställer högre krav på säkerhetslägesuppfattning och förmåga att klarlägga säkerhetshotande verksamhet.

Den ökande användningen av informationsteknik ställer högre krav på utveckling av skyddsmekanismer inom IT-säkerhets- och kryptoområdet.

Behovet av att arbeta förebyggande inom säkerhetstjänsten är tydlig, då stora resurser måste läggas på att rätta till misstag som begåtts på grund av att befattningshavare har fått för lite säkerhetsutbildning och har för lågt säkerhetsmedvetande.

Överbefälhavaren, genom chefen MUST, utövar ledning av säkerhetstjänsten bland annat genom normgivning. Normerna är uttryckta i författningsform (FFS och FIB) som utvecklas i handböcker (H SÄK) vilka sedan används vid utbildning och kontroll.

Genom såväl planlagda, överraskande som särskilda kontroller erhålls kvitto på att fastställda regelverk fått avsedd effekt i organisationen.

Den militära säkerhetstjänsten samverkar på alla nivåer med polismyndigheter och SÄPO. I det fall den militära säkerhetstjänsten misstänker att brott begåtts eller är på väg att begås, görs en polisanmälan. Den militära säkerhetstjänsten bedriver inte polisiär verksamhet.

Regelverksförändringar 2006

I föregående års årsrapport angavs att Försvarsmaktens interna bestämmelser (FIB 2006:2) om IT-säkerhet skulle träda i kraft den 15 mars 2006. De förändringar som gjordes var framförallt definitionen på produktägare

och följdändringar med hänsyn till att militärdistrikten lades ner. Utöver denna författning har inga andra förändringar gjorts i de författningar som rör Försvarsmaktens säkerhetstjänst.

Information och utbildning

Under 2006 har Säkerhetskontoret lämnat stöd till främst FM UndSäkC och TSS vid genomförandet av säkerhets-, IT-säkerhets- och signalskyddschefskurser. Vidare har utbildningsinsatser genomförts vid Försvarshögskolans olika program.

Under 2006 publicerades ett antal artiklar om säkerhetstjänsten av i Insats och Försvar.

Den militära säkerhetstjänsten har en heltäckande serie handböcker som i råd och anvisningar utvecklar de författningar och bestämmelser som styr verksamheten.

Under året har H SÄK Hot och H SÄK IT kommit ut i nya totalt reviderade versioner.

Den interaktiva utbildningen i grundläggande säkerhetstjänst går nu att genomföra via Försvarsmaktens intranät, emil. Utbildningen med godkänt slutprov skall göras en gång per år som ett komplement till den lagstadgade säkerhetsutbildningen.

SÄKERHETSHOTANDE VERKSAMHET

Inledning

Allmänt om verksamheten 2006

Den militära säkerhetsunderrättelsetjänsten syftar till att identifiera och klarlägga säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess intressen inom och utom landet. Med säkerhetshot avses, ur den militära säkerhetstjänsten perspektiv, främmande underrättelseverksamhet, kriminalitet, terrorism, sabotage och subversion vilket utvecklas vidare nedan. Säkerhetsunderrättelsetjänsten ska främst producera underlag för beslut om säkerhetsskydds- och signalskyddsåtgärder men även för fortsatt säkerhetsunderrättelseinhämtning.

För att genomföra denna verksamhet nationellt krävs en god kännedom om regionala och lokala förhållanden. Under 2006 har den Operativa enhetens säkerhets- och samverkanssektioner etablerat sig och under hösten har verksamheten utvecklats varvid det nu återigen finns en sammanhängande säkerhetsunderrättelsetjänst från taktisk och operativ till militärstrategisk nivå. Samtliga OPE J2 SäkSam-sekt har under 2006 i någon form lämnat stöd till Försvarsmaktens övningsverksamhet, prov- och försök med både svenska och utländska deltagare. Vidare har ett stort antal besök inom ramen för FM utbyte med andra länder genomförts där SäkSam-sekt har haft en stor roll vad avser planering och uppföljning och stöd till Garnisoner och enskilda förband. Mer om detta redovisas under rubriken skyddsvärd verksamhet nedan.

Provplatsen i Vidsel har även detta år haft omfattande prov- och försöksverksamhet. Värt att notera är den kraftigt ökande efterfrågan från andra länder att nyttja Vidsel för olika verksamheter. En ökning av internationellt samarbete och insatser tillsammans med andra nationer ställer andra krav än tidigare på verksamhetsägaren och hans skyldighet att identifiera vad som är skyddsvärt i respektive verksamhet.

Skyddsvärd verksamhet

Under 2006 har brister i inrapportering av skyddsvärd verksamhet utmynnat i en allvarlig säkerhetsincident. Verksamhetsägare har brustit i identifiering av planerad skyddsvärd verksamhet vilket medförde att säkerhetshotande verksamhet bedöms ha genomförts riktat mot minst en av dessa verksamheter där eventuell skada eller men fortsatt utreds.

Nationellt har den skyddsvärda verksamheten fortsatt legat på samma nivå som under 2005. Under 2006 har DEMO 06 med fältförsök genomförts i Enköping och Karlskrona (vissa enheter fanns på andra platser). Vidare har en större beredskapskontroll genomförts med stora delar av Försvarsmakens deltagande (DAGNY) samt Försvarsmaktsdagar som genomfördes i Stockholm, Göteborg och Malmö.

Den internationella övningsverksamheten har under 2006 fortsatt legat på en hög nivå. Större övningar som genomförts är en markoperativ övning i Norge, ”Cold Response”, en sjöoperativ övning i Östersjön inom NATO; övningen ”Brilliant Mariner”. Flygvapnet har genomfört en större luftoperativ övning, ”Cope Thunder”, i Alaska. Särskilda utmaningar finns kopplade till denna främst avseende informationssäkerhet kring prestanda, metoder och operativ förmåga kring våra vapensystem

och plattformar. Härvid är det viktigt att verksamhetsägaren tidigt fokuserar på säkerheten i och kring sådan verksamhet. Det finns goda exempel på att detta har fungerat som vid flygövningen ”Cope Thunder” men det finns tyvärr också information om det motsatta. Konsekvensen kan i dessa fall bli att Försvarsmakten avslöjar unika prestanda och utsätter personal och materiel för hot från främmande underrättelseverksamhet. Samtliga dessa övningar har medfört ett omfattande säkerhetsarbete. Det bör i detta sammanhang poängteras att säkerhetschefer för dessa övningar ska utses av den som ska genomföra verksamheten. Rollfördelningen måste vara klar och det tål att påpekas att det är verksamhetsägaren som bär ansvaret och skall fastställa vilken nivå på risken som kan anses vara försvarbar.

När det gäller våra insatsområden så har Försvarsmakten under 2006 fortsatt sitt engagemang i Kosovo, ökat truppbidrag och ansvar i Afghanistan, avvecklat bidraget i Liberia, genomfört en insats i Kongo under en begränsad tid och påbörjat en insats med ett sjöoperativt förband i Medelhavet inom ramen för en FN-operation. Vidare har en främre bas upprättats i Abu-Dhabi med transportflygdivisionen i syfte att höja säkerheten kring trupp- och materieltransporter in till och från Afghanistan samt att en av Marinens ubåtar har varit och fortsatt är baserad i San Diego, USA. De två sistnämnda är en särskild utmaning för säkerhetstjänsten eftersom det är en utskjuten del av en flottilj eller ett förband som grupperar utanför Sverige under lång tid och är inte, per definition, en utlandsmission. Utöver detta så är Försvarsmaktens personal grupperad på många platser i världen i enskilda missioner vilket inte ska förglömmas men där har FM ett begränsat säkerhetsskyddsansvar. Vid internationella insatser ställs ökade krav på identifiering av ”angripare och aktörer”. Här är det viktigt att den militära säkerhetsunderrättelsetjänsten, samordnat med den militära underrättelsetjänsten kan inhämta, bearbeta, analysera och delge underlag inför potentiella insatser som efterfrågas på politisk och militärstrategisk nivå. I dessa sammanhang bör det påpekas att, en svensk insats kan komma att utgöra ett hot mot de parter som förekommer i insatsområdet, vilket ställer krav på vår förmåga avseende kontraverksamhet. En beskrivning av säkerhetshot i våra insatsområden följer under respektive rubrik nedan.

Inriktning för år 2007

Under 2007 kommer stödet till Försvarsmaktens ansträngningar med att få Nordic Battle Group (NBG) samträning och operativ att vara i fokus främst under andra halvåret 2007. För den militära säkerhetsunderrättelsetjänsten innebär detta att vi måste på ett proaktivt sätt stödja C PROD och i förlängningen Garnisons och förbandschefer med säkerhetshotbedömningar inför övningsverksamhet och beredskapsställning. FM LOG verksamhet är i detta avseende särskilt viktig.

Vidare kommer säkerhetsunderrättelsetjänsten fortsatt arbeta med att förbättra rapporteringsrutinerna avseende säkerhetshotande verksamhet. Utan relevanta indata så blir inte lägesbilden tillförlitlig och därmed blir det svåra att lämna beslutsunderlag och vidta säker-

hetsskyddsåtgärder. Stödet till svensk förmågeutveckling och NBG intensifieras. Härvid är det vitalt att säkerhetsunderrättelsetjänsten kan identifiera vilka aktörer som visar ett intresse och som kan utgöra ett säkerhetshot mot FM skyddsvärda verksamhet och intressen.

För 2007 har rapporteringsrutiner för den skyddsvärda verksamheten införts i Försvarsmaktens Beredskapsorder (FM BerO Annex D). Rapportering skall i första hand ske i IS UNDSÄK eller via kryfax. Rapporteringen av planerad skyddsvärd verksamhet ska ske kvartalsvis och klassificeras som ”64” i IS UNDSÄK. Kvartalsmöten genomförs i MUST Säkerhetskontor regi. Med en väl fungerande inrapportering av skyddsvärd verksamhet ökar förutsättningarna för att kunna klarlägga eventuella säkerhetshot samt säkerställa att erforderliga säkerhetsskyddsåtgärder vidtas.

Övergripande säkerhetshotbild

De dimensionerande säkerhetshoten nationellt är, som under år 2005, fortsatt främmande underrättelseinhämtning och kriminalitet. Även terrorism måste här medräknas just mot bakgrund av de konsekvenser som ett angrepp sannolikt får samt att Försvarsmaktens insatser internationellt kan medföra ett överfört hot mot FM i Sverige. Vid de internationella insatserna varierar säkerhetshoten beroende på de förutsättningar som finns för just det specifika insatsområdet. Hotbilden för korvetten Gävle i Medelhavet är inte densamma som för den svenska insatsen i Afghanistan. Utgångsvärdena är ofta komplexa med olika konfliktparter, olika koalitionspart-

ners i insatsområdet, värdlandets förutsättningar och dess förhållande till annan stat mm.

Generellt kan sägas att det är av vikt att identifiera vem eller vilka som angriper och agerar mot Försvarsmakten och dess intressen. Härvid skall det klarläggas huruvida den/de utgör hot i någon form och grad. En av de viktigaste uppgifterna i att identifiera angriparen är att fastställa i vilken utsträckning denne har kapacitet och intention riktad mot vår skyddsvärda och säkerhetskänsliga verksamhet. I vissa fall är det även av vikt att bedöma och fastställa angriparens valmöjlighet till tillfälle i tid och rum. Identifiering och fastställande av dimensionerande säkerhetshotande angripare är av betydelse för att lämpliga säkerhetsskyddsåtgärder ska kunna väljas och vidtas. För säkerhetsunderrättelsetjänsten är det av vital betydelse att säkerhetsunderrättelserna förstås och är kommunicerade med mottagare och verksamhetsägare.

Främmande underrättelsetjänst

Hotet från främmande underrättelseverksamhet ligger kvar på oförändrad nivå både i Sverige och i de internationella insatser där Försvarsmakten deltar. Under året har det inkommit rapporter som bekräftar att det finns ett stort intresse från främmande makt för våra kvalificerade vapensystem (sjö- och luftstridskrafter) och utvecklingsprojekt som NBF. Detta har bland annat visat sig i samband med Försvarsmaktsdagarna som genomfördes i Stockholm, Göteborg och Malmö. Under dessa dagar, då Försvarsmakten förevisade flera moderna system för allmänheten, identifierades vid ett flertal tillfällen också representanter från främmande makt då de försökte skaffa fram underrättelser genom att ställa ett stort antal frågor till olika befattningshavare ur Försvarsmakten. Vidare försökte de vinna tillträde till utrymmen dit allmänheten inte ha tillträde.

När det gäller främmande underrättelseverksamhet riktat mot svenska förband i FM insatsområden så har rapporteringen under året ökat. En förklaring kan vara att Sverige i sitt truppbidrag har enheter som verkar inom underrättelsefunktionen och därmed tilldrar sig ett intresse från både samarbetspartners och aktörerna i insatsområdet. Det har bland annat förekommit kontakttagande och underrättelseinhämtning gentemot minst en svensk officer i Kosovo. I detta fall var det en serbisk lokalanställd vid UNMIK som närmade sig en svensk KFOR officer för att få tillgång till information.

Ytterligare underrättelseinhämtning har skett mot den svenska kontingenten i Afghanistan, dock i andra syften. Ett problem tycks vara aningslöshet bland svenska soldater och officerare särskilt i missioner som är etablerade. Ett relativt nytt problem är informationsförlust genom förlust eller slarv med lagringsmedia (USB-minnen etc.) där sekretessbelagd information kan ha förlorats. I minst ett fall har det i Afghanistan tvingat fram säkerhetsskyddsåtgärder som påverkat användbarheten av en hel funktion. Säkerhetshoten verkar inte tas riktigt på allvar och ytterligare utbildningsinsatser måste genomföras under 2007 både inför och under en mission.

Terrorism

Under det gångna året utsattes inte Försvarsmakten för några terroristrelaterade incidenter nationellt. Försvarets materielverk utsattes för ett misslyckat brandbombsattentat i september. Attentatsförsöket är inte att betrakta som ett terroristbrott utan kan närmare beskrivas som försök till allmänfarlig ödeläggelse. Aktören var politiskt motiverad och aktionen syftade till att manifestera missnöje mot ett bilateralt försvarsindustriellt samarbetsprojekt. De gjorda bedömningarna avseende säkerhetshotet från terrorism riktat mot Försvarsmaktens verksamhet och intressen visade sig därmed överensstämma med utvecklingen under året.

Hotbilden är högre i Försvarsmaktens insatsområden än den är nationellt. Inga incidenter som avviker från gjorda bedömningar rörande säkerhetshotet från terrorism har dock inträffat under det gångna året. I Afghanistan har under 2006 en markant ökning av antalet terrorattacker riktade mot den internationella närvaron konstaterats. Angreppen gäller både den internationella militära (ISAF) och civila närvaron samt lokala afghanska myndigheter. Inga hot har riktats mot Sverige som nation eller svenska intressen men då Sverige ingår som en del i den internationella närvaron har den svenska kontingenten en liknande hotbild som övriga i ISAF ingående länder. Detta har föranlett att skyddsåtgärder för den svenska kontingenten i ISAF har vidtagits under året.

I övriga insatsområden har inga incidenter inträffat under det gångna året. Dock verkar svenska förband i områden där hotbilden mycket snabbt kan förändras. En förändring kan orsakas av egen genomförd verksamhet samt genom överförd hotbild från samarbetsländer som verkar inom samma område. En förändrad hotbild kan eventuellt ge överspridningseffekter från ett insatsområde till Sverige nationellt eller annat geografiskt område där svenska intressen finns. Även nationella politiska och militärstrategiska ställningstaganden kan förändra detta säkerhetshot mot Försvarsmakten både nationellt och internationellt.

Ett exempel som belyser hur snabbt detta kan ske finns i vårt när-

område bl.a. vid publiceringen av Muhammedkarikatyrerna i Danmark som omedelbart resulterade i en reaktion mot danskar och danska intressen såväl i Danmark som internationellt.

Hotutvecklingen följs nogsamt för att beslut om nya skyddsåtgärder snabbt skall kunna fattas om hotbilden förändras i de olika områdena där svensk trupp är verksam.

Kriminalitet

Säkerhetshotet från kriminalitet riktat mot Försvarsmakten, såväl i Sverige som i de internationella insatser där Försvarsmakten deltar ligger kvar på oförändrad nivå.

Främsta hotet mot Försvarsmakten i Sverige utgörs av tillgreppsbrott och de säkerhetsrapporter som är av störst intresse att bearbeta är främst tillgrepp och försök till tillgrepp av vapen och ammunition. Även tillgrepp av avancerad skyddsutrustning såsom kroppsskydd, skyddsmask och den nya kevlarhjälmen tilldrar sig stort intresse från olika aktörer. Under året har antalet säkerhetsrapporter varit i stor sett oförändrat vad avser tillgrepp av vapen mm.

FM drabbades under 2006 av metallstölder i en, relativt 2005, ökad omfattning. Tillgreppen har riktats mot avvecklingsmateriel men den största ökningen har skett mot koppar som finns på en mängd platser i FM, främst kring skyddsobjekt. I huvudsak rör det sig om extern brottslighet som riktar sig mot flera samhällssektorer. Det finns tecken som tyder på att verksamheten är organiserad i någon form men ingen aktör har kunnat pekas ut än.

Även drivmedelsstölder har under 2006 drabbat FM. Främst i norra Sverige har denna verksamhet skett under flera år. Dock har modus ändrats efter det att skyddsåtgärder vidtagits och nu är det fordon i olika typer av förråd och uppställningsplatser som främst är utsatta. Några av dessa stölder har kunnat klaras upp. Det finns tecken som tyder på att det rör sig om både extern och intern kriminalitet. Under 2007 kommer detta särskilt att bevakas.

Antalet larmincidenter har ökat kraftigt under 2006 vilket bedöms främst bero på ökad rapporteringsbenägenhet vid några förband. Ett stort antal av dessa incidenter har konstaterats vara orsakade av handhavandefel från personal som har haft att hantera larmanlägg-

ningarna. Detta är ett otillfredsställande förhållande som kan leda till bristande förtroende för vidtagna säkerhetsskyddsåtgärder, en minskad benägenhet att göra insats och ett minskat säkerhetsmedvetande vid insats. En utredning av larmincidenterna under året har gjorts av Säkerhetssamverkanssektionen i Göteborg.

Det har skett en ökad rapportering som indikerar att Internet kan vara en ny arena för brottslig verksamhet riktad mot Försvarsmakten. Det handlar om sekretessbelagd information om anläggningar och som publiceras på olika s.k. ”siter” och om olika privatpersoners försäljning av Försvarsmaktens egendom genom auktions- och försäljningssiter. Denna verksamhet kommer att ägnas större uppmärksamhet under kommande år.

I de internationella insatserna har det förekommit fall av ekonomisk brottslighet, även i år kopplat till upphandlingsrutiner. Två FM anställda misstänks ha förskingrat ett antal miljoner kronor genom att bl.a. utnyttja falska fakturor under en längre period. Personerna har varit ansvariga för att upphandla tjänster inom ramen för byggnationer och anläggningsunderhåll på Camp Victoria. Ärendet är överlämnat till polisen för fortsatt utredning och FM har kunnat vidta skyddsåtgärder och upphandlingsrutinerna har ändrats. Genom sitt agerande misstänks personerna ifråga inte bara ha begått brott utan dessutom utsatt den svenska kontingenten för ett indirekt eller potentiellt säkerhetshot då installationer m.m. är kända av företag med kopplingar till grovt organiserad brottslighet i Kosovo och på Balkan.

Subversion

Under året har inga säkerhetsrapporter inkommit som kan bedömas peka på någon aktör som bedriver subversiv verksamhet riktad mot Försvarsmaktens verksamhet eller intressen, vare sig i Sverige eller i samband med internationella insatser.

Sabotage

Under året har inga säkerhetsrapporter inkommit som kan bedömas peka på någon aktör som bedriver sabotage riktat mot Försvarsmaktens verksamhet eller intressen, vare sig i Sverige eller i samband med internationella insatser.

IT-säkerhetsrelaterade incidenter

FM CERT

FM CERT (FM Computer Emergency Response Team) är Försvarsmaktens resurs på Militärstrategisk nivå (koncernnivå) vad gäller IT-säkerhet. FM CERT har två huvuduppgifter, incidenthantering och lägesbild.

Incidenthantering innebär insamling och sammanställning av IT-säkerhetsrelaterade incidenter. Vid mindre allvarliga incidenter har FM CERT normalt endast en rådgivande och stödjande funktion. Statistik sammanställs och erfarenheter delges. Vid allvarligare incidenter kan FM CERT träda fram och koordinera och/eller överta incidenthanteringen.

Den andra huvuduppgiften innebär att sammanställa och delge en lägesbild rörande IT-säkerhetsläget i Försvarsmaktens IT-system. Denna syftar ytterst till att skapa beslutsunderlag för operativ chef. Till grund för lägesbilden ligger framför allt driftlägesöver-

vakning, omvärldsbevakning och incidentrapportering. Omvärldsbevakningen tjänar också till att informera driftägare om sårbarheter och tillgängliga säkerhetsuppdateringar.

Arbetet fortskrider avseende bildande av förbandet FM CERT. Vid sidan av den operativa verksamheten har under 2006 stor vikt lagts vid förbandsutveckling som sker i samverkan med FMV. Metod, teknik och utbildning är huvuddelarna i denna utveckling. Ytterligare personal har rekryterats.

Antalet inrapporterade incidenter ligger på en nivå motsvarande tidigare år. Oftast rör det sig om felaktig hantering av sekretessbelagd information i IT-system, eller otillåtna sammankopplingar av system. Otillåten användning av trådlösa nätverk har förekommit. I samband med att UIT (Utvecklad IT-drift) börjar rullas ut på förbanden upptäcks och åtgärdas en hel del gamla brister. Centraliseringen som UIT medför innebär en bättre kontroll av säkerhetsnivån, och uppdateringar kan snabbt och enkelt distribueras inom Försvarsmakten.

Skadlig kod

Inga allvarliga utbrott av skadlig kod drabbade Försvarsmakten under 2006. Tack vare en god nätarkitektur samt en strikt policy avseende behörigheter så har vi varit relativt förskonade.
Trenden går mot mer riktade attacker. Hackare världen över har insett att de kan tjäna pengar på sina kunskaper och har därför till viss del slutat att slumpmässigt sprida skadlig kod genom e-post. Istället säljer de sina tjänster till dem som är beredda att betala, antingen till någon som är ute efter pengar eller information.

Försvarsmakten är en högst tänkbar måltavla, framför allt när det gäller teknisk information. En riktad attack kan här utnyttja att den som sitter inne

med känsliga uppgifter om militär teknik också med stor sannolikhet besöker webbplatser, läser e-post, följer länkar etc. om ämnesområdet är detsamma. Även avsändare kan förfalskas så att det verkar komma från en känd person eller organisation. Dessa webbplatser eller e-postbilagor kan vara preparerade med skadlig kod som sedan samlar information och skickas till förövaren. Ett stort svenskt företag inom försvarsindustrin utsattes under året för en liknande attack.

Datorer som ansluts till Internet blir nu inom några minuter utsatta för angreppsförsök. Syftet är att överta datorn och skapa en så kallad ”bot” eller ”zombie” som sedan utnyttjas tillsammans med andra i koordinerade angrepp eller spridning av spam. Man skall därför dagligen uppdatera sitt operativsystem, antivirus och viktiga applikationer.

Under året larmade FOI (Totalförsvarets forskningsinstitut) om att en ny sorts USB-minnen innehåller en teknik vid namn U3 som innebär en säkerhetsrisk. Tekniken innebär att skadlig kod kan planteras på en dator enbart genom att ansluta en sådan sticka.

Flera allvarliga sårbarheter har under året upptäckts i program som nyttjas flitigt inom Försvarsmakten, t.ex. Microsoft Word. Dessvärre tar det ofta lång tid innan programtillverkaren tillhandahåller rättningar. Dessa tillstånd av sårbarhet är nog tyvärr något vi måste lära oss att leva med. Detta ställer högre krav på den enskilde användaren att t.ex. inte klicka på misstänkta e-postbilagor. Mängden skadlig kod i e-post som stoppas fortsätter att minska. Fortfarande är det varianter av NETSKY som dominerar.

SPAM

Spam är ett ökande problem och många inom Försvarsmakten upplever det som en stor börda. Det var planerat att under året drifsätta ett så kallat spamfilter (ansvaret för att installera detta åvilar inte MUST SÄKK utan driftägaren). Detta har dock blivit fördröjt och kommer förhoppningsvis att genomföras fullt ut under 2007. ”Spammare” finner emellertid ständigt nya tekniker för att tränga igenom filter, nu senast genom att använda bilder istället för text. Detta gör att vi troligtvis aldrig helt blir av med problemet. De som är varsamma med att sprida sin adress till ”mailing”-listor och på webbplatser har i regel mindre problem med spam. Detta gäller även publicering av e-postadresser på www.mil.se.

FMCERT rekommendationer inför kommande år

- Var fortsatt vaksam mot misstänkt e-post. Öppna aldrig bilagor om du inte säkert känner avsändaren. Undvik att e-posta filer i formaten Word, Excel eller Powerpoint. Använd hellre formatet PDF såvida inte mottagaren ska redigera filen. Säkrast är dock alltid ren text.
- Rapportera alltid om du misstänker att din dator infekterats av skadlig kod. Var extra noga med handhavande av bärbara datorer. Se till att de är updaterade samt har aktuella antivirusprogram.
- Ha beredskap inför möjligheten att din mobiltelefon eller PDA smittats av skadlig kod. Tänk på vilken information du förvarar i dessa.

Tekniska utredningar

Under 2006 har 28 tekniska utredningar genomförts. Antal uppdrag ökar stadigt för varje år.
Utredningsmaterial har bl.a. varit hårddiskar, mobiltelefoner och USB-minnen. En stor mängd nätverkstrafik har spelats in från Försvarsmaktens nätverk i syfte att upptäcka intrångsförsök eller sekretessförlust. Analys av nätverkstrafik är mycket tidskrävande vilket har medfört en hård arbetsbelastning på denna funktion under 2006. Under 2007 kommer dock förmågan att öka men enbart inom ramen för MUST SÄKK.

Signalkontroll

Högkvarteret (MUST SÄKK SÄKA TI) inriktar teknisk signalkontroll av signalskyddet i telekommunikations- och informationssystem i syfte att klarlägga riskerna för obehörig åtkomst, störande eller manipulering av data, att systemen används enligt gällande regler samt kontroll av röjande signaler RÖS. Signalkontrollen inriktas i fred vid olika verksamheter som kräver hög eller långvarig sekretess och genomförs bl.a. genom avlyssning i syfte att klarlägga möjligheterna för främmande underrättelsetjänsts signalspaning att inhämta information, samt att bedöma vilken information som kan ha kommit obehörig till del. Teknisk signalkontroll är en integrerad del av signalskyddstjänsten.

Under 2006 har teknisk signalkontroll, tekniska utredningar och kontroll av röjande signaler (RÖS) genomförts enligt följande:

- DEMO-06 vår och höst,
- Utlandsstyrkan,
- Svensk ambassad,
- beredskapskontroll DAGNY,
- kontroll av röjande signaler vid flera garnisonsorter.

Övergripande resultat från genomförd verksamhet under 2006 visar på att det alltjämt finns stora brister vad avser hantering av sekretessbelagd information i etermedia. Under DAGNY kunde det konstateras att det, precis som under år 2005, är problem med bakgrundssamtal men också överhörning av samtal på DECT-telefoner. Vid DAGNY har det funnits anledning till allvarligare anmärkning om brister i sekretess vad avser signaltrafik i egna sambandssystem vilka delgivits FM Operative chef m.fl. för att kunna förbättra detta under 2007.

Detaljerad redovisning av resultat från genomförda verksamheter sker i hemliga årsredovisningen. I övrigt har ny kvalificerad utrustning införskaffats under året och utbildning har genomförts utomlands.

SÄKERHETSSKYDD

SÄKERHETSSKYDD

Allmänt

Säkerhetsskyddstjänsten arbetar bl a inom områdena:

- Informationssäkerhet
- Säkerhetsprövning
- Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)
- Information, utbildning, stöd och kontrollverksamhet
- Tillträdesbegränsningar
- Internationella säkerhetsskyddsavtal

Ledning

Central ledning

Den centrala ledningen i Högkvarteret av säkerhetsskyddstjänsten utövas av chefen för den militära underrättelse- och säkerhetstjänsten (C MUST) som också är Försvarsmaktens säkerhetsskyddschef. Ledningen av säkerhetsskyddstjänsten för Utlandsstyrkan och den territoriella säkerhetsskyddstjänsten utövas av Operativ chef i Insatsledningen.

Vid MUST säkerhetskontor är det i huvudsak tre av delprocessledarna som verkar inom säkerhetsskyddstjänsten, DPL Info/Utb, DPL Kontroller och Chefen säkerhetsskyddsavdelningen (säkerhetsskyddsprocessen).

Säkerhetsskyddsprocessen

- **Informationssäkerhet** skall förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras (riktighet) eller förstörs (tillgänglighet). I efterhand skall det gå att analysera informationsförlusten för att kunna minimera skadan (spårbarhet).
- **IT-säkerhet** är en del av informationssäkerheten. De tekniska förutsättningarna för IT-säkerhet skall kunna uppnås är dock så speciella att det vid den praktiska tillämpningen krävs särskilda regler och kompetens. Mer och mer av vår information hanteras i IT-system, varför detta område får en allt större betydelse.
- **Tillträdesbegränsning** innefattar fastställande av behov av tillträdesskydd, kontroll av att detta tillräckligt effektivt samt har en för ändamålet avvägd nivå.
- **Säkerhetsprövning** innebär att den enskildes lojalitet, pålitlighet, och sårbarhet bedöms. Säkerhetsprövning omfattar enligt 11§ säkerhetsskyddslagen även registerkontroll.
- **Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)** innebär att företag, som ej omfattas av säkerhetsskyddslagstiftningen, inför en upphandling som rör verksamhet som erfordrar skydd med hänsyn till rikets säkerhet skall förbindas att följa de säkerhetsskyddsbestämmelser som gäller för upphandlad myndighet. Denna förbindelse tecknas i ett säker hetsskyddsavtal. Avtalet skall i tillämpliga delar reglera för i uppdraget påkallade säkerhetsskyddsåtgärder.
- **Signalskydd** är en säkerhetsskyddsangelägenhet. Signalskyddsverksamhet bedrivs inom större delen av säkerhetskontoret.

Territoriell ledning

Under 2006 genomfördes en övergång av den territoriella ledningen från Militärdistriktscheferna till Operativ chef i Högkvarteret. Operativ chef leder den territoriella säkerhetsskyddstjänsten genom OPE J2 säkerhet- och samverkanssektioner i Malmö, Göteborg, Stockholm och Boden. De sektioner som inte fanns i en fd MD-stab fick mer utmaningar med rekrytering av personal, tillgång på lokaler och utrustning än de som i stort sett tog över de gamla und/säkavdelningarnas lokaler. Under året har de flesta problemen lösts ut. Operativ chefs övertagande av den territoriella ledningen innebar också en utmaning för ATK med en stor belastning på VB-funktionen. Bl.a fungerade säkerhetsrapporteringen från förbanden inledningsvis mycket dåligt. Huvuddelen av startproblemen har nu löst sig men det finns fortfarande utvecklingspotential.

Ledningen av säkerhetsskyddstjänsten för Utlandsstyrkan

Operativ chef i Högkvarteret leder säkerhetsskyddstjänsten för Utlandsstyrkan. Vid varje förbandsmission skall en utbildad säkerhetschef avdelas för ledning av den nationella säkerhetstjänsten inom kontingenten. Under 2006 har säkerhetschef för förbandsmissioner funnits inom KFOR, ISAF, UNMIL, UNIFIL och EUFOR.

Det skall dessutom finnas en IT-säkerhetschef för Utlandsstyrkan som skall biträdas av en biträdande IT-säkerhetschef vid varje förbandsmission. IT-säkerhetschef för Utlandsstyrkan har ännu ej tillsatts.

Rättsliga förändringar

Föreskrifter och interna bestämmelser

I föregående års årsrapport angavs att Försvarsmaktens interna bestämmelser (FIB 2006:2) om IT-säkerhet skulle träda i kraft den 15 mars 2006. De förändringar som gjordes var framförallt definitionen på produktägare och följdändringar med hänsyn till att militärdistrikten lades ner. Utöver denna författning har inga andra förändringar gjorts i de författningar som rör Försvarsmaktens säkerhetstjänst.

Informationssäkerhet

Med informationssäkerhet avses i Försvarsmakten:

- att informationen finns tillgänglig när den behövs
- att informationen är och förblir riktig
- att informationen endast är tillgänglig för dem som är behöriga att ta del av och använda den
- att hanteringen av informationen är spårbar.[1]

Försvarsmaktens informationstillgångar skall skyddas oavsett om de omfattas av någon sekretess eller inte. Detta innebär att Försvarsmakten har en vidare syn på informationssäkerhet än vad som anges i säkerhetsskyddslagstiftningen. Informationssäkerhet enligt säkerhetsskyddslagstiftningen tar enbart sikte på uppgifter som omfattas av sekretess enligt sekretesslagen och som rör rikets säkerhet.

[1] ”Beslut om Försvarsmaktens Informationssäkerhetspolicy” (HKV 2005-04-05 10 700:65482).

Tillämpning av Försvarsmaktens Informationssäkerhetsklasser

Försvarsmakten införde 2004 en indelningen av säkerhetsskydet i informationssäkerhetsklasserna HEMLIG/RESTRICTED, HEMLIG/CONFIDENTIAL, HEMLIG/SECRET respektive HEMLIG/TOP SECRET. Informationssäkerhetsklasserna skall användas i de fall uppgifterna omfattas av sekretess enligt sekretesslagen och kan medföra men för rikets säkerhet eller förhållandet till annan stat eller mellanfolklig organisation. Informationssäkerhetsklasserna skall även användas i de fall en hemlig handling har åsatts motsvarande beteckning av en utländsk myndighet eller mellanfolklig organisation.

HEMLIG/TOP SECRET

HEMLIG/SECRET

HEMLIG/CONFIDENTIAL

HEMLIG/RESTRICTED

HEMLIG
Enligt 8 kap.10 § sekretesslagen (1980:100)
2007-02-20
FÖRSVARSMAKTEN

HEMLIG
Enligt 2 kap. 2 § sekretesslagen (1980:100)
AV SYNNERLIGEN BETYDELSE FÖR RIKETS SÄKERHET
2007-02-20
Frågan om denna handlings utlämnande skall prövas av chefen för Försvarsdepartementet
FÖRSVARSMAKTEN

Under 2006 har den militära säkerhetstjänsten uppmärksammat att informationssäkerhetsklasserna använts för uppgifter som omfattas av sekretess men som inte rör rikets säkerhet. Användningen har i två fall rört myndigheter som Försvarsmakten, vad avser säkerhetsskydd, utövar tillsyn över. Inom Försvarsmakten har märkning med informationssäkerhetsklass vid flera tillfällen kommit att användas för uppgifter som omfattas av sekretess men som inte skall placeras i informationssäkerhetsklass.

Att informationssäkerhetsklasserna enbart används för de syften som avses i Försvarsmaktens föreskrifter om säkerhetsskydd[2] är viktigt för att inte uppgifterna i onödan skall ges det skydd som säkerhetsskyddslagstiftningen avser. Enbart uppgifter placerade i informationssäkerhetsklass skall ges ett säkerhetsskydd. Konsekvenserna av att felaktigt placera uppgifter i informationssäkerhetsklass är ökade kostnader, risk för missförstånd vid informationsutbyte mellan myndigheter eller mellan Sverige och andra nationer eller organisationer.

Exempel på en incident under 2006

En försvarsmaktsanställd person har av Försvarsmaktens personalansvarsnämnd ålagts en disciplinpåföljd enligt 14 § lagen (1994:260) om offentlig anställning (LOA) i form av löneavdrag.

Personen skall ha skapat, bearbetat och lagrat ett trettiotal dokument, under tiden mellan september 2005 och maj 2006, som innehöll uppgifter som omfattades av sekretess enligt sekretesslagen (1980:100) och som rörde rikets säkerhet.

[2]FFS 2003:7, http://www.hkv.mil.se/ffs/attachments/ffs2003-7.pdf

Genom detta förfarande har personen överträtt gällande säkerhetsbestämmelser och därmed gjort sig skyldig till en tjänsteförseelse. Med hänsyn till omfattningen och arten av överträdelserna bedömde personalansvarsnämnden förseelsen som allvarlig.

Trots att chefen för personens organisationsenhet förordade att personen skulle tilldelas en varning, fann personalansvarsnämnden att tjänsteförseelsens art och omfattning medförde att en annan påföljd än löneavdrag inte kunde komma i fråga.

Riksrevisionens granskning av Försvarsmaktens styrning av informationssäkerhetsarbetet

Under slutet av 2005 påbörjade Riksrevisionen granskningen. Under mitten av 2006 presenterade Riksrevisionen en Revisionsrapport över granskningen. Den huvudsakliga normkällan för de bedömningar som Riksrevisionen gjorde var från standarden Ledningssystem för Informationssäkerhet (SS 627799 och SS-ISO/IEC 17799). Riksrevisionens samlade bedömning är att Försvarsmakten har på en övergripande nivå ett samlat och strukturerat förhållningssätt till informationssäkerhetsfrågor. Under året har myndigheten påbörjat ett arbete med att vidta åtgärder för att följa de rekommendationer som Riksrevisionen ger i revisionsrapporten. Detta arbete beräknas vara slutfört under 2007.

Ett exempel på en sådan åtgärd är att militära underrättelse- och säkerhetstjänstens Säkerhetskontor skall utveckla arbetet med en tydligare central analys och sammanställning av de riskanalyser som genomförs på lokal nivå.

Skydd för landskapsinformation

Den militära säkerhetstjänsten lämnar kontinuerligt stöd vid sekretessbedömning rörande landskapsinformation.[3] Landskapsinformation rör ofta förhållanden som förändras långsamt och därför har lång giltighet. Sekretessbehovet för landskapsinformation kan därför inte utgå från dagens hotbild. Har informationen väl en gång släppts fri finns informationen tillgänglig vid en förändring av hotbilden.

Förändrad hotbild och den tekniska utvecklingen har medfört att det finns ett behov av att se över skyddet av landskapsinformation. Regeringen har 2006 gett Försvarsmakten i uppdrag att se över tillståndsprocessen rörande beslut enligt förordning (1993:1745) om skydd för landskapsinformation. I uppdraget ingår även att se över förordningen utifrån den utveckling som skett under senare år, till exempel när det gäller förändrad hotbild, digitalt lagrad information och spridning av denna.

[3]Med landskapsinformation avses lägesbestämd information om förhållanden på och under markytan samt på och under sjö- och havsbotten. För landskapsinformation finns bestämmelser om krav på tillstånd för sjömätning, för fotografering och liknande registrering från luftfartyg, upprättande av databaser med landskapsinformation, krav på tillstånd för spridning av flygbilder, av kartor samt av andra sammanställningar av landskapsinformation. Bestämmelserna avser att förhindra att landskapsinformation som kan antas medföra skada Sveriges totalförsvar upprättas och sprids.

Internationella säkerhetsskydds-överenskommelser

Allmänt

Sverige är beroende av att ha giltiga och uppdaterade säkerhetsskyddsöverens-kommelser med ett flertal länder och organisationer. Anledningen till detta är att svenska myndigheter och företag på ett säkert sätt skall kunna utbyta sekretessbelagd information med myndigheter och företag i andra länder samt med internationella organisationer som t.ex. Nato. Informationsutbytet är ofta påkallat av internationella försvarsmaterielprojekt, säkerhetskänsliga projekt inom Europeiska Unionen eller svenskt deltagande i internationella operationer och övningar. Som exempel kan nämnas svenska exportsatsningar rörande JAS 39 Gripen samt deltagande i operationer som KFOR och ISAF. Den militära säkerhetstjänsten förhandlar dessa överens-kommelser efter bemyndigande från regeringen till vilken även förhandlingsresultaten redovisas. Förhandlingarna innehåller en genomgång av de deltagande ländernas lagstiftning på området och en anpassning av avtalstexten efter detta. Ofta tecknas avtalen på regeringsnivå. Under året har förhandlingar om bi- och multilaterala säkerhetsskyddsöverens-kommelser skett med ett flertal länder. Den militära säkerhetstjänsten deltar också kontinuerligt i säkerhetsarbetet inom samarbetsavtalet rörande den europeiska försvarsindustrins omstrukturering, EDIR FA (det s.k. sexnationsavtalet), vilket också berör bilaterala säkerhetsfrågor med de deltagande länderna. Genom att Sverige är den ledande nationen i den kommande nordiska snabbinsatsstyrkan (NBG) inom ramen för EU:s krishantering, har den militära säkerhetstjänsten fått en samordnande roll gentemot de övriga deltagarländernas säkerhetstjänster.

I det utbyte av hemliga uppgifter som sker med andra länder och internationella organisationer inträffar det ibland att hemliga uppgifter röjs eller förloras. I dessa fall är det av yttersta vikt att frågan hanteras korrekt i och med att det kan påverka Sveriges utlandsförbindelser och Sveriges trovärdighet i internationella sammanhang. En viktig princip i dessa fall är att upprättaren av information som kan ha förlorats eller blivit röjd ska informeras så snart som möjligt. Informationen skall lämnas även om inte ärendet har utretts klart för att undvika att störa relationen med upprättaren ytterligare. Genom internationella säkerhetsskyddsöverenskommelser som Sverige tecknar med andra länder regleras hur informationen om incidenter skall lämnas och genom vilka kanaler. I Försvarsmakten skall denna information alltid gå via den militära säkerhetstjänsten vid Försvarsmaktens högkvarter.

IT-säkerhet

Handbok för Försvarsmaktens säkerhetstjänst, Informationsteknik (H SÄK IT) 2006

Den 1 juni 2006 började Försvarsmakten tillämpa en ny handbok för Försvarsmaktens säkerhetstjänst, Informationsteknik (H SÄK IT). Handboken ersatte bl.a. föregångaren från 2001.

H SÄK IT riktar sig främst till Försvarsmaktens ledning, chefer för organisationsenheter, produktansvariga, säkerhetschefer, IT-säkerhetschefer, biträdande IT-säkerhetschefer, IT-säkerhetsansvariga och IT-chefer. Handboken kan även i tillämpliga delar användas för de myndigheter som Försvarsmakten utövar tillsyn över.

H SÄK IT innehåller ett flertal nyheter, bl.a. beskrivs innebörden av Försvarsmaktens informationssäkerhetspolicy.

För att säkerställa att säkerhetsrelaterade frågor i och kring ett IT-system beaktas är det nödvändigt att det finns en fungerande organisation. Med hänsyn härtill beskrivs en del av de aktörer som är av betydelse för IT-säkerhetsarbetet.

En relativt stor del av handboken upptas av en beskrivning över de säkerhetsfunktioner som ger skydd åt IT-system. En av dessa säkerhetsfunktioner är skydd mot skadlig kod.

För att myndighetens verksamhet skall kunna få det IT-stöd som behövs i utvecklings-, inriktnings, produktionsinsats- liksom underrättelse- och säkerhetstjänstarbetet, måste ett antal analyser genomföras. Därför beskrivs i handboken analyser, planer och instruktioner som är av betydelse för Försvarsmaktens IT-säkerhet. Exempel på sådana analyser är hot-, risk- och sårbarhetsanalyser och säkerhetsmålsättningar.

Ett stort stöd för verksamheten borde även vara att den författningstext som är av betydelse för Försvarsmaktens IT-säkerhet på ett tydligt sätt kommenteras.

Handboken har publicerats på Försvarsmaktens intranät emil. Detta ger Försvarsmaktens personal möjlighet att nå den största delen av de handlingar och författningar som handboken refererar till. Ur ett tillgänglighetsperspektiv är detta en stor förändring gentemot möjligheterna som gavs vid den förra handbokens publicering. Idéen är att H SÄK IT 2006 kontinuerligt skall uppdateras och den senaste versionen skall alltid gå att finna på säkerhetstjänstens portal i emil.

Tillträdesbegränsning

Allmänt

Under 2006 har det, i likhet med de senaste åren, funnits ett allmänt förhöjt hot mot förråd med militära skjutvapen och ammunition. Detta hot bedöms komma att kvarstå på samma nivå under 2007. Med anledning av Försvarsmaktens fortsatta omstrukturering bedöms att risken för tillgrepp av kapitalvaror m m kommer att kvarstå. Med anledning av ovanstående är det väsentligt att kontroller av tillträdesbegränsning och av förvaring, hantering och transporter av skyddsvärd materiel, inkl skjutvapen och ammunition genomförs såväl lokalt, regionalt som centralt under 2007.[4]

[4]Se FFS 2000:10, FIB 2000:1 samt FIB 2005:2.

Vapen och ammunition

Genom polisiära åtgärder 2005 upphörde den ”egentillverkning” av kulsprutepistolliknande vapen som pågått sedan mitten av 1990-talet. Detta, tillsammans med att möjligheterna att tillgripa Försvarsmakten skjutvapen och ammunition ytterligare har försvårats, bedöms kunna resultera i att hot kan komma att riktas mot Försvarsmaktens personal. Ett hot som då kan riktas mot personal som arbetar i förråd med vapen eller ammunition eller som har tillgång till nycklar eller koder till sådana förråd. Hot bedöms också kunna komma att riktas mot personal som genomför transporter av skjutvapen och ammunition.

Hotet bedöms vara störst vid arbeten som bedrivs i förråd utanför militärt inhägnat och bevakat område, detta oavsett vilken typ av vapen eller ammunition som förvaras i dessa förråd. Även verksamhet som bedrivs inom militärt, inhägnat och bevakat område kan komma att beröras.

Detta understryker vikten av att det avdelas personal för bevakning och skydd vid arbete i vapen- och ammunitionsförråd i minst den omfattning som framgår av gällande regelverk samt att transporter av skjutvapen och ammunition genomförs som skyddade transporter i de transportnivåer m m som framgår av bl.a. H SÄK VapAm 2000.[5]

Under 2007 och ytterligare ett antal år framöver kommer omstruktureringen av Försvarsmakten och den därmed sammanhängande avvecklingen främst av ammunition, men till del även skjutvapen, att ställa stora krav på bevakning och skydd i samband med arbete i förråd och vid transporter av skjutvapen och ammunition. Den nedåtgående trenden avseende vapenförluster genom stöld har under 2006 förstärkts, dock återstår en del innan ”nollvisionen” är uppnådd. Antalet förkomna vapen kan komma att öka maa av fördjupad inventering och avslutande av undersökningar avseende under tidigare år befarade, men ej anmälda, förluster.

Förlust av vapen

Sammanställning av förkomna vapen 1998-2006

Typ/År	Pistol	Kpist	Gevär	Ak 4	Ak 5	Totalt
1998	0	1	2	8	18	29
1999	8	3	7	12	1	31
2000	3	4	4	11	4	26
2001	3	4	3	8	2	20
2002	0	1	0	9	0	10
2003	1	2	0	11	1	15
2004	1	1	6	6	0	14
2005	2	0	0	6	8	8
2006	10[6]	1	3	1	0	15[7]

Summan förkomna vapen baserar sig på antalet förkomna kompletta vapen adderat med antalet förkomna huvuddelar (vapen utan vital del).

[5]H SÄK VapAm 2000, kap 4 (bl a 4.1.2—4.1.6) samt kap 5.
[6]Varav 7 signalpistoler och 1 luftpistol.
[7]Härutöver har 2 vapen som anmälts stulna återkommit/återfunnits.

Hemvärnets vapenförvaring

Mot bakgrund av att den s k undre världen bedöms ha viss brist på bl a automatvapen bedöms att risken för tillgrepp av bostadsförvarade vapen är fortsatt hög. Under 2007 kommer det att ske en förändring avseende förvaringen av nycklar till patronlägeslås till hemvärnsmännens AK 4. Istället för att, som tidigare, den enskilde hemvärnsmannen ska förvara nyckeln till patronlägeslåset till sin AK 4 buren eller gömd i bostaden, kommer patronlägeslåsnycklarna att samlas ihop grupp- eller plutonsvis och förvaras inlåsta i säkerhetsskåp, motsv.[8] Härutöver kommer rutinerna vid antagningsförfarandet till hemvärnet att förändras och förbättras varvid bl a särskilda frågeformulär m m kommer att nyttjas vid samtal med den sökande.[9]

2006-07-01 trädde en del förändringar i vapenlagen i kraft. Förändringarna innebar bl a en skyldighet för polisen att omedelbart underrätta Försvarsmakten om en person som tillhör hemvärnspersonalen är olämplig att inneha skjutvapen. Underrättelseskyldigheten innefattar såväl brottsmisstankar som fällande domar och uppgifter som polisen erhållit från läkare.

I syfte att skapa rutiner för samverkan mellan polis och Försvarsmakten i ärenden av denna art har Högkvarteret (inledningsvis FÖRBE RIKSHV och MUST och senare även OPE) haft möten med polisen.

Likaså har handlingsregler m m för hantering inom Försvarsmakten av sådana ärenden utarbetats.[10]

Kontroller avseende vapen- och ammunitionshantering

Mot bakgrund av erfarenheter från 2006 och mot vad som bedöms kunna ske under 2007 är det väsentligt att alla organisationsenheter överser tillämpningen av gällande bestämmelser avseende vapen- och ammunitionshantering och att omedelbara åtgärder vidtages om hotbilden

förändras, d v s om hotet bedöms öka. Likaså är det väsentligt att garnisonschefer m fl, genomför kontroller av att gällande bestämmelser avseende förvaring, hantering och transport av skjutvapen och ammunition följs, inom hemvärnet såväl som vid övrig verksamhet.

Larm 2000

Driftsättningen av larmsystem 2000 för friliggande ammunitionsförråd skedde under 2003. Under 2005 och 2006 har

[8]Dessa ändrade förvaringsrutiner är en direkt följd av händelsen sommaren 2006, då en hemvärnsman i Täby sköt skarpt inom bebyggt område och sedemera även tog sitt eget liv.

[9]Ytterligare detaljer framgår av HKV skrivelse - Beslut avseende administration av hemvärnssoldater samt hantering av hemvärnssoldaternas tilldelade vapennycklar, 2006-11-07, 19 170:76685 och med tillägg 2006-12-14, 19 170:79703.

[10]HKV skrivelser- Polisens och Försvarsmaktens åtgärder vid omhändertagande av militärt hemvärnsvapen, 2006-06-12, 10 740:69378, samt Operativ chefs beslut avseende Försvarsmaktens hantering och åtgärder vid anmälan om att en person tillhörig hemvärnets personal är olämplig att inneha skjutvapen, 2007-01-22, 10 740:61296.

provinstallationer av larm 2000 skett i bergförråd och kommer att fortsätta under 2007.

Övriga larm

Försvarsmakten har, i form av ett ”gammalt arv”, många varierande typer av larm vid förråd och andra anläggningar. Dessa larm genererar, i icke ringa omfattning, fellarm som resulterar i att insatsstyrkor i många fall måste genomföra fysiska kontroller vid objekten.

Försvarsmakten kommer efter hand att byta ut eller modifiera dessa larm till Larm 2000 eller till varianter av detsamma.[11]

Låsbyten på dörrar vid vissa ammunitionsförråd

FORTV har sedan några år haft i uppdrag att vidareutveckla låsenheter för dörrar vid vissa av försvarsmaktens ammunitionsförråd. Under 2005 genomfördes provinstallationer av de nya låsen vid några ammunitionsförråd i södra Sverige. Utvärdering har skett och låsbyten vid flera ammunitionsförråd har skett under 2006 och kommer att fortsätta under 2007.

Legitimationshandlingar

Den 1 januari 2002 trädde *Försvarsmaktens interna bestämmelser (FIB 2001:4) om legitimationshandlingar m m* i kraft. FMLOG upphandling av tjänstekort och identitetskort m m slutfördes under december 2004. Det företag som nu tillverkar tjänstekort m m åt bl a Försvarsmakten är SETEC TAG, AB. Alla Försvarsmaktsanställda tilldelas tjänstekort. Dessa tjänstekort innehåller magnet-

[11]Detta bl a som ett resultat av den s k Bevakningsutredningen.

remsa, datachip samt s k Mifare-slinga, detta bl a i syfte att i kunna nyttja tjänstekorten i automatiska passersystem.

Härutöver tillverkar SETEC TAG AB identitetskort för militärpolis, legitimationsbevis för hemvärnets personal, värnpliktskort, m m åt Försvarsmakten. Med anledning av att utseendet bl a på de nya tjänstekorten, på identitetskorten för militärpolis m fl inte tillfullo överensstämmer med *Försvarsmaktens interna bestämmelser (FIB 2001:4)* om legitimationshandlingar m m kommer denna författning att skrivas om under våren 2007.

Skyddade transporter, främst avseende hemlig materiel och s k skyddsvärd materiel

I Försvarsmaktens interna bestämmelser (FIB 2005:2) om säkerhetsskydd och skydd av viss materiel regleras hur hemlig och s k skyddsvärd materiel skall transporteras. Författningen har under hösten 2006 reviderats och kommer att utges som ny FIB. I kommande utgåva av H SÄK Skydd kommer även skyddade transporter att beröras.

Nyttjande av försvarsmaktsanställda civila skyddsvakter

I syfte att, vid behov, kunna nyttja försvarsmaktsanställda civila skyddsvakter hemställde Försvarsmakten häromåret om att regeringen skulle göra vissa ändringar i 5, 14 och 18 §§ Förordningen (1990:1334) om skydd för samhällsviktiga anläggningar m m, samt i 1 § Förordningen (1992:98) om användande av skjutvapen vid vakttjänst inom Försvarsmakten.

Dessa förändringar skedde våren 2006 och trädde i kraft 2006-04-30. Förändringarna innebär bl a att begreppet *militär personal* har ersatts, vad avser Försvarsmakten, av *myndighetens personal.*[12]

Transportskydd före

Transportskydd efter

[12]För ytterligare detaljer se Förordningen (1990:1334) om skydd för samhällsviktiga anläggningar m m inkl förordning (2006:152) om ändring av densamma, samt Förordning (1992:98) om användande av skjutvapen vid vakttjänst inom Försvarsmakten inkl förordning (2006:153) om ändring av densamma.

Nyttjande av civila vakt- och bevakningsbolag som transportskyddsstyrka och för bevakning vid arbete i ammunitionsförråd m m

I syfte att minska behoven av att ta värnpliktiga i anspråk för transportskyddsverksamhet och bevakning vid arbete i förråd, beslöt Högkvarteret 2003 att pröva möjligheterna att nyttja civila bevakningsbolag. FMLOG gavs i uppdrag att upphandla tjänsten och slöt hösten 2005 avtal med dåvarande Falck Security AB, numera Group 4 Securicor (G4S).

Bevakningsutredning

I januari 2006 fick chefen för Försvarsmaktens tekniska skola (C FMTS) i uppdrag av Högkvarteret (HKV FÖRBE PROD) att utreda försvarsmaktens bevaknings- och transportskyddstjänst.[13] Utredningen skulle bl a genomlysa och ta fram förslag på dimensionering, utrustning och metoder samt belysa möjligheten att nyttja civil leverantör för delar av verksamheten och möjligheterna till rationaliseringar syftande till ekonomiska besparingar.

Under våren 2006 genomfördes ett antal arbetsdagar med deltagande personal från FMTS, HKV MUST, HKV OPE J 2 SäkSam, HKV OPE ATK, FMLOG och FMUndSäkC.
2006-06-29 slutredovisade C FMTS utredningen.[14]
Under hösten 2006 har utredningens slutsatser och förslag bearbetats och resulterat i att Högkvarteret har fattat beslut om ansvarsfördelning, uppgifter m m för det fortsatta arbetet.[15] Mycket kortfattat kan sägas att Arméinspektören (AI) ges i uppdrag att funktionsutveckla bevakningsverksamheten, att operativ chef även fortsättningsvis skall insatsleda bevakningstjänsten, att övriga enheter inom Högkvarteret på olika sätt skall ge erforderliga riktlinjer och styrningar samt stödja verksamheten, att FMLOG skall genomföra viss upphandling, att FMUndSäkC skall ge AI visst stöd och att det inom varje organisationsenhet skall avdelas en funktionsföreträdare för för bevakning och transportskydd, m m. Mycket av arbetet avses genomföras under 2007.

Säkerhetsprövning

Allmänt

Infiltration kallas metoden att placera eller värva personer på viktiga befattningar i syfte att spionera, sabotera, sprida vilseledande information, uppvigla eller i övrigt bedriva säkerhetshotande verksamhet mot viktiga funktioner som rör rikets säkerhet.

Säkerhetsprövning är en sammanfattande benämning på åtgärder som skall klarlägga om en person kan antas vara lojal mot de intressen som skyddas i säkerhetsskyddslagen och i övrigt pålitlig från säkerhetssynpunkt.

Det är chef för organisationsenhet som ansvarar för att säkerhetsprövning genomförs.
En väl genomförd säkerhetsprövning kräver ett nära samarbete mellan chefer och deras företrädare för personal-, ekonomi- och säkerhetsfunktionerna. Säkerhetsprövning är en kontinuerlig process. Chef har ett ansvar för att

[13]HKV skrivelse – Utredningsuppdrag avseende bevakning och transportskydd, 2006-01-18, 10 900:60321.
[14]FMTS skrivelse – Bevakningsutredningen, 2006-05-30, 10 900:20587.
[15]HKV skrivelse – Beslut avseende ansvarsfördelning för bevakning och transportskydd i Försvarsmakten, 2006-12-20, 02 300:78894.

bedöma och följa upp individens lojalitet, pålitlighet och sårbarhet såväl inför som under anställningen eller deltagande i verksamhet i en miljö där säkerhetshot kan förekomma. Härutöver bör säkerhetsskyddsåtgärder genomföras när en anställning eller ett deltagande i verksamhet upphör.

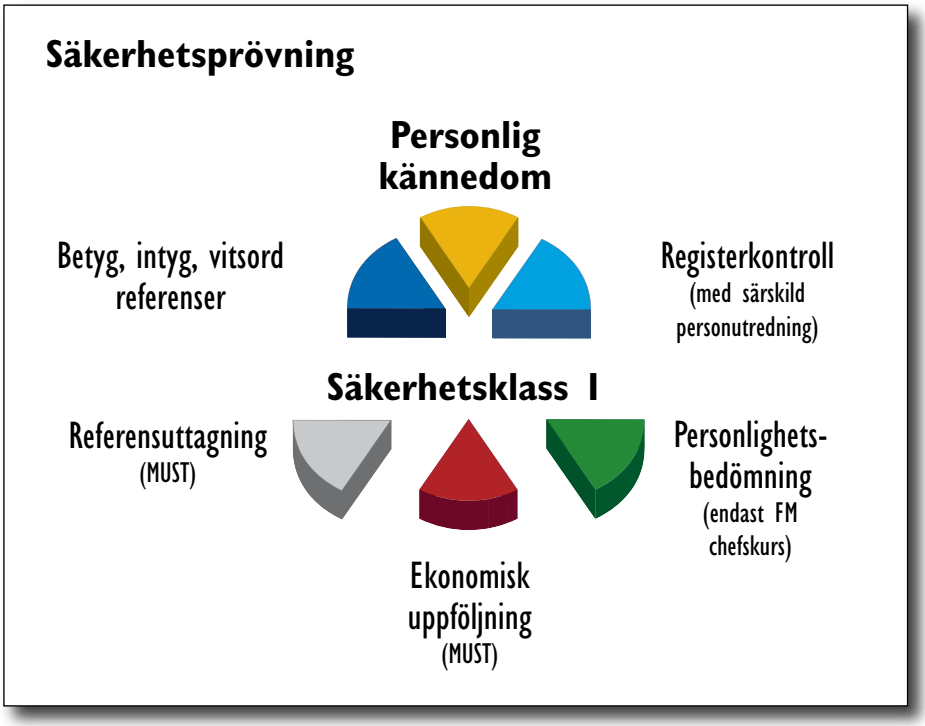
Vid bedömningen av individers pålitlighet, lojalitet och sårbarhet används främst följande indikatorer:

1. Besvikelse, är individen besviken exempelvis beroende på utebliven befordran, låg lön, brist på uppskattning eller är individen kanske har en bitter personlighet?
2. Ekonomi, har individen stora skulder, spelmissbruk eller för dyrt leverne eller liknande?
3. Social misär, lever individen i social misär, med missbruk av alkohol eller stimulantia eller har en psykisk stör ning, eller särdrag i sin personlighet.
4. Har personen olämpliga kontakter, exempelvis med kriminella,främmande underrättelsetjänster, utomparlamenta riska grupperingar eller grupperingar som vill omstörta samhället med våld.

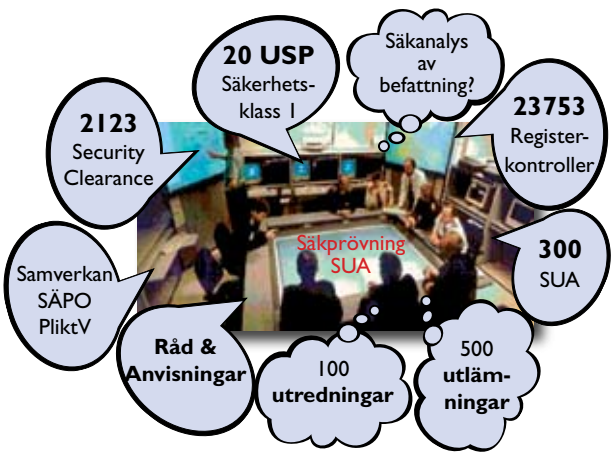
Säkerhetsprövning innefattar från säkerhets- skyddssynpunkt följande olika delmoment:

- säkerhetsanalys av anställning (befattning) eller deltagande i verksamhet
- inplacering av befattningen i säkerhetsklass
- intervjuer för att klarlägga eventuella sårbarhet och brister i pålitlighet och lojalitet
- referenstagning (och personlig kännedom) för att klarlägga eventuella sårbarhet och brister i pålitlighet och lojalitet
- Bedömning av betyg och intyg för att klarlägga eventuella sårbarhet och brister i pålitlighet och lojalitet
- registerkontroll samt vid behov särskild personutredning,
- vid behov ekonomisk kontroll och psykologisk personlighetsbedömning för att klarlägga eventuella sårbarhet och brister i pålitlighet och lojalitet samt skyddssamtal
- säkerhetsskyddsbeslut i personärende,
- uppföljning under anställning eller deltagande i verksamhet

Särskilt viktig är den sista punkten, säkerhetsprövningen är en kontinuerlig process som skall pågå under hela anställningen.

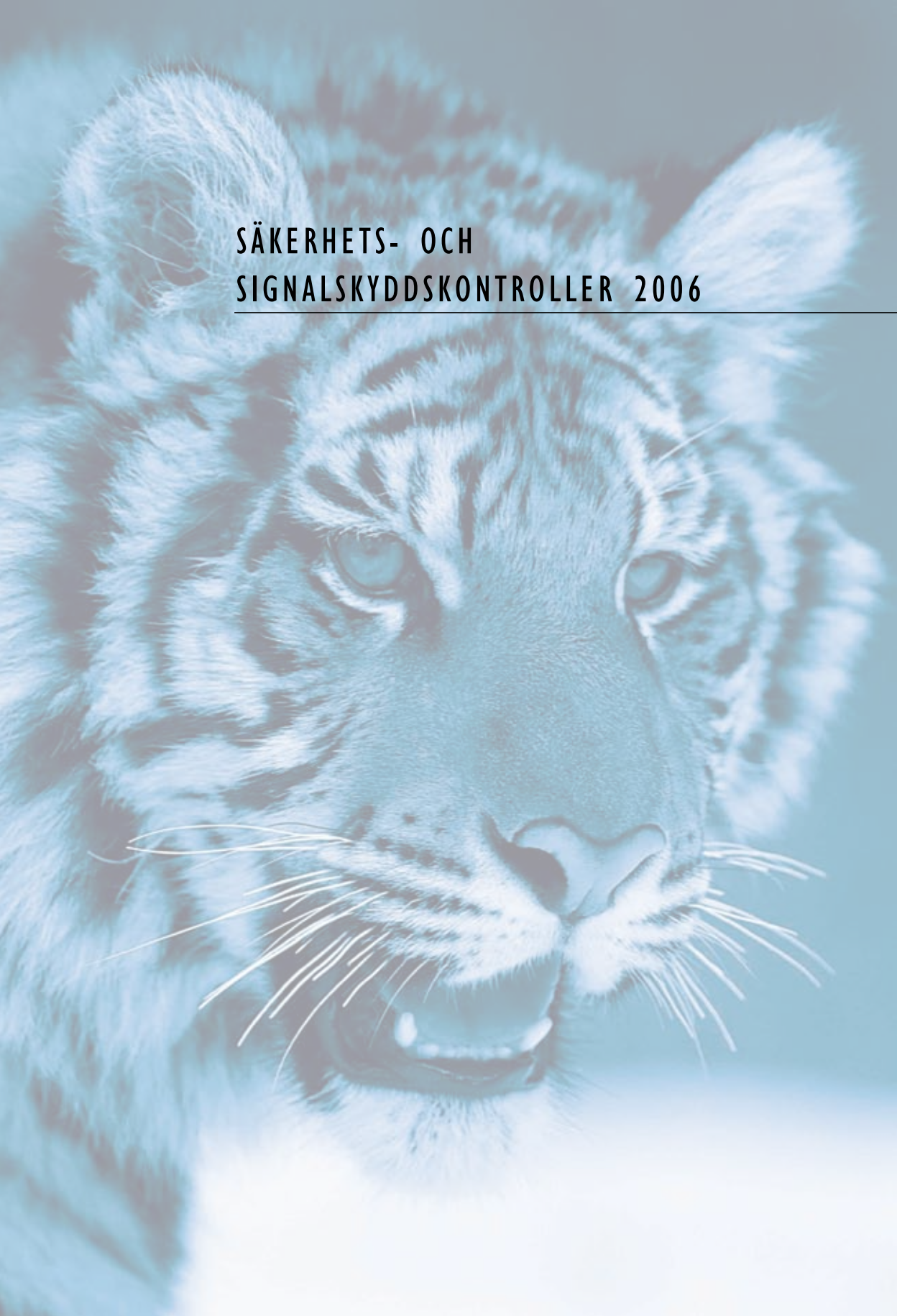


Genomförd säkerhetsprövning under 2006



Inriktning av säkerhetsprövning under 2007

- Utvecklad säkerhetsprövning
- Fortsatt utveckling av metodik samt RK-rutin i IS UndSäk
- Säkerhetschefskurs (SOK)
- Skyddssamtal
- SUA
- Uppföljning
- Stöd
- Säkanalys av befattning
- Slutgör förnyade registerkontroller
- Framtagning av H SÄK SKYDD
- Framtagning av H SÄK SUA



SÄKERHETS- OCH SIGNALSKYDDSKONTROLLER 2006

SÄKERHETS- OCH SIGNALSKYDDS-KONTROLLVERKSAMHETEN 2006

Allmänt

För att Försvarsmakten och totalförsvaret i övrigt ska ha möjlighet att uppfylla aktuella säkerhetsbestämmelser till skydd för rikets säkerhet genomför MUST Säkerhetskontor ett stort antal säkerhets- och signalskyddskontroller årligen. MUST SÄKK Delprocess Kontroller ansvarar för denna kontrollverksamhet som främst sker i Sverige men även, med hög prioritet, utomlands på de platser där Försvarsmakten löser uppgifter med exempelvis utlandsmissioner och försvarsattachéavdelningar. Utöver detta genomför MUST SÄKK säkerhets- och signalskyddskontroller vid vissa myndigheter under Försvarsdepartementet samt en myndighet under Finansdepartementet. MUST SÄKK ansvarar och genomför dessutom ett omfattande signalskyddskontrollarbete mot samtliga myndigheter inom totalförsvaret.

Det är viktigt för kontrollverksamheten att i dialog med myndigheternas och förbandens säkerhetsorganisationer utvisa om organisationen uppfattat och följer gällande säkerhetsbestämmelser.

På detta sätt utgör kontrollprocessen ett stöd till den lokala säkerhetstjänsten i syfte att myndigheten eller förbandet ständigt ska ha initiativet och i tid kunna vidta korrekta säkerhets- och signalskyddsåtgärder för att förebygga och effektivt kunna möta nya hot och risker.

FMGL Kontrolläge

I strävan att övergripande åskådliggöra säkerhetsbrister inom Försvarsmakten samt de myndigheter där Försvarsmakten har tillsynsansvar gällande säkerhetstjänsten samt signalskyddet har under 2006 MUST SÄKK upprättat det så kallade FM Kontrolläge.

Kontrolläget redovisas veckovis i Försvarsmaktens gemensamma lägesbild (FMGL) och belyser de brister i säkerhetsskyddet som uppdagats vid de senaste säkerhets- och signalskyddskontrollerna.

Därmed möjliggör FMGL Kontrolläge att säkerhetsbrister uppmärksammas på bredd inom Försvarsmakten samt att Försvarsmaktens högsta ledningen omedelbart orienteras om viktigare delar av aktuellt säkerhetsskyddsläge.

Utlandsverksamheten

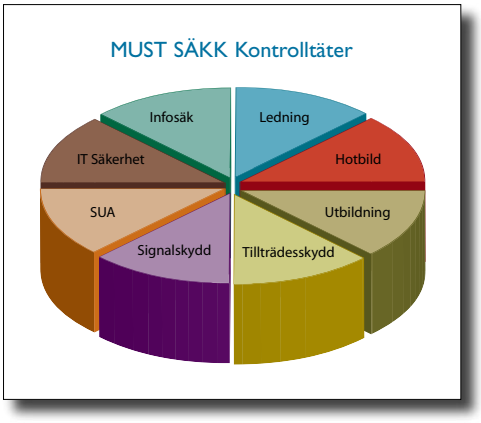
Under 2006 har, för kontrollverksamheten, ett starkt fokus legat på utlandsstyrkan. MUST har vid dessa kontroller haft ett nära samarbete med OPE J2 samt ATK, vilket givit resultatet att upptäckta säkerhetsbrister förhållandevis snabbt kunnat åtgärdats. Flertalet kontroller har genomförts vid de svenska truppmissionerna i Liberia, Afghanistan, samt Kosovo. Kontrollerna har inriktats

mot att nå även de geografiskt yttersta delarna av förbanden; vilket visat sig nödvändigt för att få en relevant uppfattning om det verkliga säkerhetsläget.

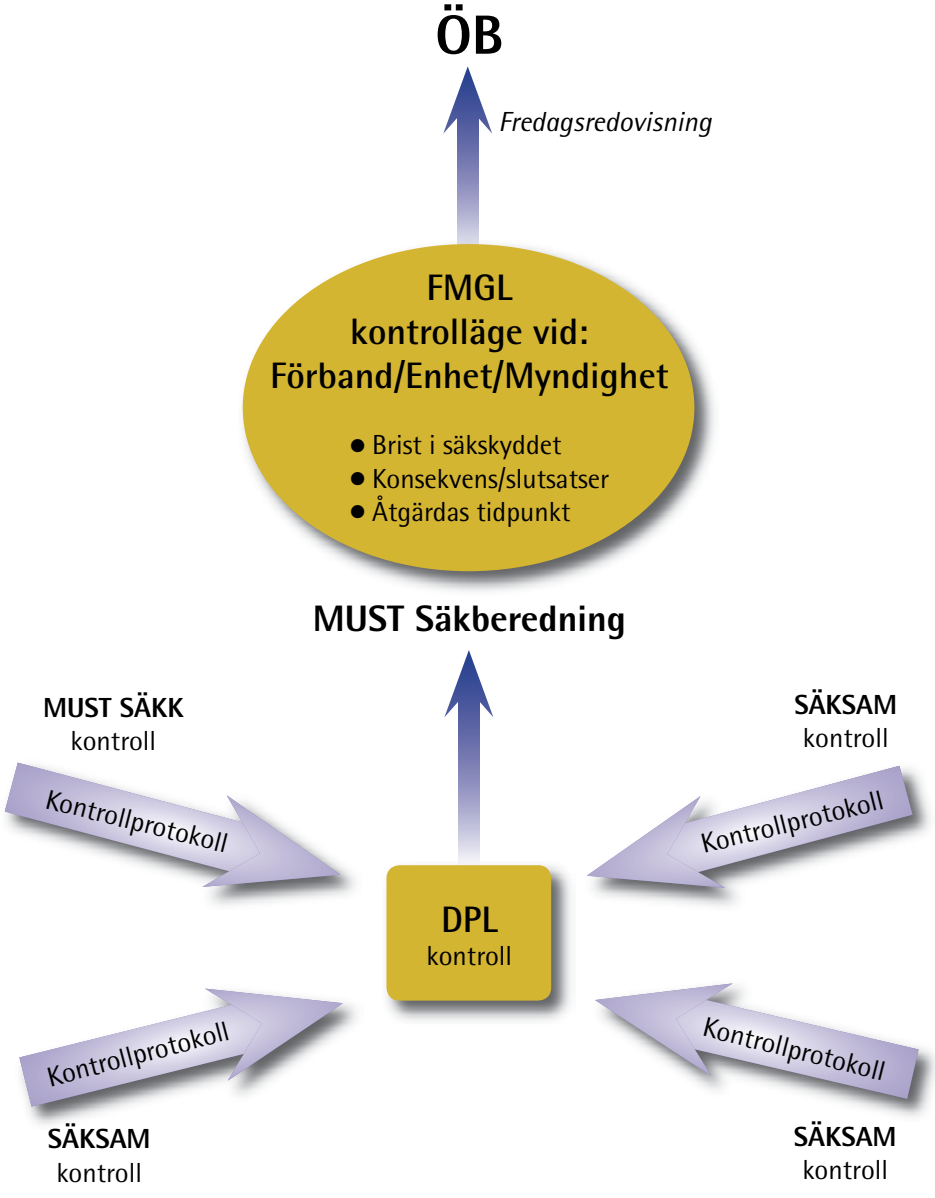
Strävan är att MUST så tidigt som möjligt, efter nedrotation av ett förband till missionsområdet, genomföra säkerhets- och signalskyddskontroll. Detta för att tidigt i missionen ge förbandets säkerhetsorganisation stöd inför kommande tjänst.

MUST SÄKK:s säkerhets- och signalskyddskontroller utomlands har, utöver utlandsstyrkan, genomförts vid försvarsavdelningarna i Frankrike och USA samt vid ”Ubåt i Västerled” det vill säga HMS Gotland i San Diego vilken genomför övningsverksamhet tillsammans med US Navy längs den amerikanska västkusten.

Den internationella dimensionen inom Delprocessen kontroller kommer att vara prioriterad.



Försvarsmaktens kontrollläge



Kontroll av FMV säkerhets- och signalskyddstjänst samt kontroll av FM HKV MUST

Utöver kontroller av FM utlandsverksamhet har MUST SÄKK genomfört grundkontroll av FMV centrala delar.

MUST SÄKK har även tillsett att det genomförts en omfattande grundkontroll av säkerhets- och signalskyddstjänsten vid HKV MUST. Kontrollpersonen har vid detta tillfälle hämtats ur enheten utanför MUST.

Kontroll av territoriet

Under 2006 har OPE J2 fyra Säkerhets- och samverkanssektionerna (SäkSam-sekt) i Malmö, Göteborg, Stockholm och Boden tagit över det regionala kontrollansvar som tidigare var ålagt de nedlagda Militärdistrikten.

SäkSam-sekt har under 2006 kraftsamlat sina säkerhetskontroller av garnisoner och förband till hösten och vintern. Ett flertal garnisoner, centrum och skolor har kontrollerats och rapporterats in till MUST SÄKK för redovisning i FMGL

Kontrollresultaten har varierat; dock har signifikant under 2006, varit det direkta stöd som SäkSam-sekt givit de kontrollerade att snabbt ombesörja omedelbara åtgärder för att stärka säkerhetsskyddet.

Admininstrativa signalskyddskontroller av civila myndigheter

Utöver att signalskyddskontroller ingår som en betydande del i kontrollverksamheten, både vid utlandskontroller och vid kontroller på territoriet, har explicita signalskyddskontroller genomförts vid civila myndigheter i ett antal län.

Brister förekommer men överlag är resultaten bra vid de myndigheter som berörts.

Delprocess Kontroller (DP Ktrl)

Både chefer och den enskilde är ansvariga för att säkerhetsskyddskontroller genomförs regelbundet. Den enskilde är enligt sin lokala säkerhetsorganisations närmare bestämmelser ansvarig för kontroll av egen arbetsplats och arbetsområde.
Vid säkerhets- och signalskyddskontroller är det av vikt att kontroll av hotbildsuppfattning görs i syfte att avstämma denna gentemot FM gällande hotbildsbedömning. Kontroll och avstämning av hotbildsuppfattning görs på alla kontrollerade nivåer och funktioner.

Kontroller genomförs vanligen som föranmälda kontroller men även överraskande kontroller (med kort förvarning eller utan förvarning) förekommer samt särskilda säkerhetskontroller.
Kontroll genomförs som grundkontroll (GK) samt uppföljningskontroll (UK) och följer en i detalj uppgjord kontrollorder. För den långsiktiga planeringen ger MUST ut en nationell kontrollplan som omfattar de fem kommande åren med lägre detaljeringsgrad än kontrollordern. Denna plan rullas årligen.
Vid en GK av säkerhets- och signalskyddet upprättas en rapport där brister, förbättringsåtgärder och tidskrav för att åtgärda bristerna dokumenteras. UK omfattar främst de områden inom vilken bristerna uppmärksammats vid föregående GK.

Överraskande kontroll genomförs utan förvarning vid exempelvis säkerhetsoperationer.
Särskild säkerhetskontroll genomförs för att kontrollera viss verksamhet där ett akut säkerhetsproblem har uppstått eller kan förväntas uppstå. Kort förvarning används normalt när ett visst område (geografiskt eller funktionellt) behöver en fördjupad kontroll för att undanröja risker för rikets säkerhet.
För att tillfälligt ersätta mer omfattande kontroller finns säkerhetsskyddsbesök (SSB). Ett säkerhetsskyddsbesök ersätter inte den mer omfattande kontrollen men kan vara ett lämpligt sätt att tillfälligt lösa en kontrollsituation om exempelvis en grundkontroll nödgas senareläggas. Syftet med ett SSB är oftast att klarlägga den kontrollerades läge i stort och behov av stöd avseende säkerhetsskyddet.

MUST SÄKK upprättar en kontrollorder där det cirka ett år i förväg framgår tidpunkt för planerad kontroll som ska genomföras av MUST SÄKK eller OPE J2 SäkSam-sekt.
Cirka sex månader innan kontrolltillfället meddelas myndighet eller förband/enhet vad som ska kontrolleras. Inför en kontroll får det förband eller den myndighet som ska kontrolleras ett underlag som beskriver kontrollens omfattning i stort.

Myndighet/enhet som ska kontrolleras sänder senast två månader innan kontrollen in styrdokument som rör säkerhetstjänsten i form av arbetsordning, interna bestämmelser, verksamhets- och säkerhetsanalyser, säkerhetsskyddsplan, signalskyddsplan, avbrottsplaner, nätskisser och IT säkerhetsplan m m.

SIGNALSKYDDSTJÄNST

SIGNALSKYDDSTJÄNST

Inledning

Föreliggande årsrapport signalskydd 2006 utgör en sammanfattning över de viktigaste händelser och erfarenheter som inträffat under det gångna signalskyddsåret. Signalskyddsåret inleds och avslutas med det årliga centrala signalskyddsmötet som enligt plan genomförs under vecka 49. Nedan behandlas signalskyddsverksamhet som inträffat sedan det centrala signalskyddsmötet 2005 som genomfördes den 7 och 8 december, fram till det centrala mötet den 6 och 7 december 2006 i Bålsta.

Sammanfattning signalskydd

Försvarsmakten har enligt 4 § förordningen (SFS 2000:555) med instruktion för Försvarsmakten uppgiften att leda och samordna signalskyddstjänsten inom Totalförsvaret inklusive arbetet med säkra kryptografiska funktioner. Uppgiften ”arbetet med säkra kryptografiska funktioner” är ett tillägg som har tillkommit i instruktionen till Försvarsmakten sedan föregående utgåva. Inom Försvarsmakten pågår ett arbete med att definiera begreppet för att utröna i vilken mån Försvarsmaktens roll att leda och samordna signalskyddstjänsten påverkas av detta.

Såsom verkställande organ för Försvarsmaktens ledning och samordning av signalskyddstjänsten har Militära underrättelse och säkerhetstjänsten (MUST) Säkerhetskontor (SÄKK), inom funktionen för Totalförsvarets signalskyddssamordning (TSA) i likhet med tidigare år genomfört verksamhet inom hela signalskyddsområdet. Detta innebär bl a utveckling och granskning av kryptografiska metoder och signalskyddssystem för totalförsvarets behov. Framtagande av regelverk samt försörjning till totalförsvaret med kryptonycklar, certifikat och aktiva kort. Året har präglats av fortsatt åtaganden inom det internationella området i rollen som **National Communications Security Authority (NCSA).**

Som grund för den årliga verksamheten ligger en kontinuerligt rullande kontrollplan samt en plan för signalskyddsverksamheten under aktuellt år. I dessa planer fastställs datum för kontroller samt för de möten, dialoger och beredningar som avses genomföras. Dessa planer ger en god grund för en på dialog baserad utveckling av signalskyddsverksamheten syftande till att säkerställa ett fullgott signalskydd inom totalförsvaret, i dag och i framtiden.

Signalskyddsåret inleddes i december 2005 med det centrala signalskyddsmötet i Kolmården som under 1:a kvartalet 2006 följdes upp med 3 regionala signalskyddsmöten Örebro, Umeå och Växjö. De regionala mötena genomfördes av de nybildade SäkSam-sektionerna i samverkan med KBM.

Syftet med ovanstående möten är att informera och orientera om genomförd och pågående signalskyddsverksamhet inom områdena regelverk, systemutveckling, utbildningsfrågor mm. Mötena vänder sig till signalskyddschefer och övriga företrädare för signalskyddstjänsten som genom sitt deltagande ges möjlighet att bibehålla aktuell signalskyddsbehörighet.

Under hösten genomfördes de sedvanliga dialogerna mellan TSA-funktionen och enskilda myndigheter och organisationer inom totalförsvaret.

Dialogerna syftar dels till ett ömsesidigt informationsutbyte, dels ett klarläggande av respektive myndighets framtida behov av kryptoprodukter. Dessa dialoger utgör ett väsentligt underlag för TSA-funktionen i syfte att planera framtida utveckling. Vid dialogerna har representant från FMV och i några fall KBM och HKV FÖRBE deltagit.

Det centrala signalskyddsmötet 2006 genomfördes i Bålsta. Till mötet var signalskyddschefer och företrädare för signalskyddstjänsten vid centrala myndigheter och organisationsenheter samt Försvarsmaktens centrala och regionala ledningsorgan inbjudna. Mötet samlade ca 150 deltagare vilka representerande militära och civila verksamhetsställen. Mötet var planlagt i samråd med KBM.

Förutom sedvanliga programpunkter såsom lednings- och samordningsfrågor, kryptoutveckling, utbildningsfrågor mm fick deltagarna en föreläsning om hur signalskyddstjänsten vid Luftfartstyrelsen bedrivs och är organiserad. Vidare gavs mötesdeltagarna ett mycket uppskattat föredrag om IT-hotet genom Säkerhetskonsulten Tomas Djurlings försorg.

Erfarenheterna från signalskyddsårets möten, dialoger och beredningar, är att de fyller ett väsentligt behov av ömsesidiga kontakter och kontinuerlig uppföljning av signalskyddstjänsten och dess utveckling. Väsentligt är att rätt deltagare deltar i de möten som genomförs, annars föreligger risk för uteblivna resultat.

TSA-funktionen ser kontinuerligt över formerna för möten och dialoger för att uppnå största möjliga effektivitet. Avslutningsvis understryks vikten av att TSA-funktionen i samråd med KBM även framgent genomför denna utåtriktade verksamhet mot samtliga signalskyddsintressenter inom totalförsvaret. Det kontaktnät och den kännedom om vår gemensamma verksamhet som byggts upp under lång tid är en grundförutsättning för en väl fungerande signalskyddstjänst och ett högt signalskyddsmedvetande inom totalförsvaret.

Rollen som National Communications Security Authority (NCSA)

Rollen som sakansvarig inom kryptoområdet och som stöd till Regeringskansliet i kryptofrågor innebär för närvarande deltagande i 12 internationella arbetsgrupper t ex i Galileo-projetet (satellitnavigeringssystem), EDA (European Defence Agency), SESAME-projektet (EU:s nästa system för nivån EU SECRET) och samarbeten med EU:s starkaste kryptonationer.

Flera s k COMSEC-avtal har förhandlats fram och tecknats under året. Avtal utarbetas vid tillfällen då svenska signalskyddssystem tillhandahålls åt annan nation eller internationell organisation samt då Sverige tillhandahålls annan nations eller internationell organisations kryptosystem.

Ledning

Militärdistriktsstaberna med dess uppgift att leda och samordna Försvarsmaktens signalskyddstjänst samt samverka med det civila försvarets signalskyddsföreträdare upphörde 2005-12-31 i och med nedläggelsen av militärdistrikten. Vissa av MD-stabernas uppgifter såsom genomförande av administrativa kontroller, regionala signalskyddsmöten samt stöd till högre chef inom signalskyddstjänstområdet har övertagits av de nyinrättade SäkSam-sektionerna i Malmö, Göteborg, Stockholm och Boden.

Regelverk

Översyn av Försvarsmaktens interna bestämmelser om signalskyddstjänsten har under året fortsatt. De interna bestämmelserna kommer att fastställas så snart pågående utredning om ledningen av FM interna signalskyddstjänst är slutförd.

Följande instruktion har givits ut under 2006:

- I TST MGCI 2006

Arbetet med revidering av Handbok Totalförsvarets Signalskyddstjänst (H TST Grunder 2001) har under året fortsatt, dock med en långsammare takt än beräknat, bl a på grund av FM omstrukturering. Ny utgåva beräknas fastställas och ges ut våren 2007.

Bild 1 (Kryapp 1401)

Kryptoutveckling

Under 2006 har tre nya signalskyddssystem godkänts, nämligen:

- MGS/MGSI med FKA är ett signalskyddssystem för kryptering av data filer upp till och med signalskyddsgrad SECRET (SG S). Systemet har driftsatts och kommer att införas i Försvarsmakten under 2007.
- Signalskyddssystemet MGZI, det s k kryptomodemet (kryapp 1401) är ett datakrypto avsett för modem förbindelser upp till och med SGS. Kryptomodem 1401 skyddar kom munikationen över uppringda och fasta förbindelser, t.ex. analog teleförbindelse, ISDN, och externt modem för kommunikation över radio eller via GSM. Systemet som är under införande/installation inom Marinen, avser ersätta systemet MGG för att skydda bl a kommunikation över radioförbin delser. (Se bild 1).
- MGCI, Telefonkrypto 7201, kallas även för Mobilt krypto SG R. Telefonkrypto 7201 är ett kryptosystem som erbjuder krypterat tal, krypterad data och kryp terade SMS. Systemet är framtaget för SG R. (Se bild 2).

Bild 2 (Kryapp 7201)

Pågående utvecklingsprojekt:

- Signalskyddssystem PGBI. Filkrypto SG R. Avses driftsättas under 2007.
- Signalskyddssystem PGCI. Hårddiskkrypto SG R. Avses driftsättas under 2007.
- Signalskyddssystem MGB/MGBI (kryapp 920/9201). VPN-krypto SG S. Systemet planeras att driftsättas under våren 2007. (Se bild 3). Ytterligare en version av VPN-krypto är under utveckling.
- Höghastighetskrypto: Definiering av krav m m pågår. Upphandling av utveckling kommer att påbörjas under 2007.

Bild 3 (Kryapp 920)

- Elektronisk nyckelförsörjning (ENFÖ). Som ett första steg i att ta fram och utveckla ett elektroniskt nyckelförsörjningssystem har projektet Kundanpassad produktion (KAP) påbörjats. KAP innebär att nuvarande produktion av kryptonycklar läggs om för att bättre kunna möta de förutsättningar som kommer att krävas vid införandet av ENFÖ.

Dessutom deltager kryptopersonal med stöd till Försvarsmaktens viktigaste projekt där krav på krypto- och signalskyddssystem erfordras.

IT-säkerhetsutveckling

Inom MUST SÄKK TEK har den nya IT-säkerhetsutvecklingssektionen etablerats. Sektionen ansvarar bland annat för att vidmakthålla och utveckla Försvarsmaktens krav på säkerhetsfunktioner (KSF). Med KSF som grund lämnar sektionen stöd åt Försvarsmaktens utvecklingsprojekt. Syftet är att tidigt etablera rätt IT-säkerhetsarkitektur och säkerhetsmekanismer så att skyddsvärda uppgifter och verksamhetskritiska system ges ett tillräckligt skydd. Sektionen deltar i arbetet med att avge MUST yttrande inför driftsättning.

Sektionen arbetar även med att kravställa, verifiera och godkänna gemensamma IT-säkerhetsmekanismer som kan användas i flera olika system. För närvarande pågår utveckling och utvärdering av ett antal olika funktioner och produkter där syftet är att godkänna dessa för användning inom Försvarsmakten såsom:

- Skydd mot okänd kod.
- Dataslussar, lösningar för att koppla samman och utbyta information mellan system med olika skyddsnivåer. (Se bild 4).
- Produkter och komponenter för autentisering och åtkomstkontroll.
- Komponenter och arkitekturer för Restricted-miljöer.

Sektionen deltager även i verifiering av säkerhetskritiska delar i kryptosystem t ex i hårddisk- och filkryptoapplikationer.

Kryptonycklar, certifikat och aktiva kort

Produktion och distribution av kryptonycklar, certifikat och aktiva kort (TAK) har genomförts enligt plan. Byte av samliga användares aktiva kort generation 1 till generation 2 har inletts under året och så gott som slutförts.

Bild 4 Filterapparat GARM, komponent i datasluss

Utredningen av Totalförsvarets framtida försörjning av kryptonycklar, med hänsyn till organisation och framtida tekniska möjligheter, har under året fortsatt. Detta arbete har resulterat i en detaljerad kravspecifikation. Utifrån kravspecifikationen har det under året påbörjats ett arbete med framtagning av ett prototypsystem för elektronisk nyckelförsörjning. Prototypen byggs på plattformen IS UNDSÄK TSA Nycklar.
Som ett första steg för genomförande av kundanpassad produktion (KaP) har det under året genomförts en anpassning av nyckelförsörjningen inom Försvarsmakten vilket innebär att samtliga organisations-

enheter inom FM fr o m 2006-07-01 beställer kryptonycklar direkt vid NDA och NDA levererar direkt till beställaren. Efter vissa inkörningsproblem fungerar nu denna verksamhet bra.

Signalskyddsincidenter

Antalet incidenter är även detta år i stort sett konstant i förhållande till tidigare år. Det kan även konstateras att den procentuella fördelningen av olika typer av rapporterade incidenter helt faller in i den traditionella bilden. Nivån är godtagbar med hänsyn till det stora antalet nycklar och signalskyddsutrustningar som dagligen hanteras inom totalförsvaret.

Anmälan angående:

Misstänkt röjd nyckel…..……50 %
Saknad nyckel…..……35 %
Övriga incidenter totalt…….……..15 %

- Materielincident
- Felsänd nyckel
- Felaktigt tillverkad nyckel
- Hemlig information om nyckel i öppet nätverk

Felaktig förvaring är den vanligaste orsaken till en anmälan om misstänkt röjd nyckel, vilket ofta innebär att obehörig kan ha haft möjlighet att ta del av nyckeln.

Ett annat skäl till anmälan kan vara att förstöring av kryptonycklar inte har skett enligt föreskrifterna. Detta är t ex fallet då det upptäcks att exemplar av en utgången nyckel inte med säkerhet förstörts och förts upp i förstöringsliggare, samtidigt som exemplaren inte längre finns under kontroll för den ansvarige.

Det bör betonas att förstöringen av nycklar alltid skall ske enligt bestämmelserna. I samband med omorganisation och avveckling finns en tendens till slarv med just den uppgiften. I ett fall rapporterades upphittade nycklar i ett säkerhetsskåp, efter att skåpet fick öppnas med hjälp av låssmed, då varken kod eller ansvarig *person kunde spåras. Nycklarna skulle ha varit förstörda för flera år sedan.*

Skälet till att nycklar anmäls som saknade kan vara att nycklarna:

- Ej kan redovisas efter genomförd övning
- Saknas vid förstöring
- Upptäcks saknade vid kontroll av förstöringsliggare
- Upptäcks saknade vid kontroll efter uppackning
- Ej når mottagaren på grund av bristande leverans

Med ett ökat nyttjande av öppna nätverk blir det allt vanligare att information om kryptonycklar kan lagras och spridas i dessa. Det är viktigt att bestämmelserna här följs och att inte hemlig information rörande nycklar skrivs in i ett öppet system. Beakta t ex att en fullständig beteckning på en nyckel normalt är klassad som hemlig.

Försvarsmaktens omstrukturering med nedläggningar av förband och personalförändringar tycks inte ha påverkat det totala antalet uppkomna incidenter. I flera fall av nyckelincidenter under just 2006 har insatser krävts som inneburit att man på kort tid har varit tvungen att tillverka och distribuera nya nycklar.

De kostnader som en ”medelstor”

incident kan medföra då det skall tillverkas nya nycklar med kort varsel kan illustreras med nedanstående siffror.

Porto totalt	30 000:-
Övertid totalt	15 000:-
Materiel	5 000:-

Summa centralt vid NDA och för insats vid KBM Sollefteå……....…..ca 50 000:-

Därtill skall läggas eventuella kostnader för merarbete ute hos - alla mottagare av kryptonycklar - våra kunder.

Även om en inträffad nyckelincident i slutändan kan medföra omfattande kostnader är det viktigt att detta aldrig får bli ett skäl att avstå från att göra en anmälan.

Ett viktigt led i att nå en bättre kontroll vad gäller signalskyddsmateriel är det arbete med inventering av signalskyddsmaterielen som pågått och pågår främst inom Försvarsmakten och som är nödvändigt för att komma till rätta med ett relativt stort antal s k ”inventeringsförluster”.

Administrativa kontroller

Uppföljning och kontroll av signalskyddstjänsten har under året genomförts vid 49 enheter fördelat på fem centrala myndigheter, 36 regionala/lokala myndigheter eller företag, sex förband samt två försvarsavdelningar. Generellt kan sägas att resultatet, med några undantag, varit gott.

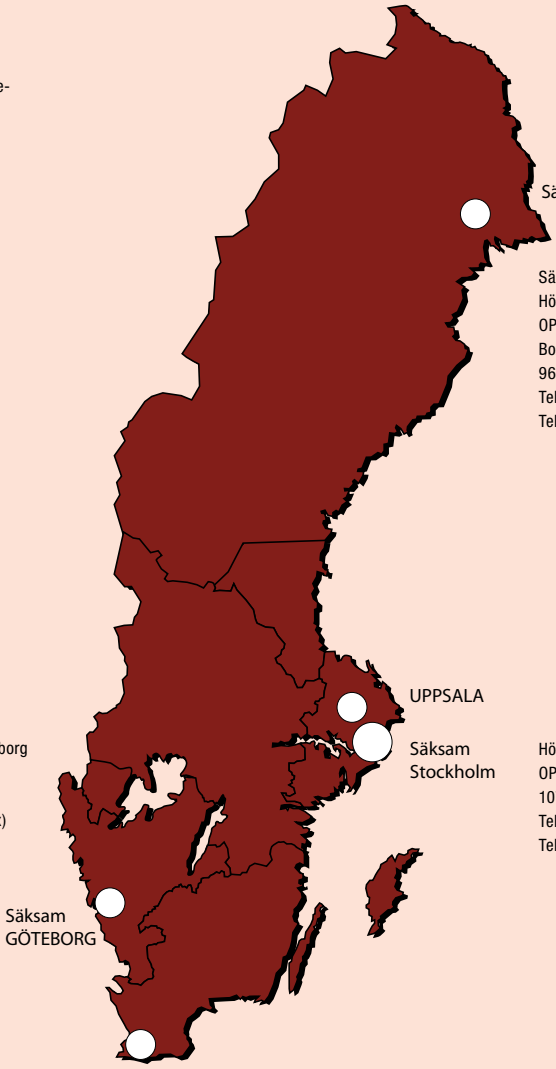

EN SVENSK TIGER®

Här finns den militära säkerhetstjänsten

Centralt

Högkvarteret (HKV)
med Militära underrättelse-
och säkerhetstjänsten
(MUST)
107 86 Stockholm
Telefon: 08-788 75 00
Telefax: 08-788 77 78
E-post: exp-hkv@mil.se
www.hkv.mil.se

Högkvarteret
OPE J2
Box 660
751 28 Uppsala
Telefon: 08-788 75 00
Telefax: 08-788 72 13



Säksam Boden
Högkvarteret
OPE J2/Säksamsekt Boden
Box 9101
961 19 Boden
Telefon: 0921-34 80 00 (vx)
Telefax: 0921-34 81 22

Säksam Göteborg
Högkvarteret
OPE J2/Säksamsekt Göteborg
Box 5155
426 05 Västra Frölunda
Telefon: 031-69 20 00 (vx)
Telefax: 031-69 20 49

Högkvarteret
OPE J2/Säksamsekt Stockholm
107 85 STOCKHOLM
Telefon: 08-788 75 00 (vx)
Telefax: 08-788 91 26

Säksam Malmö
Högkvarteret
OPE J2/Säksamsekt Malmö
247 82 Södra Sandby
Telefon: 046-36 80 00
Telefax: 046-36 89 18

FÖRSVARSMAKTEN