

Årsrapport Säkerhetstjänst  
2005



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-, signal-skydds- 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.



# FÖRSVARSMAKTEN

Militära underrättelse- och säkerhetstjänsten MUST

ÅRSRAPPORT SÄKERHETSTJÄNST 2005

FOTO: © Digital Vision



## Omslagsbild

Foto: Digital Vision

## Fotografer

- Sid 8 Utbildning av minörer. Foto: FBB/Håkan Nyström
- Sid 9 F 21 basjågarare. Foto: FBB/Ulf Petersson
- Sid 12 Utbildning. Foto: FBB
- Sid 13 Foto: FBB
- Sid 13 Liberia övning helikopter. Foto: FBB/Rick Forsling
- Sid 14 Soldat värnpliktig. Foto: FBB/Anders Sjödén
- Sid 15 Ammunition Bosnien BA09. Foto: FBB
- Sid 16 Foto: Clip Art
- Sid 17 Carlskrona skjutövning. Foto: FBB/Håkan Nyström
- Sid 17 Foto: Clip Art
- Sid 20 Swedint utbildning. Foto: FBB
- Sid 21 JAS 39 Gripen. Foto: FBB
- Sid 22 Flygbas övning. Foto: FBB
- Sid 23 Foto: Clip Art
- Sid 25 Utbildning värnpliktiga. Foto: FBB/Håkan Nyström
- Sid 25 Vårnpliktig vapenvård. Foto: FBB
- Sid 26 Lastning. Foto: FBB
- Sid 28 FHS. Foto: FBB
- Sid 33 Foto: SECTRA
- Sid 34 Foto: FM
- Sid 37 Basförsvar. Foto: FBB/Peter Liander

Denna årsredovisning publiceras även på Försvarsmaktens hemsida på internet [www.mil.se](http://www.mil.se), sökord "årsåk05".

Omslaget är tryckt på Arctic the silk 170 g och inlagan på Arctic the silk 115 g.

© Försvarsmakten

Grafisk form: FMLOG Serviceenhet Öst ToD.

Tryckeri: Davidsons Tryckeri AB, Växjö 2006.

# Innehållsförteckning

---

Den militära säkerhetstjänsten .....	6
Inledning .....	6
Omfattning .....	6
Förändringar i regelverk .....	7
Information och utbildning .....	8
Kontroller .....	8
Inledning .....	8
Genomförande .....	9
Genomförande verksamhet 2005 .....	9
Administrativa kontroller .....	9
Teknisk IT-kontroll .....	9
Signalkontroll .....	10
Inriktning för 2006 .....	10
Säkerhetshotande verksamhet.....	12
Sammanfattning.....	12
Inledning .....	12
Skyddsvärd verksamhet.....	14
Främmande underrättelseverksamhet.....	14
Terrorism .....	15
Kriminalitet .....	15
Subversion.....	16
Sabotage .....	16
IT-säkerhetsrelaterade incidenter .....	17
Incidentrapportering .....	18
SPAM.....	18
Slutsatser från FM CERT verksamhet 2005 .....	18
FM CERT i framtiden .....	18
Tekniska utredningar .....	18
Säkerhetsskydd .....	20
Inledning .....	20
Territoriell ledning .....	21
Ledningen av säkerhetsskyddstjänsten för Utlandsstyrkan .....	21
Internationella säkerhetsskyddsöverenskommelser .....	21
Allmänt .....	21
Informationssäkerhet.....	22

Informationssäkerhetsutredningen .....	23
Teknisk informationssäkerhet .....	24
Allmänt .....	24
Auktorisation och ackreditering .....	24
Tillträdesbegränsning .....	24
Allmänt .....	24
Vapen och ammunition .....	25
Förlust av vapen .....	26
Hemvärnets vapenförvaring .....	26
Kontroller avseende vapen- och ammunitionshantering .....	26
Larm 2000 .....	26
Övriga larm .....	26
Legitimationshandlingar .....	26
Skyddade transporter .....	27
Nyttjande av försvarsmaktsanställda civila skyddsvakter .....	27
Nyttjande av civila vaktbolag som transportskyddstyrka .....	27
Låsbyten på dörrar vid vissa ammunitionsförråd .....	28
Säkerhetsprövning .....	28
Allmänt .....	28
Genomförd verksamhet 2005 .....	28
Verksamhetsinriktning 2006 .....	29
Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA) .....	29
Signalskyddstjänst .....	32
Inledning .....	32
Sammanfattning signalskydd .....	32
Pågående utvecklingsprojekt .....	33
Kryptonycklar .....	34
Nyckelincidenter .....	34
Bilaga 1 Omorganisation till Säkerhets- och samordningssektioner .....	36
Historik .....	36
Militärdistrikt .....	36
Operativa Enhetens Säkerhets- och samverkanssektioner .....	38

# Den militära säkerhetstjänsten

---

# Den militära säkerhetstjänsten

## Inledning

2005-02-01 omorganiserades den militära underrättelse- och säkerhetstjänsten (MUST). MUST Säkerhetsavdelning, IT-säkerhetsavdelningen (ITSA) inkluderande totalförsvarets signalskyddsamordning (TSA) organiserades i MUST Säkerhetskontor (MUST SÄKK). Säkerhetskontoret har många uppdragsgivare och intressenter inom totalförsvaret, vilket innebär att Säkerhetskontoret måste arbeta processinriktat med uppdragsgivarnas behov i fokus där stöd till internationell verksamhet ökar i omfattning. Rollspel och arkitektur måste vara tydligt syftande till en optimal samordning av den militära säkerhetstjänsten.

I slutet av 2005 förändrades även ansvar och uppgifter på den operativa och regionala nivån avseende säkerhetstjänsten då militärdistriktsorganisationen avvecklades och ersattes av Säkerhets- och samverkanssektioner (Säksam). Se bilaga 1.

## Omfattning

Den militära säkerhetstjänsten syftar till att tillgodose det långsiktiga säkerhetsskyddet inom Försvarmaktens verksamhet såväl nationellt som internationellt.

Militär säkerhetstjänst omfattar säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalskyddstjänst.

Säkerhetsunderrättelsetjänsten syftar till att bedöma säkerhetshot som riktas mot Försvarmakten 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 att

hindra eller försvåra säkerhetshotande verksamhet samt förlust av skyddsvärd information.

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

Utöver detta tillkommer delprocesserna information/utbildning, säkerhetsoperationer 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 har förändrats och det ställer krav på att säkerhetstjänsten följer med i dessa förändringar. 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 för lite säkerhetsutbildning och för lågt säkerhetsmedvetande.



Den militära säkerhetstjänsten leds på central nivå inom Försvarsmakten av MUST. Chefen för MUST är Försvarsmaktens säkerhetsskyddschef, Försvarsmaktens informationssäkerhetschef och chef för Försvarsmaktens signal-skyddstjänst.

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

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

Den militära säkerhetstjänsten samverkar med polisen på alla ledningsnivåer och med Säpo. I det fall då den militära säkerhetstjänsten misstänker att brott begåtts eller är på väg att begås, görs en polisanmälan. Den militära säkerhetstjänsten har inga befogenheter att bedriva polisiär verksamhet.

### Förändringar i regelverk

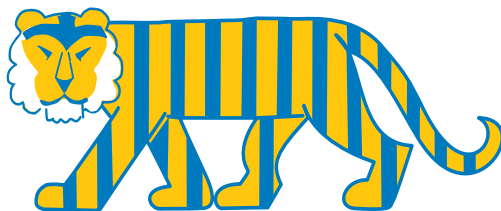
Under det gångna året har Försvarsmaktens interna bestämmelser

(FIB 1999:4) om säkerhetsskydd ersatts av Försvarsmaktens interna bestämmelser (FIB 2005:2) om säkerhetsskydd och skydd av viss materiel.

Bestämmelsen skiljer sig mot sin föregångare bl.a. att säkerhetsskyddet delas in i fyra informationssäkerhetsklasser. Vidare finns nya bestämmelser om hur skyddsvärd materiel, oavsett om den innehåller hemliga uppgifter eller ej, skall förvaras och transporteras.

Den 15 mars 2006 träder Försvarsmaktens interna bestämmelser (FIB 2006:2) om IT-säkerhet i kraft. Genom författningen upphävs Försvarsmaktens interna bestämmelser (FIB 2003:3) om IT-säkerhet. De förändringar som är gjorda är framförallt definitionen på produktägare och följdändringar med hänsyn till att militärdistrikten har lagts ned.

Översyn och fastställande av Försvarsmaktens föreskrifter om signal-skyddstjänsten inom totalförsvaret har genomförts (FFS 2005:2). Översyn av FM interna bestämmelser om signalskyddstjänsten har endast delvis genomförts pga FM omstrukturering. Arbetet kommer att återupptas under 2006 då FM framtida ledning och organisation är fastställd.



**EN SVENSK TIGER®**



## Information och utbildning

Under 2005 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.

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

Revideringen av handboksserien fortsätter under 2006. Serien kommer att bestå av H SÄK Hot, H SÄK Skydd, H SÄK IT, H SÄK Sekrbed, H SÄK SUA, H SÄK Int. H SÄK IT Hot kommer att gälla tills vidare. Under året har fortsatt revidering skett av handbok HTST Grunder 2001. Ny utgåva beräknas fastställas och ges ut under 2006. Ny utgåva av CD-SÄK planeras att utges i samband med att samtliga publikationer är fastställda.

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

Under hösten 2005 publicerades en artikel om Säkerhetskontoret i *Insats och Försvar* vilket är ett led i en strävan till ökad öppenhet.

## Kontroller

### Inledning

Vid den omorganisation som skett av Försvarsmakten under 2005 har MUST valt att organisera Försvarsmaktens säkerhets- och signalskyddskontroller under delprocess kontroll. Strävan är att utnyttja resurser inom hela Försvarsmakten för att lösa kontrollverksamheten.

Kontroller genomförs såväl nationellt som internationellt på de platser där Försvarsmakten löser uppgifter (exempelvis utlandsmissioner och försvarsattachéavdelningar).

Utöver detta genomförs säkerhets- och signalskyddskontroller vid myndigheterna under Försvarsdepartementet. Vidare genomförs ett omfattande signalskydd- och signalkontrollarbete vid samtliga myndigheter inom totalförsvaret.

Inte minst är det viktigt för kontrollverksamheten att i dialog med myndigheternas och förbandens säkerhetsorganisationer utvisa om organisationen uppfattat och följer säkerhetsbestämmelser. På detta sätt utgör kontrollprocessen ett stöd till den lokala säkerhetstjänsten i syfte att myndigheten eller förbandet ständigt ska inneha initiativet och i tid kunna vidta korrekta säkerhets- och signalskyddsåtgärder för att förebygga och effektivt kunna möta hotbildernas utveckling.

Säksamsektionerna har tagit över det regionala kontrollansvar som tidigare var ålagt de nu nedlagda militärdistrikten. Stöd för kontrollerna kan avropas från central nivå enligt särskilda bestämmelser.

## Genomförande

Chefen är ansvarig för att säkerhets- skyddskontroller genomförs regelbundet. Den enskilde är enligt den lokala säkerhetsorganisationens bestämmelser ansvarig för kontroll av egen arbetsplats och arbetsområde.

Som grund för kontrollverksamheten upprättas en kontrollplan där det ett år i förväg framgår tidpunkt för planerade kontroller. Sex månader innan en kontroll ska genomföras meddelas myndighet eller förband vad som ska kontrolleras. Inför själva kontrollen får det förband eller den myndighet som ska kontrolleras ett underlag som beskriver kontrollens omfattning i stort.

## Genomförd verksamhet 2005

Mot bakgrund av den omorganisation som den militära säkerhetstjänsten genomgått under 2005 har kontrollverksamheten genomförts i begränsad omfattning och stor del av kontrollerna har skjutits upp till 2006.

De säkerhets- och signalskyddskontroller som genomförts under 2005 vid utlandsstyrkan har varit vid kontingenterna i Afghanistan (FS 08), Kosovo (KS 11) och Bosnien (EB 01).

Grundkontroll har genomförts vid OPE i Uppsala samt vid Försvarsavdelningen i Prag, där även ambassaden erhöll stöd inom signalskyddsområdet.

## Administrativa kontroller

Uppföljning och kontroll av signalskyddstjänsten har under året genomförts vid 50 enheter fördelat på sju centrala myndigheter, 41 regionala/lokala myndigheter eller företag, ett förband, en försvarsavdelning samt i samband

med detta givit ambassaden stöd inom signalskyddsområdet. Vidare har utlandsstyrkan ej kontrollerats under 2005. Generellt kan sägas att resultatet, med några undantag, varit gott.

## Teknisk IT-kontroll

Den tekniska IT-säkerhetskontrollen har under 2005 varit inriktad på särskilda IT-säkerhetskontroller. I huvudsak har skyddsvärdverksamhet inom FM prioriterats. Stöd till militärdistriktet har lämnats vid två tillfällen genom en planlagd säkerhetskontroll i Uppsala samt under övning Viking 05. Övrigt stöd till militärdistriktet har skett genom FMTS försorg.

Erfarenheter från 2005 har visat på en i vissa fall stor skillnad mellan den faktiska IT-säkerheten i IT-systemen och den upplevda hos ansvariga för IT-systemen. Detta torde vara en tydlig indikering till ansvariga att vara mer delaktiga i hot-, risk- och sårbarhetsanalyserna av sina system.



## Signalkontroll

Säkerhetskontoret inriktar signalkontroll av signalskyddet i kommunikations- 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). Se FFS 2005:2 om signalskyddstjänsten inom totalförsvaret.

Signalkontrollen inriktas i fred till olika verksamheter som kräver hög eller långvarig sekretess och genomföres 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.

Signalkontroll har genomförts vid arméns slutövning i Skövde, Natomöte i Östersund (*Clear Spring*), Demo 05 vår och höst samt vid Viking 05. Vid dessa tillfällen har inte funnits anledning till allvarigare anmärkning om brister i sekretess vad avser signaltrafik i egna sambandssystem.

Bakgrundssamtal är mycket vanligt vid telefonsamtal och framförallt under tiden som man väntar på att uppringande samtal skall kopplas. Det bör påpekas att ljud går ut så fort man lyfter på luren.

Mobiltelefontrafiken är omfattande och det finns anledning att ännu en gång påpeka att mobiltelefon inte får användas för meddelanden som innehåller sekretess.

Kontrollgruppen har också under året

medverkat vid verifiering och förbättring av funktioner i larmsystem tillhörande Försvarsmakten.

Kontroll avseende RÖS har under 2005 genomförts vid ett flertal militära enheter. Metodiken för att kontrollera förekomsten av RÖS har delvis förändrats under året. Som ett alternativ till att (med RÖS-mottagare) försöka inhämta information från exempelvis olika datorskärmar har egengenererade signaler skapats i de lokaler som kontrollerats genom mätningar. Lokalernas dämpande egenskaper i kombination med avstånd till obevakat område har legat till grund för uttalanden om risken för informationsförluster på grund av RÖS. Under året har även fortsatt installation av avancerad materiel pågått med tester och prover både i Sverige och utlandet.

## Inriktning för 2006

Efter huvuddelen av kontrollerna kan det konstateras att säkerhets- och signalskyddet vid de kontrollerade objekten håller en godtagbar nivå. Tydligt är också att det inom Försvarsmakten finns både stor förståelse och vilja för säkerhet- och signalskyddstjänst. Under kontrollerna kan brister i säkerhets- och signalskyddstjänst åtgärdas oftast omedelbart genom utbildning på plats.

Hög prioritet kommer att läggas på Försvarsmaktens internationella verksamhet men även signalskyddskontrollerna inom totalförsvaret får som tidigare en framskjuten plats. Uppföljning skall ske så att upptäckta brister åtgärdas.

Säkerhetshotande verksamhet

---

# Säkerhetshotande verksamhet

## Sammanfattning

Nationellt är det f.n. främmande under rättelseinhämtning och kriminalitet som är de dimensionerande säkerhetshoten. Vid de internationella insatserna varierar säkerhetshoten mellan de olika insatsområdena. Ingångsvärdena är komplexa med olika konfliktparter, olika koalitionspartners i insatsområdet, värdlandets förutsättningar och dess förhållande till annan stat m.m.

Den militära säkerhetsunderrättelse-tjänsten står inför flera utmaningar under 2006.

Detta berör de bedömningar och beslut som härleds till FB 04<sup>1</sup>, där avvecklingen alltjämt fortgår. Det berör den nya organisationen i HKV 05 där den militära säkerhetstjänstens processer måste inarbetas och omhändertas på ett bättre sätt.

Ett annat angeläget område är att, våra utlandsmissioner är bemannade med lämpliga, välutbildade, välmotiverade och respekterade säkerhetstjänstföreträdare. Detta har varit ett påtalat och eftersatt område under lång tid. Vidare skall även

samarbetet med bl.a. Säpo, RKP<sup>2</sup> och Försvarmaktens tillsynsmyndigheter utvecklas ytterligare under året i syfte att skapa en bättre lägesuppfattning rörande säkerhetshot.

## Inledning

Den militära säkerhetsunderrättelse-tjänsten syftar till att identifiera och klarlägga säkerhetshot som riktas mot Försvarmakten och dess intressen inom och utom landet. Bedömningar tjänar främst som underlag för beslut om skyddsåtgärder men även att utreda och avbryta de säkerhetshot som förekommer.

Metodmässigt tar hot- och riskidentifieringen normalt avstamp ur den skyddsvärda och säkerhetskänsliga verksamheten. Det är av vital betydelse att identifiera och prioritera vad som är skyddsvärt och av betydelse, för att kunna nyttja våra disponibla resurser på ett försvarbart och kostnadseffektivt sätt. Med detta som inriktning kan säkerhetsunderrättelsetjänsten därefter inhämta och bearbeta information, för att i ett senare skede analysera och delge de hot och risker/sårbarheter som kan påverka det skyddsvärda. Beroende på hur långtgående delgivningen sker, kan även förslag till skyddsåtgärder föreslås, dvs. hur verksamhetsägaren kan och bör hantera hot och risker. Delgivning av säkerhets-hotbilder tjänar även som underlag för att förändra och utveckla våra regelverk samt utformning av nödvändiga säkerhets-skyddsmekanismer.

Ansvarsfördelningen måste vara klar och det tål att påpekas att det är verksamhetsägaren som bär ansvaret och skall fastställa vilken nivå på risken som kan



1 Försvarsbeslut 2004

2 RKP = Rikskriminalpolisen



anses försvarbar. Vid all verksamhet är det av betydelse att en verksamhetsanalys leder ansvarig chef vidare till en säkerhetsanalys och därefter till en upprättad säkerhetsplan.

Inför år 2006 kommer ytterligare fokus att läggas på Försvarsmaktens internationella verksamhet, där organiserandet och utvecklingen av Nordic Battle Group (NBG<sup>3</sup>) utgör en viktig komponent. På den nationella arenan är den fortsatta utvecklingen av Säksams ansvar och förmåga av stor betydelse under år 2006. Andra områden som är av betydelse, är att utveckla rutiner och metoder kring besöksverksamheten till Försvarsmakten samt förmågan till snabb och korrekt säkerhetsrapportering från lokal vidare upp till central nivå.

Generellt kan sägas att det är av vikt att identifiera vem eller vilka som påverkar 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 olika aktörer är att fastställa i vilken utsträckning dessa har kapacitet och intention riktad mot vår skyddsvärda och säkerhets känsliga 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 säker-

hetshotande aktörer är av betydelse för att lämpliga säkerhetsskyddsåtgärder ska kunna väljas och vidtas.

Vid internationella insatser ställs ökade krav på identifiering av "angripare och aktörer". Här är det av vital betydelse att den militära säkerhetsunderrättelsetjänsten, samordnat med den militära underrättelsetjänsten, kan inhämta, bearbeta, analysera och delge underlag inför potentiella insatser.



3 NBG = Nordic Battle Group skall stå i beredskap från 2008-01-01 till 2008-06-30 för eventuell insats.

### Skyddsvärd verksamhet

Under 2005 har varit i fokus verksamheten i Sverige med den ökande internationella verksamheten både vad avser prov och försöksverksamhet, forskning och utveckling men även internationella övningar och besök. Det har under 2005 bl.a. berört det nätverksbaserade försvaret (NBF) med dess demonstrationer (DEMO), den multinationella övning Viking 05 och det stora internationella NATO mötet i Åre – Östersund under våren 2005.

Under 2006 kommer ett ökat fokus läggas på de internationella insatserna i Afghanistan, västra Balkan och västra Afrika samt särskild uppföljning och stöd till NBG utvecklingen.

### Främmande underrättelseverksamhet

Nivån är oförändrad vad avser säkerhetshotet från främmande underrättelseverksamhet, både i Sverige och i de internationella insatser där Försvarmakten deltar.

Hoten har utgjorts av såväl interna som externa hot. När det gäller interna hot så bedöms dessa fall främst utgöras av felaktig hantering eller bristande kunskap och misstag vad avser hantering av hemliga handlingar. Det finns i några fall även bristande kunskap avseende hot och risker avseende kontakter med annan makts personal, där de gemensamma intressena bedöms ha övergått i vänskap. Dessa händelser har dock kunnat hanteras i ett tidigt skede och bedöms i dagsläget inte utgöra något inre hot.

Vid de internationella insatserna är främmande underrättelsehot främst kopplat till de pågående operationerna. I några fall berör det Försvarmaktens





utveckling avseende vissa materiel och förmågeutveckling.

### Terrorism

Tidigare bedömningar kvarstår rörande säkerhetshotet från terrorism, både i Sverige och i samband med internationella insatser finns inget direkt riktat hot mot Försvarsmaktens verksamhet eller intressen. Förutsättningarna är dock annorlunda i samband med de internationella insatserna då koalitionspartners kan ha ett betydligt högre direktriktat hot från aktör som bedöms vara en terroristorganisation. Härvid kan dessa hot överföras till de svenska truppbidragen. Detta är dock ett område som följs noggrant då följderna av detta säkerhetshot snabbt kan förändra förutsättningarna och behov av nya beslut om förändrade skyddsåtgärder snabbt kan bli nödvändiga. Ett sådant ställningstagande berör även bedömningen av eventuella överspridningseffekter från ett insatsområde till Sverige eller annat geografiskt område där svenska intressen finns. Även nationella politiska och militärstrategiska ställningstaganden kan förändra detta säkerhetshot mot Försvarsmakten.

### Kriminalitet

Nivån är oförändrad vad avser säkerhetshotet från kriminalitet, både i Sverige och vid de internationella insatser där Försvarsmakten deltar.

I Sverige utgörs hotet främst i form av tillgreppsbrott och mängdbrottslighet. Den fortsatta ökade våldsanvändningen av kriminella riktad mot främst värdetransporter är oroväckande och följs noggrant av Försvarsmakten. Av den säkerhetsrapportering som inkommit under året

är det främst försök att tillgripa vapen och ammunition som är av intresse att bearbeta och analysera. Den kriminalitet som riktar sig mot denna materiel är på en oförändrad nivå. Vad avser tillgrepp av drivmedel är även denna bild oförändrad. Detta bedöms både till viss nivå vara organiserat men även av mer tillfällig art och kopplat till marknadens drivmedelsprisutveckling.

De tidigare bedömningar som gjordes i anslutning till FB 04 och de materielavvecklingar som genomförts har inte i alla delar besannats, vilket är positivt. Försvarsmaktens anseende kan dock påverkas negativt då tillgrepp sker av avvecklad materiel.

I de internationella insatserna har något fall förekommit som kan härledas till ekonomisk brottslighet. Dessa fall har varit kopplade till upphandlingsrutiner. Översyn av rent förebyggande karaktär har skett rörande bedömt stöldbegärlig materiel och utrustning som transporteras till och från missionsområdena.

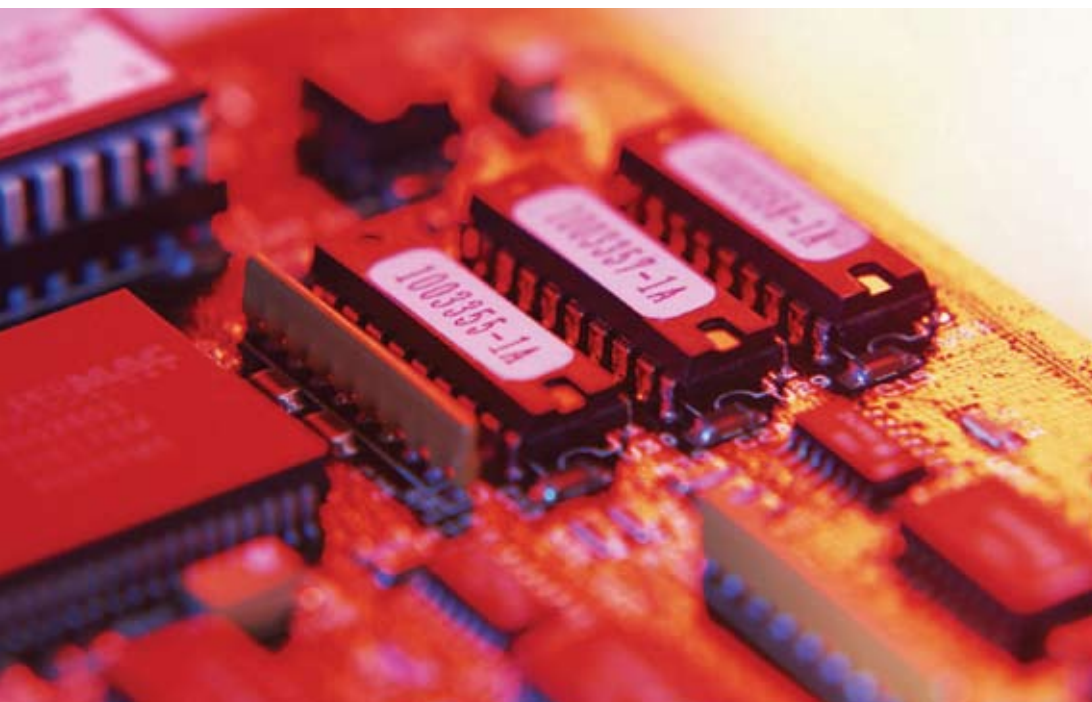


### Subversion

Under året har ingen säkerhetsrapportering inkommit som kan härledas till aktör som bedriver subversion riktad mot Försvarmaktens verksamhet eller intressen, vare sig i Sverige eller i samband med internationella insatser.

### Sabotage

För Försvarmaktens långsiktiga säkerhetsskydd är det av betydelse att sekretessbelagd information rörande kritiska sårbarheter för landets försvar och hävdande av territoriell integritet inte röjs. Detta berör även tidigare sekretessbelagd information som bedöms vara av intresse för en möjlig angripare att nyttja i framtiden vid en ogynnsam och oväntad förändrad omvärldsbild.





## IT-säkerhetsrelaterade incidenter

Försvarsmaktens *Computer Emergency Response Team* (FM CERT) ansvarar bland annat för insamling, hantering och koordinering av IT- säkerhetsrelaterade incidenter inom Försvarsmakten. Under 2005 har FM CERT expanderat, både vad gäller verksamhet och personal.

Antalet inrapporterade incidenter har under året legat på en nivå motsvarande 2004, och fortfarande rör flertalet felaktig, eller misstänkt felaktig hantering av sekretessbelagd information på data-media.

Förutom det tidiga utbrottet av masken Sasser som drabbade Försvarsmakten under våren 2005 har det varit få utbrott av skadlig kod i IT-systemen. Trots detta har FM CERT ett par gånger agerat för att säkerställa att IT-säkerheten upprätthålls. Under året har ett antal allvarliga sårbarheter upp-

täckts i operativsystemen. Flera av sårbarheterna har genererat så kallade "zero-day-exploits". Med det menas att innan leverantören meddelats om den funna sårbarheten har hackare skrivit kod som bekräftar och utnyttjar sårbarheten. Tiden mellan att hackaren släpper denna "proof-of-concept-kod" och till att leverantören distribuerat en säkerhetsuppdatering är vi alltså sårbara för attacker.

Genom en kontinuerlig lägesbild rörande IT-säkerhetsläget i Försvarsmaktens IT-system tar FM CERT, genom verksamheten omvärldsbevakning, höjd för att informera driftägare om de nya säkerhetsuppdateringar och föreslå säkerhetshöjande åtgärder då Försvarsmaktens IT-system är särskilt sårbara. Generellt har 2005 varit ett lugnare år vad gäller känd skadlig kod som sprids med e-post. Mängden stoppad e-post mer än halverades jämfört med 2004. Det är samma kod (e-postmasken NETSKY) som toppar statistiken för de två senaste åren.

Under sommaren 2005 skrev media om att myndigheter i Storbritannien utsatts för en attack med e-post. Om man läser rapporten som finns på Internet<sup>4</sup> kan man se att den som attackerade utnyttjade *social engineering* på ett sätt som inte setts tidigare. Ämnesrad och innehåll i e-posten hade anpassats till varje mottagare för att göra e-posten mer legitim, och få användaren att exekvera den bifogade trojanen.

Detta är ytterligare ett tecken på att man måste vara mycket försiktig med den e-post som kommer till myndigheten. Man kan inte längre lita på avsändare, ämnesrad eller att e-posten inte innehåller skadlig kod.



4 [www.niscc.gov.uk/niscc/docs/ttea.pdf](http://www.niscc.gov.uk/niscc/docs/ttea.pdf), tillgänglig 2006-02-07 kl 09:30.

## Incidentrapportering

För att FM CERT skall kunna delge en korrekt lägesbild vad avser säkerhetsläget i våra ledningssystem är det viktigt att bli bättre och noggrannare på att rapportera uppkomna incidenter. Som fastställdes gemensamt under 2004 skall IT-säkerhetsrelaterade incidenter i första hand rapporteras som verksamhet i IS UndSäk. Rapporten skall bearbetas i linjeorganisationen där FM CERT ansvarar för sammanställning av incidenter på militärstrategisk nivå samt för koordinering vid större incidenter.

## SPAM

I ÅR SÄK 2004 skrevs att Försvarmakten tittade på en lösning av SPAM med anledning av Statskontorets utredning. Nu har vi kommit ytterligare en bit på vägen och vår förhoppning är att en teknisk lösning kan driftsättas under våren 2006.

## Slutsatser från FM CERT verksamhet 2005

- Vid hantering av sekretessklassad information måste användaren säkerställa att sekretessen inte äventyras. Det är inte tillåtet att hantera sekretessklassad information i IT-system, på datorer eller i nätverk som inte är godkända för detta.
- Då virus och maskar sprids på ett sätt som gör att en traditionell antivirusprogramvara kan bli för långsam, krävs att användaren blir än mer uppmärksam på e-post som ankommer oväntat. Att avsändaren ser ut att vara känd behöver inte längre betyda att innehållet är oskadligt.

## FM CERT i framtiden

FM CERT skall fr o m 2008 vara ett krigsförband där arbetet med att sätta upp förbandet har påbörjats under 2005.

## Tekniska utredningar

Under 2005 har 17 tekniska utredningar genomförts. Utredningsuppdragen har varierat i både omfattning och typ. Vissa ärenden har utretts i samverkan med civila myndigheter och varit omfattande medan andra ärenden har haft karaktären att återskapa förlorad information ur ett begränsat antal lagringsmedia. Utredningsuppdragen har kommit från den centrala ledningen, lokala förband samt andra myndigheter. Den utredningstyp som ökar i omfattning och som troligtvis kommer öka under 2006 är analys av inspelad nätverkstrafik. Detta syftar till att kunna redogöra för skeenden i och att återskapa filer som skickats genom Försvarmaktens IT-system.

# Säkerhetsskydd

---

# Säkerhetsskydd

## Inledning

Den centrala ledningen av säkerhetsskyddstjänsten utövas av chefen för MUST som också är Försvarsmaktens säkerhetsskyddschef. Ledningen av säkerhetsskyddstjänsten för Utlandsstyrkan och den territoriella säkerhetsskyddstjänsten utövas av Operativ chef i Insatsledningen.

Vid Säkerhetskontoret är det i huvudsak tre av delprocessledarna som verkar inom säkerhetsskyddstjänsten, Chefen för Säkerhetsskyddsavdelningen (säkerhetsskyddsprocessen), Dpl Info/ Utb och Dpl Kontroller.

## Säkerhetsskyddstjänsten arbetar bl.a. inom områdena:

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



## Säkerhetsskyddsprocessen är i sin tur indelad enligt nedan:

- **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. Förutsättningarna för att en godtagbar IT-säkerhet skall kunna uppnås och upprätthållas är dock så speciella att det krävs särskilda regler och särskild kompetens. Beroende på den ökande komplexiteten i omfattningen av IT-systemen får detta område en allt större betydelse.
- **Tillträdesbegränsning** innefattar fast ställande av behov av tillträdes skydd, kontroll av att detta tillräckligt effektivt samt har en för ändamålet avvägd nivå.
- **Säkerhetsprövning** innebär att personalens pålitlighet, lojalitet, påverkbarhet och allmänna integritet 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 upphandlande myndighet. Denna förbindelse tecknas i ett säkerhetsskyddsavtal. Avtalet skall i till-

lämpliga delar reglera för i uppdraget påkallade säkerhetsskyddsåtgärder. Affärsavtal får ej tecknas före ett säkerhetsskyddsavtal.

- **Signalskydd är en säkerhetsskyddsangelägenhet.** Signalskyddsverksamhet bedrivs inom större delen av säkerhetskontoret.

### Territoriell ledning

I slutet av 2005 övergick den territoriella ledningen från militärdistriktscheferna till Operativ chef i Högkvarteret. Operativ chef leder den territoriella säkerhetsskyddstjänsten genom OPE J2 Säksam-sektioner i Malmö/Revinge, Göteborg, Stockholm och Boden. (Se bilaga 1)

### Ledningen av säkerhetsskyddstjänsten för Utlandsstyrkan

Operativ chef i Högkvarteret leder säkerhetsskyddstjänsten för Utlandsstyrkan. Vid varje förbandsinsats skall en utbildad säkerhetschef avdelas för ledning av den nationella säkerhetstjänsten inom kontingenten. Under 2005 har säkerhetschef för förbandsinsatser funnits inom KFOR, ISAF, UNMIL och EUFOR.

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

### Internationella säkerhetsskyddsöverenskommelser

#### Allmänt

Sverige är beroende av att ha giltiga och uppdaterade säkerhetsskyddsöverenskommelser 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 överenskommelser 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 säkerhetsskyddsöverenskommelser 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.



Under kommande år kommer arbetet med säkerhetsfrågorna för den nordiska snabbinsatsstyrkan vara den högst prioriterade frågan av den militära säkerhetstjänstens internationella uppgifter. Arbetet kommer att inriktas mot att bryta ner de övergripande säkerhetsbestämmelser som finns i det *Memorandum of Understanding* (MOU) som reglerar deltagarländernas förpliktelser.

## Informationssäkerhet

Inom Försvarsmakten finns en Försvarsmaktsstandard för ett integrerat verksamhetsledningssystem, FMS VHL 2003. Verksamhetsledningssystemet består bl.a. av en informationssäkerhetsdimension. Informationssäkerhetsdimensionen bygger på den internationella standarden Ledningssystem för informationssäkerhet - Riktlinjer för ledning av informationssäkerhet ("LIS", ISO/IEC 17799). Av standarden framgår bl.a. att en organisation måste ha en informationssäkerhetspolicy och ett uttalande om tillämplighet (*SOA, eng. statement of applicability*).

Överbefälhavaren beslutade under

året att Försvarsmaktens informationssäkerhetspolicy skulle börja tillämpas den 1 maj 2005.<sup>5</sup> informationssäkerhetspolicyen anges bl.a. att "Det övergripande målet med Försvarsmaktens informationssäkerhet är att säkerställa ett tillräckligt skydd för myndighetens informationstillgångar såväl inom som utom landet, så att rätt information är tillgänglig för rätt person i rätt tid på ett spårbart sätt."

Ett uttalande om tillämplighet beskriver i vilken omfattning och på vilket sätt

<sup>5</sup> HKV skr 2005-04-05, "Beslut om Försvarsmaktens Informationssäkerhetspolicy", bet. 10 700:65482.



specificerade styrmedel i standarden (LIS) är tillämpliga. Ett styrmedel är t.ex. policydokument för informationssäkerhet. Inom Försvarsmakten tillämpas just detta styrmedel genom myndighetens informationssäkerhetspolicy. Under året beslutade Försvarsmakten om ett uttalande om tillämplighet.<sup>6</sup>

Under slutet av 2005 påbörjade Riksrevisionen en granskning av Försvarsmaktens informationssäkerhetsstyrning. Granskningen utgick från LIS-standarderna och har genomförts på central nivå. Granskningen kommer att fortgå på lokal nivå under första kvartalet 2006. Resultatet från revisionen av Försvarsmaktens styrning av informationssäkerheten kan ge en bild dels över hur myndigheten har lyckats implementera ledningssystemet i sin verksamhet, dels vilka förbättringsåtgärder som myndigheten bör vidta.

Under året har säkerhetstjänsten uppmärksammat hur information om Försvarsmaktens utlandsinsatser publicerats på Internet i en allt större omfattning. Informationen delges genom hemsidor, resebloggar, vanliga bloggar eller via olika diskussionsforum.

I allt väsentligt har de publicerade uppgifterna inte inneburit ett röjande av sekretess eller utgjort ett hot mot förbandens operationssäkerhet. I de flesta fall är det helt enkelt svenska soldater som vill dela med sig av sina upplevelser i länder och på platser långt hemifrån.

Offentliggörande av uppgifter om

utlandsmissionerna kan dock innebära risker då det kan ge olika aktörer kunskap om svenska förbands uppgifter, beredskap, rörelsemönster, stridstekniskt och taktiskt uppträdande samt eventuella begränsningar i stridsvärdet. Denna typ av kunskap om våra förband kan i värsta fall användas i negativt syfte och utgöra ett hot mot operationssäkerheten samt minska förbandens förmåga att upprätthålla en hög nivå avseende force protection.

Den militära säkerhetstjänsten kommer därför att intensifiera uppföljningen av denna typ av uppgifter samtidigt som en översyn av nuvarande regelverk och bestämmelser genomförs.



### Informationssäkerhetsutredningen

Under 2005 har Säkerhetskontoret lett Försvarsmaktens remissbehandling av Informationssäkerhetsutredningens (Infosäkuutredningen) del- och slutbetänkanden. Försvarsmakten har avstyrkt utredningens organisatoriska förslag. Utöver detta har myndigheten tillstyrkt en del av de initiativ som följer av utredningens förslag till nationell informationssäkerhetsstrategi. Försvarsmaktens ställningstagande innebär i huvudsak att en översyn av bl.a. säkerhetsskyddslagstiftningen tillsammans med andra utgångspunkter i utredningen måste utgöra grunden för eventuella organisatoriska förändringar av statens informationssäkerhetsarbete.

<sup>6</sup> HKV skr 2005-06-13, "Beslut angående informationssäkerhetsdimensionen i försvarsmaktsstandard för integrerat verksamhetsledningssystem (FMS VHL 2003)", bet. 25 530:70017 och HKV skr 2005-10-13, "Beslut om rättelse i beslut angående informationssäkerhetsdimensionen i försvarsmaktsstandard för integrerat verksamhetsledningssystem (FMS VHL 2003)", bet. 25 530:75468.

## Teknisk informationssäkerhet

### Allmänt

Säkerhetskontorets auktorisations- och ackrediteringsarbete har bedrivits i nära samverkan mellan respektive process. På så sätt har erfarenheter och kunskaper från tidigare processteg tagits om hand. Processamverkan har bidragit till att Säkerhetskontoret har kunnat lämna ett ändamålsenligt och förutseende informationssäkerhetsstöd till Försvarsmaktens IT-systemutveckling under 2005.

En gemensam slutsats för auktorisations- och ackrediteringsarbetet är att antalet IT-system som har hanterats har minskat något jämfört med föregående år; samtidigt har omfattningen av och komplexiteten i systemen har ökat. Försvarsmaktens internationella åtaganden har också märkts i auktorisations- och ackrediteringsprocesserna. Exempel på handläggning av komplexa ärenden med internationella kopplingar är granskningar som har skett i samband med JAS 39-exporten till Ungern och Tjeckien, liksom granskningar av framtida användningsfall i utvecklingen av resursledningssystemet PRIO.

### Auktorisation och ackreditering

Under året har Säkerhetskontoret lämnat handläggningsstöd till förbandsenhets (HKV FÖRBE) auktorisationsgrupp inom ramen för Högkvarterets stödprocess, CIO-processen. Stödet har främst lämnats i form av granskning av säkerhetsmålsättningar för IT-system som är avsedda för behandling av hemliga uppgifter. Även säkerhetsmålsättningar för IT-system som inte är avsedda för

behandling av hemliga uppgifter har granskats. Exempel på sådana IT-system är system som har bedömts som verksamhetskritiska för Försvarsmakten, t.ex. system för uppföljning och egenrapportering samt system som skall stödja internationella övningar (VIKING 05).

Säkerhetsprocessen är den process vid Säkerhetskontoret som hanterar yttranden över säkerheten i IT-system, s.k. ackrediteringsyttranden. På samma sätt som Säkerhetskontorets auktorisationsarbete har varit koncentrerat till IT-system som är avsedda för behandling av hemliga uppgifter, har främst yttranden över sådana IT-system handlagts. Utöver yttranden över IT-system som t.ex. insatsledningssystem för markstridskrafterna (IS MARK), system för planering (IOR FM) samt system inom underrättelse- och säkerhetstjänsten (IS Undsäk) har även yttranden över vissa övriga verksamhetskritiska IT-system, som t.ex. Palasso II, handlagts under året.

## Tillträdesbegränsning

### Allmänt

Under 2005 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 2006. Med anledning av Försvarsmaktens pågående omstrukturering bedöms att risken för tillgrepp av kapitalvaror m.m. kan komma att kvarstå. Detta innebär att det är väsentligt att kontroller av tillträdesbegränsningar och av förvaring, hantering och transporter av skjutvapen och ammunition m.m. genomförs under 2006.



## Vapen och ammunition

Eftersom det blivit allt svårare att tillgripa skjutvapen och ammunition ur förråd har, under ett antal år, en viss "egentillverkning" av kulsprutepestolliknande skjutvapen skett i kriminella kretsar. Denna tillverkning har under 2005, genom polisiära åtgärder, tvingats upphöra varvid Försvarsmakten bedömer att hot, i syfte att få tillgång till skjutvapen och ammunition, kan komma att riktas mot personal som arbetar i förråd 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 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.

Under 2006 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.

## Sammanställning av förkomna vapen 1998-2005

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	0	8

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

### Förlust av vapen

Den nedåtgående trenden avseende vapenförluster har under 2005 fortsatt, dock återstår en del innan "nollvisio-nen" är uppnådd. Förlusterna har främst drabbat hemvärnsmän som förvarat sina vapen i hemmet.

### Hemvärnets vapenförvaring

Mot bakgrund av att det bedöms råda viss brist bl.a. på automatvapen i kriminella kretsar bedöms risken för tillgrepp av bostadsförvarade vapen som fortsatt hög.

### Kontroller avseende vapen- och ammunitionshantering

Mot bakgrund av erfarenheter från 2005 och mot vad som bedöms ske under 2006 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 ha ökat. Likaså är det väsentligt att garnisonschefer m.fl., genomför kontroller av att gällande bestämmelser avseende förvaring, hantering och transport av skjutvapen och ammunition följs.

### Larm 2000

Driftsättningen av larmsystem 2000 för friliggande ammunitionsförråd skedde under 2003. Under 2005 har provinstallationer av larm 2000 skett i bergförråd och kommer att fortsätta under 2006.

### Övriga larm

Försvarsmakten har, i form av ett "gam-malt 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 efterhand att byta ut eller modifiera dessa larm till Larm 2000 eller till det kommande systemet "Larm 3000".

### 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. är bl.a. Försvarsmakten är Setec TAG AB. Alla Försvarsmaktsanställda tilldelas tjänstekort.

Dessa tjänstekort innehåller magnetremsa, datachip samt s.k. Mifare-slinga, detta i syfte att i högre utsträckning än tidigare kunna nyttja tjänstekorten i automatiska passersystem.

Härutöver tillverkas identitetskort för militärpolis, legitimationsbevis för hemvärnets personal, värnpliktskort m.m. åt Försvarsmakten. Med anledning av utseendet

på de nya tjänstekorten, identitetskorten för militärpolis m.m. inte tillfullo överensstämmer med Försvarsmaktens interna bestämmelser (FIB 2001:4) om legitimationshandlingar m.m. avses denna att skrivas om under 2006.

### Skyddade transporter

I oktober 2002 utkom skrivelsen Riktlinjer för skyddade transporter, utom skjutvapen och ammunition, inom Försvarsmakten (HKV MUST 2002-10-03, 10 780:70519).

Dessa riktlinjer har i stor utsträckning överförts till författningstext Försvarsmaktens interna bestämmelser (FIB 2005:2) om säkerhetsskydd och skydd av viss materiel och kommer även att framgå av kommande utgåva av H SÄK Skydd.

### Nyttjande av försvarsmaktsanställda civila skyddsvakter

Med anledning av att Försvarsmakten omstrukturerar och därpå följande avveckling av militära förband inom ett antal geografiska orter och områden såsom Östersund, Vaxholm, Strängnäs, Gotland etc föreligger, åtminstone under en övergångsperiod, behov av att tillskapa någon form av insatsberedda skyddsstyrkor, bevakningsstyrkor och transportskyddsstyrkor på dessa platser. Detta för att kunna bibehålla vissa nödvändiga förråd för vapen och ammunition bl.a. för hemvärnets behov, kunna omförrådsställa viss materiel samt för att tillgodose behovet av bevakning vid arbete i förråd m.m. Behovet avses bl.a. tillgodoses genom nyttjande av vissa officerare och genom att viss personal i rubricerade styrkor anställs såsom för-

svarsmaktsanställda civila skyddsvakter. Detta har regleras genom tillägg i VU 2005.

För att underlätta nyttjandet av försvarsmaktsanställda civila skyddsvakter, bl.a. avseende förordnande samt utrustning för dessa har Försvarsmakten hemställt om att Regeringen skall 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 vaktjänst inom Försvarsmakten.

Dessa förändringar är f.n. under behandling i Regeringskansliet. Handläggningen har försejats men förändringarna bedöms kunna träda i kraft under våren 2006.

### Nyttjande av civila vaktbolag som transportskyddsstyrka

I syfte att minska behoven av att ta värnpliktiga i anspråk för transportskyddsverksamhet och bevakning vid arbete i förråd, ska möjligheterna att nyttja civila bevakningsbolag prövas. FMLOG är den organisationsenhet inom Försvarsmakten som har som uppgift att ombesörja för Försvarsmakten erforderlig logistik, inklusive upphandling och transporter, varför Högkvarteret 2003 gav FMLOG i uppdrag att upphandla bevaknings- och transportskyddstjänster av civilt bevakningsbolag. Upphandlingen avslutades, efter försejningar, hösten 2005 varvid avtal slöts med Falck Security AB.

### Läsbyten på dörrar vid vissa ammunitionsförråd

FORTV har sedan några år haft i uppdrag att vidareutveckla läsenheter för



dörrar vid vissa av Försvarsmaktens ammunitionsförråd. Under 2005 genomfördes provinstallationer av de nya låsen vid några ammunitionsförråd i södra Sverige. Utvärdering pågår och låsbyten vid flera ammunitionsförråd bedöms komma att ske under 2006.

## Säkerhetsprövning

### Allmänt

Skyldigheten att företa säkerhetsprövning omfattar all personal i FM och den som skall delta i verksamhet som har betydelse för rikets säkerhet även om förutsättningarna för registerkontroll inte är uppfyllda.

### Säkerhetsprövning omfattar:

- säkerhetsanalys av anställning,
- rekrytering, urval och anställning,
- utbildning om hot och säkerhetsknydd,
- registerkontroll med i förekommande fall särskild personutredning,
- uppföljning under anställning, tjänstgöring och uppdrag,
- personsäkerhetsutredningar.

Inte sällan sätts likhetstecken mellan registerkontroll och säkerhetsprövning vilket är felaktigt.

Tyngdpunkten vid en säkerhetsprövning skall alltid ligga på personlig kännedom och inhämtade betyg, intyg och referenser. Registerkontroll och särskild personutredning samt kontroll mot militära säkerhetstjänsten säkerhetsregister skall ses som betydelsefulla delar av säkerhetsprövningen.

En väl utvecklad samverkan mellan chefer och företrädare för personal-,

ekonomi- och säkerhetsfunktionerna är en förutsättning för att säkerhetsprövningen skall kunna genomföras på ett sätt som säkerställer att personer, som inte bedöms lojala och pålitliga från säkerhetssynpunkt, inte tas i anspråk av Försvarsmakten. Det är viktigt i detta sammanhang att påpeka att den militära säkerhetstjänstens huvuduppgift vad avser säkerhetsprövning är att pröva den enskildes lojalitet, pålitlighet och sårbarhet från säkerhetsskyddssynpunkt och skall därför inte genomföra någon "rättslig" prövning, mot vad som har framkommit om den enskilde

Det är viktigt att följa upp anställda, i syfte att tidigt uppmärksamma problem och vidta stödåtgärder för dem som brister i sitt säkerhetsmedvetande eller som riskerar att utsättas för säkerhetshot. Detta är av särskild vikt för de kategorier av personal som är inplacerade i de högre säkerhetsklasserna samt för personal som deltar i internationell verksamhet.

### Genomförd verksamhet 2005

Försvarsmaktens ökade internationella åtaganden har inneburit fler framställningar om *Security Clearance*. Under året har 1500 *Security Clearance* behandlats och utfärdats.

Förnyade registerkontroller i säkerhetsklass 3 för yrkesofficerare, reservofficerare och aspiranter har genomförts i stort enligt plan. Vissa förband som har fått ny personal släpar efter med dessa kontroller, som skall fullföljas under 2006. Totalt har Säkerhetskontoret under 2005 (t.o.m. 2005-12-11) genomfört 13 534 registerkontroller avseende anställning och SUA-uppdrag inom Försvarsmakten.

Anställning eller verksamhet som skall

placeras i säkerhetsklass eller kontrolleras till skydd mot terrorism skall årligen analyseras och dokumenteras i IS Undsäk. Detta har inte genomförts fullt ut under 2005 och kommer att fullföljas under 2006. Förband som ej gjort detta kommer att följas upp särskilt eftersom chef med arbetsgivaransvar inte får begära registerkontroll utan att varje befattning har analyserats.

Framtagning av särskilda bestämmelser för prövning och uppföljning från säkerhetsskyddssynpunkt av personal ingående i Försvarmaktens chefskrets har påbörjats och kommer att fullföljas under 2006.

### Verksamhetsinriktning 2006

**Införandet av Säksam-sektioner innebär bl.a. att de skall stödja Säkerhetskontoret med:**

- Genomförande av skyddssamtal och säkerhetssamtal.
- Utbildning och information i säkerhetsprövningsärenden.
- Kontroll och uppföljning av säkerhetsprövningsärenden.
- Personutredningar.

Chef för förband där utbildningsgrupper (f.d. militärdistriktsgrupper) ingår är ansvarig för handläggning och beslut i personärenden för personal som ingått avtal med hemvärdet.

### Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)

Omstruktureringen av Försvarmakten har under 2005 medfört ett fortsatt ökande behov av upphandling av tjänster i verksamheter som enligt svensk lag skall

ha säkerhetsskydd med hänsyn till rikets säkerhet.

Kraven och resurserna är alltså i obalans. FMLOG:s uppgift som stöd åt kärnverksamheten i FM tolkas på olika sätt. Beställaren har alltid ansvaret för säkerhetsskyddet i sin verksamhet. En särskild balansakt i detta säkerhetsskyddsarbete är samverkan mellan beställaren som säkerhetsskyddsansvarig och FMLOG Upphandlings- och försäljning-enhet.

### Är det skillnad på säkerhetsskydds-kravet vid anställning respektive köp av tjänst?

*- Nej i princip inte.*

Under 2005 har många av FM stödverksamheter som tidigare lösts av försvarmaktsanställda ersatts av externa leverantörer. Även verksamheter, som skall avvecklas, har blivit outsourcade fullt (inklusive personal). Personalen har m. a.o. bytt arbetsgivare och i stället för att vara arbetstagare blivit uppdragstagare via ett företag vid sitt "gamla" förband. Det handlar här om komplicerade upphandlingar där det är lätt att tycka att säkerhetsskyddet som finns i den organisation som skall avvecklas följer personalen.

Vid upphandling blir det säkerhetsskydd, som förbandet anser behövs i uppdraget, bindande för företaget först i och med att ett säkerhetsskyddsavtal har slutits mellan företaget och förbandet. Affärsavtal får inte ingå förrän säkerhetsskyddsavtalet har ingåtts.





# Signalskyddstjänst

---

# Signalskyddstjänst

## Inledning

Försvarmakten har enligt 4 § förordningen (SFS 2000:555) med instruktion för Försvarmakten uppgiften att leda och samordna signalskyddstjänsten inom totalförsvaret.

## Sammanfattning signalskyddstjänst

Signalskyddsverksamheten inleds och avslutas med det årliga centrala signalskyddsmötet i november. Nedan behandlas signalskyddsverksamhet mellan det centrala signalskyddsmötet 2004 som genomfördes den 1 och 2 december i Visby, fram till det centrala mötet den 7 och 8 december 2005 i Kolmården.

Såsom verkställande organ för Försvarmaktens ledning och samordning av signalskyddstjänsten har Säkerhetskontoret, 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 av totalförsvaret med kryptonycklar, aktiva kort och certifikat.

Året har präglats av fortsatta åtaganden inom det internationella området, framförallt inom EU-samarbetet där kunskaper har inhämtats för att möjliggöra interoperabilitet för våra förband inför kommande internationella uppdrag.

Signalskyddssystem finns idag förutom inom Försvarmakten, Regeringskansliet och vid statliga myndigheter och verk inom en mängd företag, företrädesvis

inom försvarsindustrin. Många av de statliga myndigheterna har även signalskyddsverksamhet vid respektive "regionala och lokala" enheter.

Det centrala signalskyddsmötet i Visby följdes upp under första kvartalet 2005 med 3 regionala signalskyddsmöten (ett inom varje militärdistrikt). Syftet med dessa möten är att informera och orientera om genomförd och pågående signalskyddsverksamhet inom områdena regelverk, systemutveckling, utbildningsfrågor m.m. 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 och 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 2005 genomfördes i Kolmården. Till mötet var signalskyddschefer och företrädare för signalskyddstjänsten vid centrala myndigheter och organisationsenheter samt Försvarmaktens centrala och regionala ledningsorgan inbjudna. Mötet samlade ca 130 deltagare vilka representerade militära och civila verksamhetsställen. Mötet var planlagt i samråd med KBM.

Erfarenheterna från årets olika verksamheter såsom möten, dialoger och

beredningar, är att de tillgodoser ett behov av ömsesidiga kontakter och kontinuerlig uppföljning av signalskyddstjänsten och dess utveckling.

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 signalskyddsintressenter inom totalförsvaret. Det kontaktnät och den kännedom om vår gemensamma verksamhet som byggts upp under lång tid inom totalförsvaret är en grundförutsättning för en väl fungerande signalskyddstjänst och ett högt signalskyddsmedvetande.

### Pågående utvecklingsprojekt

Under året har ett antal kryptosystem och kryptokort modifierats och godkänts i ny version. Utveckling av mobilt krypto för Signalskyddsgrad (SG) Restricted (Kryapp 7201, Signalskyddssystem. m.GC) har genomförts och driftsättning planeras till första kvartalet 2006. MGC är ett tal- och datakrypto som kan användas tillsammans med flertalet kommunikationsutrustningar såsom mobiltelefon, satellit, fast telefonnät m.m. Signalskyddssystemet ger möjlighet till förenklad nyckelhantering, där inga kryptonycklar behöver läsas in. Dock erbjuder systemet även möjlighet att nyttja gemensamma nycklar.

FM har beställt utveckling av en kryptomodul med benämning KM6i, som under senhösten har kryptoverifierats och godkänts för SG Secret. Kryptomodulen är främst avsedd för att användas i Mobilt Krypto - SG Secret.

Modulen har tagits fram i samarbete med NCSA i Nederländerna och har en gemensam arkitektur men anpassas för en svensk och en nederländsk variant. Nederländerna utvecklar för närvarande ett Mobilt Krypto som innehåller ovan nämnda modul som kryptokärna. Samarbetet syftar till att genom gemensam utveckling och utvärdering få en för parterna bättre och billigare produkt än om båda var för sig skulle genomfört motsvarande utveckling.

Utveckling av nästa generationskryptomodul pågår. Det är en snabb kryptomodul som skall klara mer än 2.5 Gbit/s och kunna användas i krypto-apparater avsedda för höghastighetskryptering i



FTN (Försvarets telenät) och vid kommunikation mellan servrar.

Fortsatt arbete har bedrivits under året med införande av nästa generations aktiva kort samt nya kortterminaler. Vissa förseningar har uppkommit och planerad driftsättning är nu under första kvartalet 2006.

Under året har arbete bedrivits med att vidareutveckla KrAPI som är det Krypto-

API som möjliggör anrop till krypto-komponenter i form av både hård- och mjukvara. Andra mjukvarumoduler för att integrera aktiva kort i Microsoft-miljö är under utveckling.

- Utveckling av Kryptomodem 1401 (Signalskyddssystem GZI) pågår fortfarande. Dock har anpassning mot marina krav gjorts, vilket har ställt särskilda krav på storlek och miljötåligghet.
- Prototyper av det nya VPN-kryptot som är under utveckling har levererats och tester pågår.
- En ny filkryptoapplikation (FKA) för SG S har utvecklats och verifierats. Driftsättning planeras till första kvartalet 2006.
- En ny filkryptoapplikation i mjukvara för SG R är under utveckling.
- Ett hårddiskkrypto för SG R har specificerats och är under upphandling.

TSA-funktionen har deltagit i internationella konferenser om krypto och deltagit i flera kryptosamarbeten inom EU.

### Kryptonycklar

Produktion och distribution av kryptonycklar och totalförsvarets aktiva kort (TAK) har genomförts enligt plan. Utredningen av totalförsvarets framtida försörjning av kryptonycklar, med hänsyn

till organisation och framtida tekniska möjligheter, har fortsatt under året. Resultatet av utredningen skall ligga till grund för framtagning av ett nytt elektroniskt nyckelförsörjningssystem (eNFÖ). Detta arbete har resulterat i en detaljerad kravspecifikation som kommer att fastställas under första kvartalet 2006. Kravspecifikationen skall i första hand ligga till grund för framtagning av ett prototypsystem för elektronisk nyckelförsörjning.

### Nyckelincidenter

Antalet incidenter under 2005 är i stort sett konstant i förhållande till tidigare år. Försvarsmaktens omstrukturering med nedläggningar av förband och personalförändringar tycks inte ha påverkat det totala antalet uppkomna incidenter. Nivån är godtagbar med hänsyn till det stora antal nycklar som dagligen hantteras inom totalförsvaret.



# Bilaga I Omorganisation till Säkerhets- och samverkanssektioner

---

# Bilaga I Omorganisation till Säkerhets- och samverkanssektioner

---

## Historik

En regional militär säkerhetstjänst av betydelse har det funnits sedan mycket lång tid tillbaka och blir tydlig från 1833 då riket indelades i militärdistrikt. Uppgifterna innebar bland annat ordningstjänst, att motverka brottslighet mot krigsmakten samt skydd mot spioneri och sabotage m.m. Resurserna utgjordes av fältpolis, militärpolis och efter hand särskilda säkerhetsförband. Från 1893 var riket indelat i fördelningsområden och från 1943 i militärområden. Dessa områden indelades under första världskriget i hemliga försvarsområden som rustades under inledningen av andra världskriget och från 1942 blir offentliga för att efter kriget utgöra delar av såväl grund- som krigsorganisationerna.

Under 1900-talet genomgick den svenska krigsmakten - Försvarsmakten ett otal omorganisationer samtidigt som organisationen växte eller minskade i takt med yttre hot och händelseutvecklingar.

Från de tidiga militärdistrikten via olika indelningar och namnbyten så tillhörde alltid en säkerhetstjänst den territoriella organisationen. Vid slutet av 1990-talet beslöts att den dåvarande ledningsorganisationen med tre militärområden och ett stort antal försvarsområden, marin- och flygkommandon m.m skulle ersättas av en mindre, modernare organisation. Därvid skulle operativa uppgifter centraliseras medan territoriella uppgifter skulle lösas av den nya organisationen genom att efter mer än 100 år åter bilda militärdistrikt dit bl.a. den regionala MUST koncentrerades. Den gamla indelningen ansågs inte längre vara funktionell då existentiella hot mot Sverige hade

upphört och förbandsmassan minskat påtagligt. Det viktigaste motivet till omorganisationen var dock, som vanligt, att spara pengar.

2000-07-01, efter Försvarsbeslutet 1999, skapades alltså den nya territoriella organisationen med fyra militärdistrikt (MD) för ledning över ytan, utbildning av hemvärn m.fl. och samverkan inom totalförsvaret samt, som en av de viktigaste uppgifterna, ledning av den samlade regionala militära säkerhetstjänsten.

## Militärdistrikt

I samband med omstruktureringen år 2000 ärvde de nybildade militärdistrikten hela den regionala militära säkerhetstjänstens uppgifter från såväl militärområdes- som från försvarsområdesnivån. Alla uppgifter kvarstod alltså, fast i en betydligt mindre organisation.

Detta innebar dock att de nya territoriella staberna kunde dra nytta av milostabernas övergripande kunskaper och särskilda uppgifter inom säkerhetsunderrättelseområdet samt högre regional samverkan liksom detaljkunskaper, samordning och kontaktnät från försvarsområdesnivån. Få medarbetare ur den gamla organisationen följde dock med till den nya. Det blev alltså ändå nödvändigt med en omfattande uppbyggnad av kunskaper och kontakter. Detta innebar åtskilliga besök hos alla polismyndigheter, Säpo-sektioner med flera. Ett stort arbete lades ned på samordning och kontaktverksamhet för att bygga upp och förvalta förtroenden mellan den regionala säkerhetstjänsten och berörda myndigheter liksom att etablera nya rapporteringsvägar. Allt detta lyckades distrikten väl med.

Militärdistrikten var i sin tur indelade i militärdistriktsgrupper (MD-grp) för rekrytering och ledning av hemvärnet samt stöd till frivilligorganisationerna. Detta innebar att MD, förutom garnisonernas lokala säkerhetstjänst, hade tillgång till många "ögon och öron" över ytan och därmed rapportering av säkerhetshändelser från alla delar av territoriet. Genom kontaktpersoner vid alla MD-grp, ledningsgrupperna i Stockholm och Malmö samt säkerhetscheferna vid alla förband, garnisoner och enheter byggdes en relativt heltäckande militär säkerhetstjänst upp inom respektive MD. Funktionsmässigt styrdes alla dessa delar av MD-stabernas J2-avdelningar (J2 är en Nato-beteckning för underrättelse- och säkerhetstjänst). Militärdistriktens J2-avdelningar funktionsstyrdes direkt från MUST.

De begränsade personalresurserna inom underrättelse- och säkerhetsområdet medförde att en stor del av specialkunskaperna koncentrerades till respektive J2-avdelning såsom säkerhetsunderrättelsetjänst, säkerhetsutredningar, hotbildsanalyser, informationssäkerhet, skydds- och säkerhetssamtal, skyddsobjektshantering, tillträdesbegränsningar, kartsekretess, flygfotoinspektion, avancerad IT-säkerhet på teknisk nivå samt signalskyddsverksamhet mm. Genom optimering av resurserna och stöd från bl.a.

MUST blev de små säkerhetstjänsterna ändå väl fungerande. Härutöver ska påpekas att förmågan att genomföra säkerhetsoperationer genom samordning av resurserna inom respektive militärdistrikt och användning av reservofficerare blev goda.

MUST och Säpo hotbilder bearbetades fortlöpande till MD hotbilder som grund för regionala/länsvisa och lokala hot- och



riskanalyser där framförallt kriminalunderrättelsetjänsten fick stor påverkan.

En viktig del av den regionala säkerhetstjänsten har varit kontrollverksamheten (till del också dimensionerande) med såväl omfattande garnisonskontroller med lång framförhållning, uppföljningskontroller, mindre förannmälda kontroller av olika anledningar och säkerhetsskyddsbesök till överraskande kontroller inom något begränsat område eller funktion.

Utbildning är en av de viktigaste verksamheterna inom säkerhetstjänsten genom t.ex. kurser, kortare utbildningar,

seminarier och orienteringar. Uppgiften har varit belastande men gett mycket tillbaka då utbildning har varit och är det viktigaste instrumentet för att säkerställa ett gott säkerhetsmedvetande hos FM personal.

Härutöver har under åren genomförts ett stort antal säkerhetstjänstmöten såväl inom allmän säkerhetstjänst som IT-säkerhet och signalskydd med bra dialoger och intressanta föredragningar.

Sammantaget kan konstateras att de fem och ett halvt åren som militärdistrikten svarade för den regionala militära säkerhetstjänsten har innehållit en god förmåga till hantering och analys av säkerhetsrapporter, uppföljning av säkerhetsändelser, stöd till garnisoner och förband rörande säkerhetstjänst, omfattande kontrollverksamhet, stora lyckade utbildningsinsatser och ett effektivt samarbete med framförallt polisen.

## Operativa Enhetens Säkerhets- och samverkanssektioner

I och med Försvarsbeslutet 2004 (FB 04) så beslöts att en ny organisation för ledning och territoriell verksamhet inom Försvarmakten skulle införas från 2006-01-01. Det stod tidigt klart att den militära säkerhetstjänsten inte kunde klara av sina uppgifter utan att vara representerad regionalt i någon form.

Flera idéer såg dagens ljus men till sist beslutades att landet skulle indelas i fyra områden för säkerhetstjänst. Från 2006-01-01 har ansvaret för den

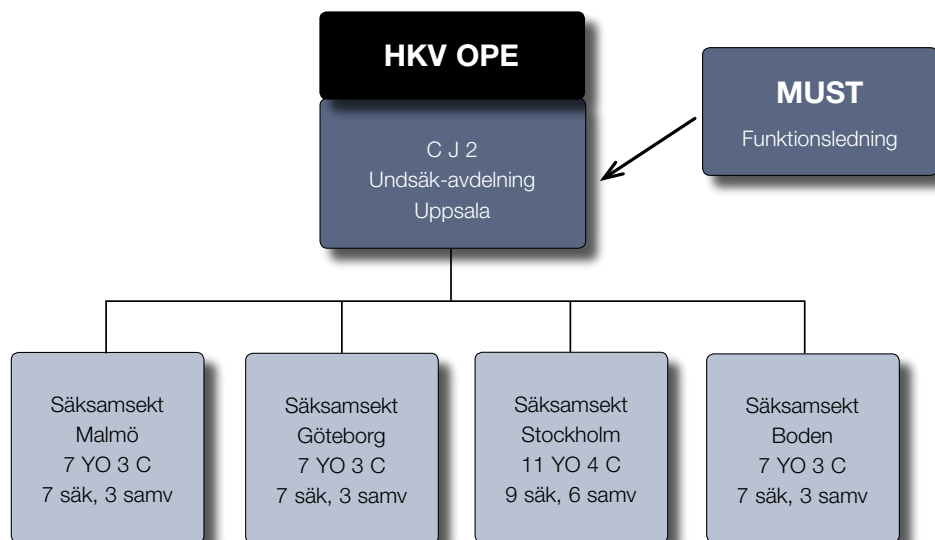
militära säkerhetstjänstens territoriella uppgifter övertagits av de nybildade Säkerhets- och samverkanssektionerna Säksamsekt i Malmö, Göteborg, Stockholm och Boden. Dessa sektioner ingår i Högkvarterets (HKV) Operativa Enhets (OPE) Underrättelse- och säkerhetsavdelning (J2). Sektionerna utgör alltså delar av den centrala nivån men är utlokaliserade för att på bästa sätt fånga upp säkerhetsändelser, analysera hot i samråd med Säposektionerna och kriminalunderrättelseenheterna hos polismyndigheterna samt bedriva allmän säkerhetstjänst till stöd för garnisoner och förband, delta i säkerhetsutbildning, genomföra kontrollverksamhet och enligt funktionsstyrning från MUST delta i eller leda säkerhetsoperationer. Härutöver skall säkerhetsskyddsuppgifter, IT-säkerhets- och signalskyddsfrågor inklusive signalskyddsnyckeladministration hanteras.

Underrättelsetjänstsuppgifterna, som fanns inom militärdistriktsorganisationen som en tung uppgift vid beredskapshöjning, kris och krig, har helt tagits bort från den nya Säksam-organisationen.

Förutsättningarna är goda för att de nya sektionerna, efter viss kompetensuppbyggnad och en inkörningsperiod, kommer att bli en bra fungerande säkerhetstjänstorganisation. Dock kommer resurserna att vara begränsade och uppgifterna stora och omfattande varför Försvarmakten måste acceptera en viss effektnedgång inom säkerhetstjänstområdet under Säksam-sektionernas premiärår.



Organisationskiss: Säksam-sekt kopplat till  
HKV MUST, OPE, J2 och förbanden







# 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 Göteborg  
Högkvarteret  
OPE J2/Säksamsekt Göteborg  
Box 5155  
426 05 Västra Frölunda  
Telefon: 031-69 20 00 (vx)  
Telefax: 031- 69 16 81

Säksam  
GÖTEBORG

Säksam  
MALMÖ

Säksam Malmö  
Högkvarteret  
OPE J2/Säksamsekt Malmö  
247 82 Södra Sandby  
Telefon: 040-680 59 61  
Telefax: 040-680 59 64

Säksam Boden

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

UPPSALA

Säksam  
Stockholm

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



FÖRSVARSMAKTEN