FÖRSVARSMAKTEN

Militära underrättelse- och säkerhetstjänsten MUST

# Årsrapport Säkerhetstjänst 2004

# 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 hemliga uppgifter från att röjas, obehörigen förändras eller förstöras samt skydda materiel, anläggningar och personal mot sabotage, stöld och terrorism.

Delområden:

- Informationssäkerhet
- Tillträdesbegränsning
- Säkerhetsprövning
- Utbildning, stöd och kontrollverksamhet
- Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)
- Internationella säkerhetsfrågor

**IT-säkerhetstjänst och signalskydd**

Följa riskutvecklingen och klarlägga säkerhetshotande verksamhet mot Försvarsmaktens information, IT-system och IT-infrastruktur samt tillse att dessa har erforderligt skydd.

Detektera, avbryta och återställa (återgälda) angrepp eller försök till angrepp på information, IT-system och IT-infrastruktur.

Förhindra att information som rör rikets säkerhet kommer obehöriga till del.

*Snövandrare.*
*FOTO: © Digital Vision*

# FÖRSVARSMAKTEN

**Militära underrättelse- och säkerhetstjänsten MUST**

## ÅRSRAPPORT SÄKERHETSTJÄNST 2004


## Omslagsbilder

1 LA02 Liberia. Foto: FBB/Rick Forsling
2 Jas 39 Gripen. Foto: SAAB/Caspersson
3 Bärgning DC 3:an.
Foto: FBB/Andreas Karlsson
4 Våreld 2003. Foto: FBB/Andreas Karlsson
5 Våreld 2003. Foto: FBB/Andreas Karlsson
6 Foto: Digital Vision

## Foton inlaga

Sid 6-7 KS04, Kosovo. Foto: FBB/Erik Thulin
Sid 8 Mönstring, IQ-test, Pliktverket. Foto: FBB/Lasse Sjögren
Sid 9 ”Mindungen”, Kosovo. Foto: FBB/Andreas Karlsson
Sid 10 Svenska soldater i Fassama, Liberia. Foto: FBB/Rick Forsling
Sid 11 Hedersvakt inför kungens besök, Kosovo. Foto: FBB/Andreas Karlsson
Sid 12 ISAF utbildar poliser i Afghanistan. Foto: FBB/Henrik Berger
Sid 13 Snöstorm 2001 Strf 90. Foto: FBB/Ivar Blixt
Sid 14-15 HMS Halland i Hårsfjärden. Foto: FBB/Roger Argerius
Sid 16 LSÖ 01. Foto: FBB/Lasse Sjögren
Sid 17 LSÖ 01 Bataljonsstab IS Mark. Foto: FBB/Lasse Sjögren
Sid 19 Kommunikationssysem, stridcentral. Foto: FBB/Peter Liander, Art Explosion
Sid 20 Brandövning. Foto: FBB/Thomas Wingstedt
Sid 24 Pansarsoldater, Våreld 2003. Foto: FBB/Lennart Andersson
Sid 25 Afghanistan. Foto: Peter Bengtsson
Sid 26 Våreld 2003, Tidaholm. Foto: FBB/Andreas Karlsson
Sid 27 Strong Resolve, Polen. Foto: FBB/Peter Liander
Sid 28 Minförråd. Foto: FBB/Andreas Eliasson
Sid 29 Hkp 4, Våreld 2003. Foto: FBB/Andreas Karlsson
Sid 31 Teleskopmast till AP. Foto: FBB/Lasse Sjögren
Sid 32 LSÖ 01, Boden. Foto: FBB/Lasse Sjögren
Sid 33 Trika. Foto: FBB/Lasse Sjögren
Sid 34 Hemvärnsman. Foto: FBB/Sven-Åke Haglund
Sid 36 Svenska soldater i Monrovia, Liberia. Foto: FBB/Rick Forsling

Denna årsredovisning publiceras även på Försvarsmaktens hemsida på internet (www.mil.se, sökord ”årsäk04”).

Omslaget är tryckt på Silverblade Silk 170 g och inlagan på Silverblade Silk 115 g.


Grafisk form: FMLOG Serviceenhet Stockholm C – ToD.
Tryckeri Bodoni Tryck AB – Stockholm 2005.

# Innehållsförteckning

# Den militära säkerhetstjänsten

## Omfattning

Militär säkerhetstjänst omfattar *säkerhetsunderrättelsetjänst* och *säkerhetsskyddstjänst*.

*IT-säkerhet* är en del av säkerhetsskyddstjänsten och nämns som regel särskilt på grund av dess omfattning och betydelse.

*Signalskyddstjänst* är en säkerhetsskyddsangelägenhet och tillsammans med IT-säkerhetstjänsten utgör den grunden för den tekniska informationssäkerheten.

Den militära säkerhetstjänsten arbetar alltså inom fyra nära samverkande delfunktioner:

- *säkerhetsunderrättelsetjänst*
- *säkerhetsskyddstjänst*
- *IT-säkerhetstjänst*
- *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 och säkerhetsskydd redovisas under kapitlet om säkerhetsskydd.

*Säkerhetsskyddstjänsten* arbetar inom områdena:

- *informationssäkerhet*
- *säkerhetsprövning*
- *säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)*
- *information, utbildning, stöd och kontrollverksamhet*
- *tillträdesbegränsning*
- *internationella säkerhetsfrågor*

*IT-säkerhetstjänsten* har som mål att:

- tillse att IT-infrastruktur, IT-system, information och anläggningar såväl inom som utom landet har *erforderligt* skydd.
- detektera, avbryta, återställa (och återgälda) angrepp eller försök till angrepp på information, IT-infrastruktur och IT-system.
- förhindra att information som rör rikets säkerhet kommer obehöriga till del.

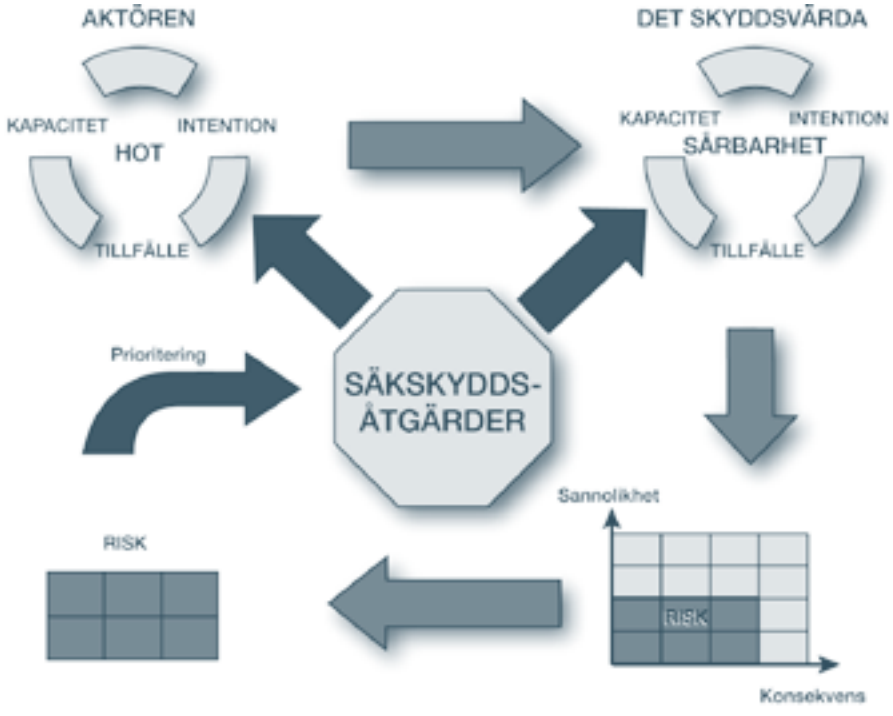
*Signalskyddstjänsten* syftar till att förhindra obehörig insyn i och påverkan av totalförsvarets informations- och kommunikationssystem, samt övrig användning av kryptografiska funktioner i informationssystem.

*TIGERN, med devisen "En svensk tiger", har utgjort symbol för den militära säkerhetstjänsten sedan 1940-talet.*

Den militära säkerhetstjänsten ska verka förebyggande genom att beskriva den säkerhetshotande verksamheten på kort och lång sikt för att skyddsåtgärder ska kunna vidtas i tid.

Verksamhetsanalys- analysen inleds med att det skyddsvärda identifieras. Därefter görs en bedömning av hotet, sårbarheten och risken, som ligger till grund för förslag om säkerhetsskyddsåtgärder. Hotet är en bedömning av aktörens *kapacitet, intention* och *tillfälle*. Hotet bedöms i fem nivåer utifrån sannolikheten att någon skall bedriva den aktuella säkerhetshotande verksamheten riktad mot det skyddsvärda. Sårbarheten är hotets motsats, d v s det skyddsvärdas kapacitet, intention och tillfälle. Risken är produkten av sannolikheten och konsekvenserna. Säkerhetsskyddsåtgärder kan vidtas och riktas både mot hotet och sårbarheten och syftar till att minska risken. Eftersom vidtagna säkerhetsskyddsåtgärder påverkar de övriga faktorerna i analysmodellen och leder till ett förändrat läge skall säkerhetsanalysen inte ses som en isolerad företeelse med en klart definierad början och slut utan som en ständig, föränderlig analysprocess.

Den militära säkerhetstjänsten leds på central nivå inom Försvarsmakten av den Militära underrättelse- och säkerhets-




*Modellen visar vilka komponenter och moment som ingår i en säkerhetsanalys. Modellen är generell och kan användas vid analys av alla typer av säkerhetshot och traditionella militära hot.*

tjänsten (MUST). Chefen för MUST är Försvarsmaktens säkerhetsskyddschef och tillika chef för totalförsvarets signalskyddstjänst.

Överbefälhavaren, genom chefen för MUST, utövar styrning av säkerhetstjänsten på regional nivå (MD) och på lokal nivå (garnisoner) genom främst *normgivning*. Normerna uttryckta i författningsform (FFS och FIB) utvecklas i *handböcker* (H SÄK) vilka sedan används vid *utbildning*.

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

Den militära säkerhetstjänsten samverkar på alla ledningsnivåer med polisen.

I det fall då den militära säkerhetstjänsten misstänker att brott begåtts eller är på väg att begås, överlämnas ärendet till polisen. Den militära säkerhetstjänsten har inga befogenheter att bedriva polisiär verksamhet.

## Rättsliga förändringar

### Föreskrifter och interna bestämmelser

Den 1 januari 2004 trädde Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd och Försvarsmaktens interna bestämmelser (FIB 2003:3) om IT-säkerhet i kraft.

Det främsta syftet med dessa föreskrifter och interna bestämmelser är att anpassa säkerhetsskyddet utifrån de internationella krav som ställts på Sverige, bland annat genom de säkerhetsbestämmelser som har meddelats av Europeiska unionens råd samt de säkerhetskrav om ställts på Sverige genom deltagandet i samarbetet inom Partnerskap för fred (PFP).

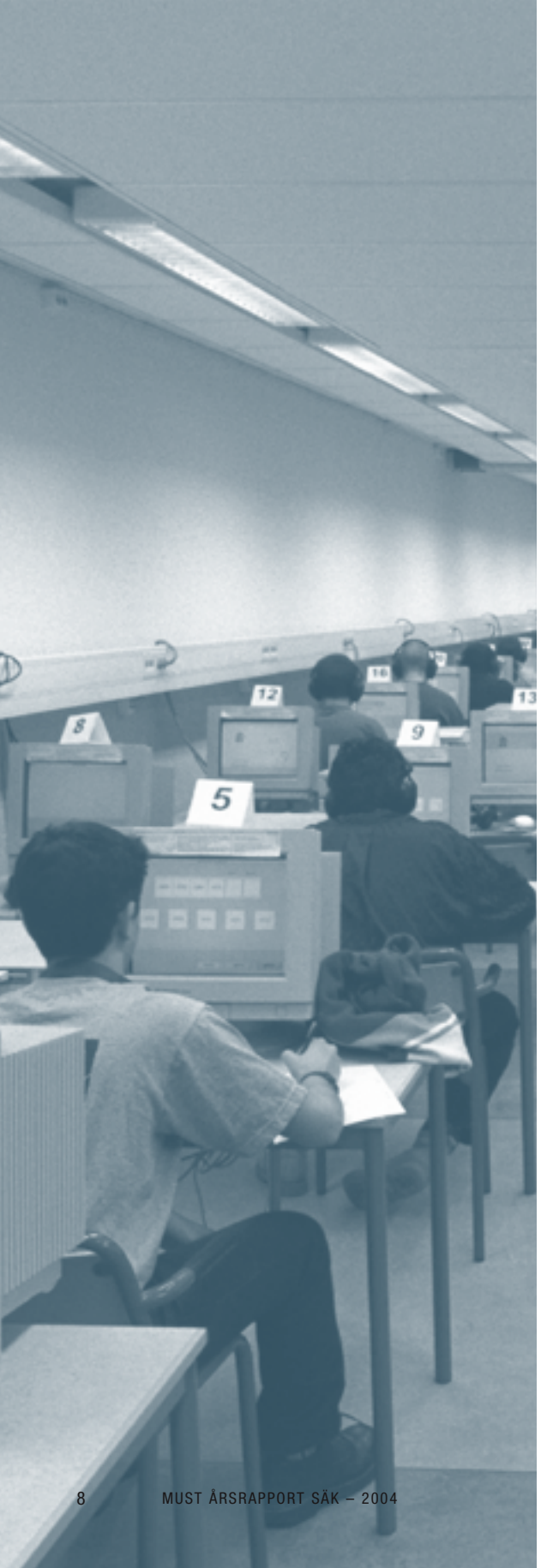
För att ge en bättre förståelse för författningarnas tillämpning gav MUST ut kommentarer till nämnda författningar (HKV 2004-04-07, bet.10 700:66177).


## Handböcker i säkerhetstjänst

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

På grund av förseningar i framtagandet av nya författningar (FIB säkerhetsskydd som bedöms fastställas första halvåret 2005) har framtagandet av nya publikationer i H-SÄK-serien försenats.

Handboksserien är, förutom smärre ändringar och total omarbetning av enstaka kapitel, f.n. endast uppdaterad vad gäller sådant som påverkats av de nya författningarna. Gjorda ändringar och uppdateringar framgår av CD-skivan ”Säkerhetstjänst”. Denna kommer fortsättningsvis att ges ut årligen i december, men utgåva 9 (tänkt utgivning december 2003) har försenats i avvaktan på fastställandet av ny FIB säkerhetsskydd.



## Utbildning

Under året gav MUST SÄK i samverkan med HKV GRO UTB, ut en webbaserad grundläggande säkerhetsutbildning där samtliga anställda vid Försvarsmakten, under 2004 fått möjligheten att vid sin dator och när tiden medgivits, att utbilda sig i grundläggande säkerhetstjänst samt genomföra ett slutprov.

Utbildningsunderlaget är kapitelindelat för varje delfunktion. Varje kapitel avslutas med flervalsfrågor, där svar kommer direkt. Efter att samtliga kapitel är genomgångna kan ett slutprov genomföras. Är alla svaren rätt i slutprovet skrivs ett diplom ut för den personen som genomfört slutprovet. Diplomet skrivs under av närmaste chef och överlämnas till den lokakala säkerhetschefen för uppföljning.

# Säkerhetshotande verksamhet

## Inledning

Årets beskrivning av den säkerhetshotande verksamheten är inte lika omfattande som återredovisats i ÅR SÄK 2002 och 2003. De beskrivningar av hot, hotbedömning och generell inriktning för säkerhetsunderrättelsetjänsten som redovisats tidigare år är fortfarande aktuell. Syftet med dessa beskrivningar är att öka förståelsen för säkerhetshotande verksamhet och beslutsunderlag för policyfrågor till att beskriva vilken information som behövs för att skapa ett väl avvägt säkerhetsskydd. Förnyat studium av de senaste två årens ÅR SÄK rekommenderas.

I samverkan med RPS och SÄPO har ett stort antal säkerhetshotbilder tagits fram avseende Försvarsmaktens verksamhet och intressen såväl inom landet som utlandsverksamheten. Dessa har omsatts till olika åtgärder inom Försvarsmakten för att tidigt förhindra eller avvärja identifierade hot.

Under året har följande (insatser) genomförts:

- Ett omfattande arbete har gjorts för att ta fram och presentera bedömningar avseende säkerhetshot inför internationell verksamhet.
- Underrättelseverksamheten riktad mot Försvarsmaktens utveckling har särskilt studerats.
- Hotbildsutbildningen har varit omfattande, i syfte att informera om säkerhetshotbilden och för att öka säkerhetsmedvetandet.
- Ett antal utredningar har genomförts i syfte att klarlägga säkerhetshotande verksamhet eller för att identifiera personer som varit olämpliga ur säkerhetssynpunkt. Några av dessa utredningar har resulterat i omplaceringar.
- Säkerhetsunderrättelsetjänsten har kraftsamlat till att identifiera olika aktörers intentioner avseende underrättelseverksamhet och kriminalitet riktat mot Försvarsmaktens intressen.
- Terrorhotet har främst bearbetats avseende hoten mot Försvarsmaktens intressen utomlands.
- Säkerhetsunderrättelsetjänsten har ökat sin operativa verksamhet, framför allt i våra missionsområden.

## Generell hotbild

För första gången sedan 1927 är officerare föremål för uppsägning på grund av arbetsbrist. Även en stor grupp civilanställda kommer att drabbas av uppsägning. Detta kan innebära att försvarsmaktsanställda känner besvikelse mot Försvarsmakten (FM) som arbetsgivare. För den uppsägningsberörde medarbetaren kan en personlig osäker ekonomisk och social framtidssituation väntas, där naturliga och trygga kontaktnät hotas. Som en följd av detta finns en risk att medarbetare, medvetet eller omedvetet, kan komma att eftersätta gällande säkerhetsskyddsbestämmelser och härvid direkt eller indirekt agera säkerhetshotande mot FM intressen på både kort och lång sikt.

Resultatet av detta kan få allvarliga konsekvenser för FM över lång tid.

Chefers vilja, förmåga och förståelse för en väl fungerande säkerhetstjänst är av stor betydelse för FM, oavsett var i organisationen dessa chefer återfinns. Det bör i detta sammanhang påpekas att alla och envar har och ska ta ansvar för att säkerhetstjänsten fungerar i hela FM. Lika självklart som förståelsen och medvetenheten om risken för minor och oexploderad ammunition utgör vid internationella insatser, lika självklart och naturligt ska olika säkerhetshot beaktas och säkerhetsskyddsbestämmelser följas i det dagliga arbetet inom FM verksamhet. Såväl humana som ekonomiska värden utsätts för betydande risker om säkerhetstjänsten eftersätts.

I dagens FM och för dess anställda är det internationella engagemanget en naturlig del med fredsbevarande operationer under FN, EU och NATO flagg m.m. Annan internationell verksamhet genomförs i oförminskad omfattning, t.ex. övningar med andra nationer, såväl inom som utom vårt lands gränser. Övergripande genomförs dessa i syfte att skapa interoperabilitet inför framtida insatser samt skapa förtroende och avspänning. Det är fullt naturligt att vänskapsband knyts i dessa sammanhang. Det bör dock påpekas att alla nationer i olika utsträckning har behov att skydda information rörande personal, dokument, utrustning och anläggningar, FM utgör här inget undantag.

Vid den här typen av verksamhet är det av stor betydelse att en säkerhetsanalys genomförs och att en säkerhetsplan upprättas för att undvika att bl.a. informationsförluster inträffar. Vidare, att med stöd av säkerhetsanalysen och säkerhetsplanen få andra aktörer att uppfatta FM som professionell och att förtroende för vår förmåga skapas. Härvid är det av betydelse att bestämmelser rörande kontakter med andra nationer följer gällande protokollära bestämmelser, såväl före som efter genomförd verksamhet. Att t.ex. upprätthålla personliga kontakter efter genomförd verksamhet kan innebära säkerhetsrisker.

Med den tydliga inriktningen att FM framtida roll är internationella insatser, är det viktigt att påminna om, och inte bortse från att FM huvuddel finns kvar inom landets gränser på olika verksamhetsorter och platser. Det är därför av vikt att säkerhetstjänsten på det nationella planet inte eftersätts och att FM verksamhet i Sverige har erforderligt säkerhetsskydd mot det säkerhetshot som alltjämt finns i den fredliga vardagen.

## Underrättelseverksamhet

Det har under året inkommit rapporter som tyder på såväl infiltrations- som rekryteringsförsök samt oförminskad främmande underrättelseverksamhet som riktas mot Försvarsmakten och dess intressen. Detta har skett både i Sverige och i utlandet. I några fall har utredningar som berört infiltrations- och rekryteringsförsök inneburit att åtgärder vidtagits i olika omfattning och grad för att såväl avbryta, förhindra som förebygga detta hot.

## Terrorism

Under året har inget direkt hot riktats mot Försvarsmakten, men indirekta hot förekommer vid internationell verksamhet beroende av vilka andra nationer som deltar i verksamheten. Hot om infiltration finns och följs därför nogsamt.

## Subversion

Inget fall av subversion har konstaterats under året, men indirekt förekommer detta vid internationella insatser och då främst riktat mot den organisation som leder operationen. Uppföljning har genomförts under året rörande utvecklingstendenser inom främst s.k. informationsoperationer. Vidare är det ur ett policyperspektiv viktigt för Försvarsmakten att, extrema grupper i samhället som inte följer demokratiska grundvärden, inte kan infiltrera och härvid bereda sig militär kunskap för egna syften. Detta berör såväl grundutbildning av värnpliktiga som hemvärns- och frivilligorganisationerna.

## Sabotage

Inget fall av sabotage har förekommit under året. Åverkan och skadegörelse kan härledas till kriminella handlingar eller förberedelser till kriminalitet.

## Kriminalitet

De kriminellas våldsbenägenhet i samhället har ökat vilket i sig är oroande. Försvarsmakten följer detta och anpassar skyddsåtgärder bl.a. efter dessa tendenser. För Försvarsmakten är nivån på den kriminalitet som riktas mot verksamheten och dess intresseområden oförändrad och har inte ökat under 2004.

Den vanligast förekommande kriminaliteten riktad mot Försvarsmakten i Sverige är vardagsbrottslighet i form av stölder och ekonomiska brott. I viss utsträckning är kriminaliteten mot Försvarsmakten organiserad då den är bunden till geografiska områden och objektstyp, dock bedöms den inte vara av grovt organiserad typ. Dessa kriminella är kända av polisen och flera är lagförda efter brott riktade mot Försvarsmakten.

Den allvarligaste typen av kriminalitet är de hot som riktas mot vapen och ammunition. De senaste årens intresse för vapen och ammunition i bruk vid Försvarsmaktens utbildningsplattformar och hemvärnsvapen är oförändrad.

I samband med internationella insatser är det kriminella hotet av överförd art och av grovt organiserad typ. I vissa fall kan denna organiserade kriminaliteten betraktas som en aktör i konfliktområdet. Dock utgör denna kriminalitet inte ett direkt hot mot Försvarsmakten i insatsområdena. Vardagskriminalitet förekommer och skiljer sig inte från svenska förhållanden.

# Säkerhetsskydd

## Allmänt

Säkerhetsskyddstjänsten arbetar inom områdena:

- informationssäkerhet
- säkerhetsprövning
- säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)
- information, utbildning, stöd och kontrollverksamhet
- tillträdesbegränsning
- internationella säkerhetsfrågor

## Ledning

### Allmänt

Det försvarsbeslut som fattades under 2004 kommer att medföra nya organisationsförändringar och behov av nya rutiner och samarbetsformer mellan de olika ledningsnivåerna (se nedan).

### Territoriell ledning

Under 2002 respektive 2003 genomfördes två utredningar av militärdistriktens organisation. Dessa skulle ligga till grund för beslut om territoriell ledning i försvarsbeslutet 2004. Så blev det inte, i stället har en ny utredning av territoriell ledning med inriktningen att avveckla militärdistriktsorganisationen genomförts. Utredningen pekar på att militär säkerhetstjänst erfordras där militär verksamhet bedrivs. Som konsekvens av FB 04 kan fyra områden i Sverige identifieras där huvuddelen av den militära verksamheten kommer att bedrivas. Det är övre Norrland, Mälardalen, västra Götaland och sydöstra Götaland. I dessa områden bör säkerhetstjänsten vara representerad. Utredningen föreslår att fyra ledningsgrupper med säkerhetsfunktion upprättas inom dessa områden. Grupperna skall ledas av OPIL men säkerhetstjänsten skall funktionsledas av MUST.


## Informationssäkerhet

Det militära hotet synes ha nedgått, åtminstone i det korta tidsperspektivet, medan andra typer av hot har ökat. Även fortsättningsvis krävs därför att hemliga uppgifter och säkerhetskänslig verksamhet hanteras på ett korrekt sätt ur informationssäkerhetssynpunkt .

Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd innebär att fyra informationssäkerhetsklasser införts. Bakgrunden har dels varit att erhålla ett balanserat skydd för hantering av hemliga uppgifter[1)], dels att anpassa våra bestämmelser utifrån de krav den internationella verksamheten ställer.

För att hemliga uppgifter skall kunna

1) En hemlig uppgift är enligt 4 § Säkerhetsskyddsförordningen en uppgift som omfattas av sekretess enligt sekretesslagen och som rör rikets säkerhet. Enligt samma paragraf är en hemlig handling en handling som innehåller hemlig uppgift. Även uppgifter som omfattas av sekretess enligt 2 kap. 1 § sekretesslagen, om utrikessekretess, och 5 kap. 1 §, om förundersökningssekretess, kan tillhöra kategorin ”av betydelse för rikets säkerhet” och därmed vara hemliga.

hanteras på bästa sätt med hänsyn till verksamheten är det viktigt att alla hemliga handlingar inplaceras i rätt informationssäkerhetsklass. En felaktig informationssäkerhetsklass för en hemlig handling kan innebära att säkerhetsskyddsåtgärder och begränsningar i behörighet leder till att verksamheten försvåras på ett onödigt sätt eller att säkerhetsskyddet blir för lågt. Det är den aktuella informationssäkerhetsklassen för en hemlig handling som styr vilket säkerhetsskydd som krävs.

Eftersom sekretesslagen inte har ändrats så skall även fortsättningsvis sekretessnivån hemlig eller kvalificerat hemlig anges på en hemlig handling[2]. Därutöver skall aktuell informationssäkerhetsklass anges på den hemliga handlingen[3].

Införandet av informationssäkerhetsklasserna har inneburit att Handbok för Försvarsmaktens Säkerhetsskyddstjänst Sekretessbedömning (H SÄK Sekrbed 1999) inte längre är tillämpbar fullt ut vid sekretessbedömning. En nyutgåva som eventuellt får ett annat namn är inplanerad och arbetet kommer att påbörjas under 2005.

I väntan på en ny handbok för sekretessbedömning har MUST givit ut kompletterande riktlinjer att använda vid inplacering av hemliga uppgifter i informationssäkerhetsklass. Avsikten med dessa riktlinjer är att de ska utgöra ett stöd vid inplacering av hemliga handlingar i informationssäkerhetsklass. Med detta följer att behovet av säkerhetsskydd och hanteringsbestämmelser för aktuella hemliga handlingar klarläggs.

2) Se 2 kap. 1 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd.
3) Se 2 kap. 2 och 3 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd.

Ansvaret för inplacering av hemliga handlingar i informationssäkerhetsklass åligger upprättaren av handlingen. Detta ansvar skall även tas av chefer och övriga när det gäller klassning och hantering av hemliga uppgifter som i övrigt hanteras inom ramen för säkerhetskänslig verksamhet. Även inkomna handlingar från såväl utlandet som från myndigheter utanför FM tillsynsområde och som har åsatts sekretessgrad, enligt deras respektive rutiner, skall placeras i informationssäkerhetsklass under förutsättning att sådana handlingar innehåller hemliga uppgifter. Rutiner för detta bör regleras i lokala säkerhetsbestämmelser.

Vid inplacering av hemliga uppgifter i informationssäkerhetsklass utgår man från det men (skada) som bedöms kunna uppstå för totalförsvaret eller i förhållandet till annan stat eller mellanfolklig organisation eller i annat fall för rikets säkerhet om de aktuella uppgifterna röjs.

I skrivelsen *Riktlinjer vid inplacering av hemlig uppgifter i informationssäkerhetsklass* (HKV 2004-05-18, bet. 10 440:68631) finns tabellen på nästa uppslag redovisad vilken tillsammans med Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd och nuvarande H SÄK SekrBed 1999 utgör ett stöd vid inplacering av hemliga uppgifter i informationssäkerhetsklass. Denna metod kan tillämpas även när det gäller handlingar som har upprättats vid myndigheter utanför Försvarsmakten tillsynsområde och som är inkomna till Försvarsmakten och därmed skall placeras i informationssäkerhetsklass.

Fördelning av hemliga handlingar mellan de fyra informationssäkerhetsklasserna går inte att på förhand bestämma, men det torde bli att en mindre del hemliga hand-

lingar placeras i informationssäkerhetsklass HEMLIG/TOP SECRET, därefter med ökande andelar i HEMLIG/SECRET och HEMLIG/CONFIDENTIAL för att merparten av handlingarna slutligen inplaceras i HEMLIG/RESTRICTED.

## Teknisk informationssäkerhet

### Beslut om regler för användning av Försvarsmaktens IT-system

Från och med den 1 januari 2005 gäller *Beslut om regler för användning av Försvarsmaktens IT-system* (HKV skr 2004-10-29, bet. 20 400:75133). Beslutet ersätter den tidigare policyn för användning av Försvarsmaktens e-post och Internet (HKV skr 2003-05-12, bet. 09 626:66449). Försvarsmaktens IT-system är i första hand till för att lösa arbetsuppgifter, men det blir även i fortsättningen tillåtet att under vissa förutsättningar använda t.ex. e-post och Internet för privata ändamål.

Beslutet gäller för all personal i Försvarsmakten som skall använda myndighetens IT-system, dvs. både civil och militär personal.

Den största skillnaden mellan beslutet och den tidigare policyn är att alla användare nu måste skriva på att de har tagit del av reglerna för att få använda IT-systemen, vare sig de tänker använda dem för privat bruk eller inte. Om man även vill ha möjlighet att använda IT-systemen för privata

| Informationssäkerhetsklass | Ett röjande av uppgift kan medföra…….men. |
|---|---|
| HEMLIG/TOP SECRET | Ett röjande av uppgift kan medföra **synnerligt** men.<br><br>I sekretessbedömningen framkommer ”nyckelord” som t ex:<br>- direkt hot (mot Försvarsmaktens totala förmågor)<br>- synnerligen allvarlig skada<br>- synnerlig stor omfattning<br>- synnerligen allvarliga långsiktiga konsekvenser<br><br>Samma metod som användes för att placera uppgifter i sekretessnivån kvalificerat hemlig kan tillämpas vid placering i informationssäkerhetsklassen HEMLIG/TOP SECRET.<br><br>Informationen är placerad i Top Secret eller motsvarande av en utländsk myndighet eller mellanfolklig organisation. |
| HEMLIG/SECRET | Ett röjande av uppgift kan medföra **betydande** men.<br><br>I sekretessbedömningen framkommer ”nyckelord” som t ex:<br>- direkt hot (mot Försvarsmaktens avgränsade förmågor)<br>- allvarliga konsekvenser<br>- stor omfattning<br>- väsentlig<br><br>Informationen är placerad i Secret eller motsvarande av en utländsk myndighet eller mellanfolklig organisation. |

›

ändamål måste man dessutom lämna sitt samtycke till att Försvarsmakten får genomföra kontroller från säkerhetssynpunkt av både nätverkstrafiken och vad man lagrar i Försvarsmaktens IT-system, även vad avser dess innehåll.

Ett sådant samtycke är frivilligt, men den som väljer att inte lämna sitt samtycke får då heller inte använda IT-systemen för privata ändamål, t.ex. skicka privata e-postmeddelanden eller lagra filer av privat karaktär. Den privata användningen får heller inte vara av sådan omfattning att den inkräktar på användarens tjänsteutövning.

Vidare anges i beslutet vad en användare skall beakta vid användning av myndighetens IT-system.

Här kan särskilt nämnas följande.

- Meddelanden (t. ex. e-post) är normalt inte skyddade från insyn.
- E-post kan komma att uppfattas som myndighetens e-post.
- Prenumeration på nyhetsbrev m.m. kan generera skräppost.
- Internetsurfande lämnar spår.
- Användning får inte stå i strid med någon föreskrift i författning, som t.ex. 4 kap. 9 c § brottsbalken (dataintrång).

De kontroller som utförs görs med stöd av säkerhetsskyddslagen (1996:627) och Försvarsmaktens interna bestämmelser (FIB 2003:3) om IT-säkerhet. Försvarsmakten har inte någon möjlighet att särskilja privat

| | |
|---|---|
| **HEMLIG/CONFIDENTIIAL** | Ett röjande av uppgift kan medföra ett **icke obetydligt** men.<br><br>I sekretessbedömningen framkommer ”nyckelord” som t ex:<br>- påtaglig<br>- begränsad omfattning<br>- äventyra<br>- vålla skada<br>- hindra<br>- underlätta (för brottslingar)<br>- innebära större avbrott<br><br>Informationen är placerad i Confidential eller motsvarande av en utländsk myndighet eller mellanfolklig organisation. |
| **HEMLIG/RESTRICTED** | Ett röjande av uppgift kan medföra **ringa** men.<br><br>I sekretessbedömningen framkommer ”nyckelord” som t ex:<br>- påverka<br>- försvåra<br>- mindre omfattning<br>- hindra<br>- undergräva<br>- misskreditera<br><br>Informationen är placerad i Restricted eller motsvarande av en utländsk myndighet eller mellanfolklig organisation. |

information från arbetsrelaterad information i IT-systemen, vilket i praktiken innebär att även privata filer kan förekomma på det lagringsmedia som kontrolleras. Eftersom även privata filer kan innehålla skadlig kod eller hemliga uppgifter, finns det ett behov av att utföra kontroller i Försvarsmaktens IT-system från säkerhetssynpunkt också av sådana filer. Det får inte förekomma kontroller som utförs med ett annat syfte än från säkerhetssynpunkt.

Myndigheten har givetvis rätt att begränsa tillgången till Försvarsmaktens IT-system, liksom hela eller vissa delar av Internet. Myndigheten får även, efter samråd med MUST, besluta att inskränka privat användning i fråga om ett visst IT-system.

### Auktorisation

MUST gav under 2004 stöd till krigsförbandsledningen (Ledningsinspektören, LI) i Försvarsmaktens auktorisationsprocess.

Genom IT-säkerhetsavdelningens (MUST ITSA) stöd till auktorisationsgruppen med IT-säkerhets- och signalskyddsexpertis, har Försvarsmaktens krav på IT-säkerhet och signalskydd kunnat tillgodoses vid framtagning av nya och vidareutveckling av befintliga IT-system. ITSA handlade ett stort antal auktorisationsärenden inom sitt sakområde under 2004.

Här kan särskilt nämnas ett auktorisationsärende, med tanke på Försvarsmaktens nya IT-säkerhetsbestämmelser. DATASLUSS är ett IT-system som är under framtagning och som är tänkt att möjliggöra kommunikation mellan IT-system som är avsedda för behandling av uppgifter med olika klassning. DATASLUSS skall således kunna möjliggöra kopplingar mellan till exempel publika nätverk och Försvarsmaktens IT-system som är avsedda för behandling av hemliga uppgifter.

Även i MUST:s interna auktorisationsgrupp har ITSA bidragit till att MUST-interna IT-system har kunnat tas i drift för bl.a. prov- och försöksverksamhet.

### Yttranden inför ackreditering

Under tiden fram till och med 2004 har IT-säkerhetsavdelningen haft uppgiften att yttra sig över säkerheten i Försvarsmaktens IT-system inför produktägarens beslut i fråga om godkännande från säkerhetssynpunkt (ackreditering). Under 2004 har mer än ett 30-tal sådana ackrediteringsärenden hanterats, både för system som är avsedda för behandling av hemliga uppgifter och för övriga IT-system. Ett antal ackrediteringsärenden har rört Försvarsmaktens internationella insatser och deltagande i olika övningar.

De av chefen för MUST beslutade kraven på godkända säkerhetsfunktioner började under slutet av 2004 göra sig gällande i ett fåtal ackrediteringsärenden, både för så kallade insats- och verksamhetsledningssystem.

### Tekniska utredningar

Det har under 2004 genomförts ett stort antal tekniska utredningar ur säkerhetssynpunkt. Flertalet av dessa har påvisat brister vad avser efterlevnad av regelverk. Många har även lett till att Försvarsmaktens personal- och ansvarsnämnd (FPAN) varit inkopplad. De tekniska utredningarna har varit ett komplement till utredningar som bedrivits vid förband, militärdistrikt samt Högkvarteret. Ett fåtal tekniska utredningar har även genomförts i samarbete med andra myndigheter, t ex FMV.

### Produkter

IT-säkerhetssektionen har under 2004 medverkat i arbetet att få fram en godkänd produkt för överskrivning av information på magnetiska lagringsmedia såsom hårddiskar eller magnetband. Inom ramen för detta arbete har det utförts tester av produkter samt begäran om auktorisation. IT-säkethetssektionen har även medverkat i arbetet att inköpa licenser tillsammans med FMLOG och KRI LED. I detta arbete har IT-säkerhetssektionen även utvärderat och godkänt en Degausser avsedd att förstöra information genom avmagnetisering. Direktiv för användning av dessa produkter har har givits ut i samband med detta arbete.

En plattform för kontroll av IT-säkerhet inom Försvarsmakten, kontrollverktyg för IT-säkerhetschefer, har tagits fram. Detta arbete har inneburit dels framtagande av verktygsplattformen samt direktiv för användning. En utbildning som är ett förkunskapskrav för att få använda plattformen har producerats i samarbete med Halmstadsskolorna. I december 2004 hölls den första kursen som

en del i ett pilotprojekt. Ett tiotal personer har genomgått kursen med godkänt resultat och licenser har distribuerats till förband.

### IT-säkerhetsrelaterade incidenter

FM CERT som under 2004 ingick i IT-säkerhetssektionen vid MUST ITSA ansvarade under året för insamling, hantering och koordinering av IT- säkerhetsrelaterade incidenter. Antalet inrapporterade incidenter har under året legat på en nivå motsvarande 2003. Av de inrapporterade incidenterna kan nämnas att de flesta rör hantering av sekretessbelagd information på nätverk och datorer avsedda för icke sekretessbelagd information.

De virusrelaterade incidenter som har rapporterats till FM CERT har i de flesta fallen gått att relatera till konfiguration av antivirusprogramvara och till inkoppling av bärbara datorer på lokala nätverk. Under våren drabbades flera lokala nätverk av masken Sasser. Masken kom in i nätverken genom att bärbara datorer som varit anslutna mot Internet, olovligen kopplades in på nätverket.

Under 2004 har vi sett en kraftig ökning av skadlig kod som spridits med e-post. Statistiken från Försvarsmaktens gateway mot Internet visar en ökning av stoppad skadlig kod på nästan 750 procent från 2003. Vi har också sett en ökning av antalet unika skadliga koder som spreds under året. En anledning kan vara att det nu är lätt att få tag i koden och ändra den så att antivirusprogramvaran inte kan detektera den. E-postmaskfamiljerna Netsky och Bagle har under året varit klart dominerande på området, och har stått för nästan 95 procent av den totala mängden stoppad skadlig kod.

En analys av den ökade mängden skadlig kod och att fler varianter av samma kod skapas, visar att vi inte längre kan säkerställa att den centrala antivirusprogramvaran hinner uppdateras för att kunna stoppa den skadliga koden. Detta innebär att användare av e-postsystemet måste bli mer varsamma på vad som mottages samt att inte öppna bifogade filer som inte är väntade.

Ett följdproblem som kommit med den ökade spridningen av e-postmaskar är att maskarna sprids med en ”stulen” e-postadress som avsändaradress. Adressen tas från den infekterade datorn, och överensstämmer nästan aldrig med den egentliga avsändaren. Många företag och organisationer hade under årets början konfigurerat sin antivirusprogramvara så att avsändaren av ett infekterat e-postmeddelande automatiskt blir informerad per e-post när ett infekterat e-postmeddelande upptäckts. Då avsändaradressen nästan aldrig överensstämde med den egentliga avsändaren drabbades oskyldiga inom Försvarsmakten av rapporter om att de spred skadlig kod. En bit in på året minskade problemen då många företag konfigurerade om meddelandefunktionen på sina e-postservrar.

### SPAM

Ett annat fenomen som uppmärksammats av användare i Försvarsmakten är antalet SPAM (skräppost) som inkommit till våra adresser. På vissa håll upplevs SPAM som ett problem då det tar tid att sortera bort SPAM från övrig e-post. I dag kan Försvarsmakten som myndighet inte överlåta klassificeringen av inkommande e-post till ett elektroniskt SPAM-filter. Som myndighet är vi skyldiga att säkerställa att den som vill komma i kontakt med oss per e-post också kan göra det. Vi får alltså inte stoppa e-post så länge vi inte med säkerhet kan garantera att e-posten verkligen är skräppost. Statskontoret och

flera andra myndigheter har under hösten tillsatt en grupp som tittar på en lösning av det ökande antalet SPAM till myndigheterna och Försvarsmakten avser följa gruppens slutsatser. För att minska risken för SPAM skall man vara väldigt restriktiv med att lämna ut sin e-postadress annat än till betrodda mottagare. Har man en gång fått ett SPAM skall man inte heller följa de anvisningar som finns om eventuell avregistrering, då detta bara bekräftar att man läst meddelandet och att e-postadressen används.

### Incidentrapportering

Under årets sista månad genomfördes en workshop i FM CERT regi där IT-säkerhetschefer på regional nivå, representanter från driftorganisationen och företrädare från OPIL samlades för att diskutera ämnet rapportering av IT-säkerhetsrelaterade incidenter. Några av slutsatserna som framkom var att rapportering skall ske via IS UNDSÄK, där de som skall tilldelas informationen tilldelas läsbehörighet. Detta kommer göra att informationen blir tillgänglig för såväl rapportör, FM CERT som övriga intressenter direkt vid rapportering.

Om inte IS UNDSÄK finns tillgängligt på den nivå där den IT-säkerhetsrelaterade incidenten inträffar skall incidenten rapporteras in i systemet vid nästa nivå i linjeorganisationen. Informationen skall också bearbetas i linjeorganisationen för att den centrala analysen skall bli så korrekt som möjligt.

För att FM CERT skall kunna delge en korrekt lägesbild vad avser säkerhetsläget i våra ledningssystem är det viktigt att vi blir bättre och noggrannare på att rapportera uppkomna incidenter.

### Slutsatser från FM CERT verksamhet 2004

- Användarna måste bli bättre på att säkerställa att sekretessen inte äventyras vid hantering av sekretessklassad information. Det är absolut förbjudet att hantera sekretessklassad information i IT-system, på datorer eller i nätverk som ej är avsedda 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.
- Vid uppkoppling till interna nätverk och LAN skall gällande bestämmelser följas. Vid ett flertal tillfällen har bärbara datorer varit orsaken till långvariga och resurskrävande avbrott i nätverk genom spridning av skadlig kod.
- Försvarsmakten har att säkerställa allmänhetens möjlighet till kontakt via e-post kan vi idag inte använda kommersiella SPAM-filter för att filtrera SPAM. Tillsvidare får därför oönskad e-post raderas manuellt hos respektive användare.
- FM CERT intar en delvis ändrad roll där huvuduppgiften blir att svara för en lägesbild avseende säkerhetsläget i Försvarsmaktens ledningssystem. FM CERT kommer fortfarande att stödja vid IT-säkerhetsrelaterade incidenter främst genom att koordinera aktuella insatser.
- Under 2005 fortsätter arbetet med att öka benägenheten och likrikta sättet att rapportera IT-säkerhetsrelaterade incidenter. Det huvudsakliga rapporteringssättet är via IS UNDSÄK där samtliga användare ges tillgång till informationen.

### FM CERT i framtiden

Under året som gått har arbete bedrivits för att fastställa FM CERT roll i framtiden. Arbetet har mynnat ut i en något ändrad roll för FM CERT. Huvuduppgifterna har fastställts till att vara:

- ansvara för en kontinuerlig lägesbild avseende säkerhetsläget i Försvarsmaktens ledningssystem
- stöd vid IT-säkerhetsrelaterade incidenter inom Försvarsmakten

För att lösa den första huvuduppgiften skall FM CERT kontinuerligt:

- bedriva insamling, korrelation och analys av IT-säkerhetsrelaterade incidenter
- bedriva omvärldsbevakning med fokus på sårbarheter i mjukvaror som används i våra ledningssystem
- bedriva särskild övervakning med egna implementerade verktyg
- delges den redan befintliga driftlägesbilden från driftägarna.

För att lösa den andra huvuduppgiften koordinerar och initierar FM CERT säkerhetskontorets stöd vid hantering av IT-säkerhetsrelaterade incidenter.


## Säkerhetsprövning

### Allmänt

Skyldigheten att företa säkerhetsprövning gäller inte bara dem som skall bli föremål för registerkontroll. Säkerhetsprövning skall också genomföras beträffande den som skall delta i verksamhet som har betydelse för rikets säkerhet utan att förutsättningarna för registerkontroll är uppfyllda.

Säkerhetsprövning innefattar:

- Säkerhetsanalys av anställning omfattande befattning som avses placeras i säkerhetsklass alternativt kontroll till skydd mot terrorism
- Rekrytering, anställning och urval
- Utbildning om hot och säkerhetsskydd
- Registerkontroll med i förekommande fall särskild personutredning
- Uppföljning under anställning, tjänstgöring och uppdrag
- Personsäkerhetsärenden

Säkerhetsprövningen är lagstadgad och skall ske innan en person anställs eller på något annat sätt deltar i Försvarsmaktens verksamhet där uppgifter av betydelse för rikets säkerhet förekommer. Säkerhetsprövningen omfattar alla personalkategorier som finns inom Försvarsmakten – anställda, värnpliktiga och frivillig personal. Säkerhetsprövning kan även innefatta kontroll mot polisregister och särskild personutredning. Registerkontroll och i vissa fall särskild personutredning, sker endast om anställningen eller verksamheten är placerad i säkerhetsklass eller kontroll till skydd mot terrorism.


Tyngdpunkten vid en säkerhetsprövning skall alltid ligga på personlig kännedom och inhämtade betyg, intyg och referenser. Registerkontroll och särskild personutredning skall ses som viktiga delar av säkerhetsprövningen.

En väl utvecklad samverkan mellan linjechefer 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 är lojala och pålitliga från säkerhetssynpunkt, inte tas i anspråk av Försvarsmakten.

Det är av oerhört stor vikt, från säkerhetssynpunkt, att följa upp anställda och övriga som deltar i Försvarsmaktens verksamhet, i syfte att tidigt uppmärksamma problem och vidta stödåtgärder för dem som riskerar att bli säkerhetsrisker eller som riskerar att utsättas för hot. Detta är av särskild vikt inför kommande omstrukturering av Försvarsmakten.

### Genomförd verksamhet 2004

Med början den 1 februari driftsattes RK-rutin 3.0 i IS UNDSÄK. Den nya rutinen innehåller tre huvuddelar, registrering, händelser, statistik och rapporter. I statistik

och rapportdelen sköts all administration av kontrollerna och behöver ej administreras i särskilda arkiv eller motsvarande. Detta har inneburit mer tid för kontroll och uppföljning av personal. Inledningsvis hade inte alla organisationsenheter tillgång till denna rutin i IS UNDSÄK. Detta innebar inledningsvis merarbete för främst militärdistriktsstaberna.

Förnyade registerkontroller i säkerhetsklass 3 för yrkesofficerare, reservofficerare och aspiranter har genomförts i stort enligt plan, dock återstår ett fåtal förband motsvarande som skall fullfölja sina registerkontroller. Totalt har under 2004 genomförts ca 20 000 nya registerkontroller vad avser anställning inom Försvarsmakten.

Anställning eller verksamhet som skall placeras i säkerhetsklass eller kontrolleras till skydd mot terrorism skall regelmässigt analyseras. Detta har inte genomförts fullt ut under 2004 och skall prioriteras och fullföljas under 2005.

## Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)

Under 2004 har ett antal myndigheter och förband kontrollerats utifrån hur de reglerar och hanterar sin SUA verksamhet. Omstruktureringen av Försvarsmakten, såväl genomförd som pågående och förestående, har medfört och medför ett ökat behov av köp (upphandling) av tjänster i verksamheter som kräver säkerhetsskydd med hänsyn till rikets säkerhet.

Kraven och resurserna är inte i balans, organisationen har inte vuxit in i det nya rollspelet. FMLOG:s uppgift som stöd åt kärnverksamheten i Försvarsmakten tolkas på olika sätt, både inom FMLOG och vid övriga Försvarsmaktens förband.

Inom Försvarsmakten har datorstöd för administration av SUA-företag och därtill hörande RK varit i bruk sedan årsskiftet, 2003-2004. Alla förband använder av olika skäl ännu inte funktionerna. Förväntade effekter av datorstödet i form av arbets-


tidsbesparing har uteblivit och därmed har önskad kraftsamling mot utbildning, uppföljning och kontroll fått skjutas framåt.

**Är det skillnad på säkerhetsskyddskravet vid anställning respektive köp av tjänst?**

**– Nej i princip inte.**

Säkerhetsskyddslagen (1996:627), som reglerar kraven på säkerhetsskydd med hänsyn till rikets säkerhet och säkerhetsskydd mot terrorism, gäller för staten, kommuner, landsting etc . Lagen gäller i princip inte företag.

Inom Försvarsmakten har varje förband ansvar för att upprätthålla för sin verksamhet erforderligt säkerhetsskydd.

Upphandlar ett förband en tjänst att utföras i sekretesskyddad verksamhet har förbandet ansvar för att erforderligt säkerhetsskydd åstadkoms.

Säkerhetsskyddslagen blir tillämplig för ett företag först efter det att ett säkerhetsskyddsavtal har slutits mellan företaget och förbandet. Detta avtal krävs för att reglera säkerhetsskydds-åtgärder avseende *informationssäkerhet (inkl IT-säkerhet), tillträdesbegränsning, säkerhetsprövning samt utbildning och kontroll.*

Utvecklingen har emellertid medfört att bolag med utländsk ledning är och kommer att vara verksamma inom Försvarsmaktens verksamhet. Det torde inte vara möjligt att utestänga utländska medborgare från känslig information. Detta är dock inte ett problem som kan lösas inom ramen för registerkontroll. Ibland erhålls via SÄPO, som vänder sig till motsvarande myndighet i den utländska medborgarens hemland, information om den utländske medborgaren. Ett sådant förfarande bör inte hindra eftersom kontrollen bygger på ett uttryckligt medgivande.

Här relaterade omständigheter utgör bakgrunden till den särlagstiftning, Lagen om offentlig upphandling (LOU), avseende upphandlingar som behöver skyddas med hänsyn till rikets säkerhet (LOU kap 6).


## Kontroller

Kontrollverksamhet är ett av säkerhetsskyddstjänstens delområden. Kontroll av säkerhets- och signalskydd skall förekomma på alla nivåer. Syftet med kontrollverksamheten är att säkerställa att föreskrifter,

bestämmelser och riktlinjer för säkerhets- och signalskyddstjänsten efterlevs samt att skyddsnivån är avpassad till aktuellt säkerhetshot. Kontrollerfarenheter ger som regel underlag för fortlöpande, kompletterande utbildning i säkerhets- och signalskyddstjänst.

MUST SÄKK genomför kontroller av säkerhetsskydd och signalskydd vid Högkvarteret, militärdistriktsstaberna och vissa andra förband samt vissa myndigheter under Försvarsdepartementet. Vidare får MUST genomföra kontroller i och kring IT-system som inte är avsedda för behandling av hemliga uppgifter. På regional nivå har C MD ansvar för att säkerhetsskyddet kontrolleras vid förband inom militärdistriktet. Stöd avropas från central nivå enligt särskilda bestämmelser. Såväl chefer som den enskilde är ansvariga för att säkerhetsskyddskontroller genomförs regelbundet. Den enskilde är enligt chefens närmare bestämmelser ansvarig för kontroll av egen arbetsplats eller eget arbetsområde.

Kontrollverksamheten indelas i; *planlagd säkerhetskontroll, överraskande säkerhetskontroll, särskild säkerhetskontroll samt säkerhetsskyddsbesök*.

Planlagda säkerhetskontroller verkställs utifrån en årligen rullande plan (kontrollplan). Planlagda kontroller utgörs av *grundkontroll* respektive *uppföljningskontroll*. Grundkontroller omfattar alla delområden inom säkerhetsskydds- och signalskyddstjänsten. Grundkontroller leder till att protokoll upprättas i vilket brister och förbättringsåtgärder dokumenteras.

Uppföljningskontroller omfattar enbart de områden inom vilket brister uppmärksammats vid föregående grundkontroll.

Överraskande säkerhetskontroll genomförs utan förvarning eller med kort förvar-

ning. Särskild säkerhetskontroll genomförs för att kontrollera viss verksamhet där ett akut säkerhetsproblem uppstått eller kan förutses uppstå. Ett exempel på särskild kontroll kan vara s k aktiv IT-kontroll. Syftet med denna är att pröva IT-systemens förmåga att motstå samt detektera intrång eller intrångsförsök. Denna typ av kontroll utförs endast av särskilt utbildad personal och enligt direktiv från MUST.

Säkerhetsskyddsbesök ersätter inte kontrollverksamhet men kan vara ett lämpligt tillvägagångssätt, t ex inför en grundläggande kontroll, som av olika skäl måst senareläggas eller för att stödja chefer vid nyetablering eller vid nya missioner i utlandsstyrkan. Syftet är därvid främst att klarlägga den kontrollerades läge i stort och behov av stöd avseende säkerhetsskyddet.

Som förberedelse inför en kontroll får den som kontrolleras ett underlag som beskriver kontrollens omfattning i stort. Cirka ett år före bestäms tidpunkten för kontrollen och cirka sex månader före bestäms kontrollens omfattning i stort. Två månader före fastställs kontrollens omfattning med detaljanvisningar och senast 14 dagar före sänds underlag i form av:

- förbandets arbetsordning
- andra interna bestämmelser som rör säkerhetstjänsten
- säkerhetsplan
- IT-säkerhetsplan
- förteckning över IT-system och lokala nätverk samt förteckning över personal med säkerhetsuppgifter från den kontrollerade till den kontrollerande.

Under 2004 har MUST SÄK och MUST ITSA genomfört säkerhetsskydds- och signalskydds-kontroller vid försvarsattachéavdelningarna vid de svenska ambassaderna i Bern, London, Singapore och Moskva. En kontroll genomfördes även vid blivande försvarsavdelningen vid Sveriges ambassad i Peking.

Grundkontroll har genomförts vid Pliktverket (PliktV). Uppföljningskontroller har genoförts vid Södra militärdistriktsstaben (MDS) samt vid Totalförsvarets forskningsinstitut (FOI). Säkerhetsskydds- och signalskyddskontroll har även genomförts vid Utlandsstyrkan i Kosovo av KS 09 och KS 10, i Liberia av LA 02, i Afghanistan av

FS 07 samt i Uzbekistan av FU 01.

Vidare har MUST ITSA vid ett flertal tillfällen under 2004 lämnat stöd i form av teknisk kompetens till Militärdistrikten vid genomförande av IT-säkerhetskontroller. Dessa kontroller har påfallande ofta visat på brister i överblicken över vilken information som finns inom den lokala informationsdomänen.

Resultatet av 2004 års kontroller är varierande. Flera kontroller har resulterat i att MUST SÄK och MUST ITSA konstaterat att säkerhets- och signalskydd vid de kontrollerade objekten håller en bra nivå och att gällande regler efterlevs. Där omedelbara åtgärder erfordrats för att uppnå en godtagbar skyddsnivå har så skett.

I de fall omedelbara åtgärder inte erfordras för att uppnå en godtagbar skyddsnivå åtgärdas bristerna efter särskilda åtgärdsplaner. I huvudsak är de identifierade bristerna relaterade till åtgärder som kan vidtas efter utbildning och övning i säkerhets- och signalskyddstjänst.

Vid kontroll av IT-säkerhet vid Utlandsstyrkan har särskilt uppmärksammats att bättre förutsättningar måste skapas, samt att erforderligt stöd måste ges för att IT-säkerheten skall uppfylla ställda krav.

Kontrollverksamheten är en viktig del av säkerhetstjänsten. Under år 2005 kommer MUST SÄK och MUST ITSA att fusioneras till ett Säkerhetskontor. I den nya organisationen, som skall arbeta processorienterat, har kontrollverksamheten blivit en egen delprocess. Organisationsförändringen och tydliggörandet av kontrollprocessen skapar förutsättningar för att kontrollfunktionen kan utvecklas samt att gemensamma resurser kan merutnyttjas.

Under 2005 kommer kontroller fortsatt vara en viktig del av den militära säkerhetstjänsten. Ansträngningarna för kontrollverksamheten kommer att bestå i att genomföra förändringar avseende organisation och arbetssätt samtidigt som kontroller fortlöper vid ett antal försvarsattachéavdelningar, myndigheter, militärdistrikt och samtliga enheter vid utlandsstyrkan.

Den tekniska IT-säkerhetskontrollen kommer att ominriktas under 2005, vilket i förlängningen kommer att innebära att stödverksamheten till enheter utanför militära underrättelse- och säkerhetstjänsten i Högkvarteret kommer att minska.

## Tillträdesbegränsning

### Allmänt

Under 2004 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 2005. Med anledning av Försvarsmaktens omstrukturering bedöms att risken för tillgrepp av kapitalvaror m.m. kan komma att öka. Med anledning av ovanstående är det väsentligt att kontroller av tillträdesbegränsning och avseende förvaring, hantering och transporter av skjutvapen och ammunition m.m. genomförs såväl lokalt som regionalt under 2005.

### Vapen och ammunition

Eftersom det blivit allt svårare att tillgripa skjutvapen och ammunition ur förråd, bedömer Försvarsmakten att hot istället 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 som framgår av bl.a. H SÄK VapAm 2000.

Under 2005 och ytterligare ett antal år framåt, kommer omstruktureringen av Försvarsmakten och den därmed sammanhängande avvecklingen av vapen och ammunition samt i viss utsträckning fortsatt överföring av materiel till Baltikum att ställa stora krav på bevakning i samband med arbete i förråd och vid transporter av skjutvapen och ammunition.

### Förlust av vapen

Ännu återstår en del innan ”nollvisionen” är uppnådd men en positiv trend är att under 2004 har tio vapen återbördats samt att en mindre del av det totala antalet för-

komna vapnen har skett genom tillgrepp. Huvuddelen av de förkomna vapnen var gevär. I de fall då AK 4 stulits har dessa varit försedda med patronlägeslås och bedöms därmed vara obrukbara.

Dock har ett antal enskilda patronlägeslås förlorats. Det är viktigt att trenden med ett omfattande antal förlorade patronlägeslås bryts.

### Hemvärnets vapenförvaring

Risken för tillgrepp av bostadsförvarade vapen är fortsatt hög. Under 2004 har hemvärnsmän i icke ringa omfattning förlagt sitt patronlägeslås, fått sitt patronlägeslås stulet eller förlorat det på annat sätt. Likaså har det inom FMLOG förlorats ett antal patronlägeslås. Detta innebär att det bland kriminella kan finns ett antal patronlägeslås som kan utgöra övningsobjekt inför försök att forcera det skydd mot obehörigt utnyttjande av vapnet som patronlägeslåset är avsett att utgöra.

Det är viktigt att trenden med ett ökande antal förlorade patronlägeslås bryts. Detta kan ske genom att MD-staber och MD-grupper påtalar hur patronlägeslåsen är avsedda att nyttjas samt kontrollerar att gällande bestämmelser efterlevs.

### Kontroller avseende vapen- och ammunitionshantering

Mot bakgrund av erfarenheter från 2004 och mot vad som bedöms ske under 2005 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 respektive MD-stab, som territoriellt säkerhetsansvariga, genomför kontroller av att gällande bestämmelser avseende förvaring, hantering och transport av skjutvapen och ammunition följs

### Larm 2000

Driftsättningen av larmsystem 2000 skedde under 2003. Vissa problem avseende den personella bemanningen föreligger fortfarande vid en av larmcentralerna.

Antalen fellarm från objekt med larmsystem 2000 har minskat i förhållande till antal fellarm under 2003.

**Sammanställning av förkomna vapen 1998-2004**

| År/Typ | 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 |

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

### Övriga larm

Försvarsmakten har, i form av ett ”gammalt arv”, många varierande typer av larm vid förråd och andra anläggningar. Dessa larm börjar nu, i viss omfattning, generera 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 framtida 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. åt bl a Försvarsmakten är Setec TAG, AB. Alla Försvarsmaktsanställda skall tilldelas tjänstekort.

Dessa tjänstekort kommer att innehålla magnetremsa, datachip samt s k Mifareslinga, detta i syfte att i högre utsträckning än tidigare kunna nyttja tjänstekorten i automatiska passer-system.

Härutöver kommer företaget att tillverka 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. kommer Försvarsmaktens interna bestämmelser (FIB 2001:4) om legitimationshandlingar m.m. att skrivas om under våren 2005 och bedöms kunna träda i kraft vid halvårsskiftet.

### Skyddade transporter

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

Dessa riktlinjer kommer i stor utsträckning att överföras till författningstext i kommande utgåva av Försvarsmaktens interna bestämmelser om säkerhetsskydd (FIB 2005:00).

### Nyttjande av försvarsmaktsanställda civila skyddsvakter

Med anledning av Försvarsmakten omstrukturering och därpå följande avveckling av militära förband inom ett antal geografiska orter och områden såsom Östersund, Vaxholm, Strängnäs, Gotland etc kommer det att föreligga 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 tillgodoses genom nyttjande av vissa officerare och genom att huvuddelen av personalen i rubricerade styrkor anställs såsom försvarsmaktsanställda civila skyddsvakter. Detta kommer att regleras genom tillägg i VU 2005.

För att underlätta nyttjandet av försvarsmaktsanställda civila skyddsvakter, bl a avseende förordnande av skyddsvakterna samt avseende 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 vakttjänst inom Försvarsmakten.

Dessa förändringar är f n under behandling i Regeringskansliet och bedöms kunna träda i kraft vid halvårsskiftet 2005.

### 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 kontraktera 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 sedan tidigare givit FMLOG i uppdrag att upphandla bevaknings- och transportskyddstjänster av civila bevakningsbolag.

Upphandlingen har försenats och bedöms bli klar under maj 2005.

## Skyddsvärd verksamhet

Med skyddsvärd verksamhet avses verksamhet som:

- bedrivs av Försvarsmakten, eller på uppdrag av Försvarsmakten i eller utom riket av sådan art att den kan komma att bli föremål för säkerhetshotande verksamhet och med anledning härav eller på grund av andra skäl måste uppmärksammas
- bedrivs av främmande makt inom riket efter vederbörligt tillstånd, men där denna verksamhet kan utnyttjas för att bedriva säkerhetshotande verksamhet.

Under året har det skett fortsatt arbete med att sammanställa den skyddsvärda verksamhet som bedrivs inom Försvarsmakten. Syftet är att tidigt identifiera verksamhet som kräver utökat säkerhetsskydd samt att försvåra underrättelseinhämtning mot verksamhet och projekt som har ett högt sekretessvärde. Såväl centrala som regionala staber har utvecklat gemensamma rutiner för hur den skyddsvärda verksamheten ska vägas mot aktuell hotbild och vilka förebyggande säkerhetsskyddsåtgärder som behöver vidtas.

# Signalskyddstjänst

## Inledning

Föreliggande årsrapport avseende signalskydd 2004 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 2003 som genomfördes den 3 och 4 december 2003 fram till centrala mötet den 1 och 2 december 2004 i Visby.

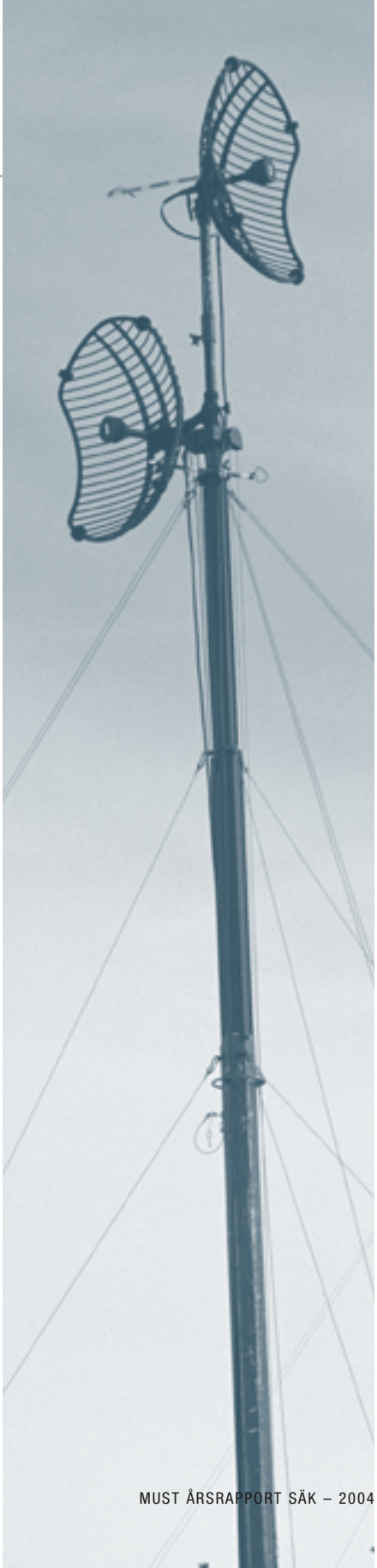
Årsrapportens syfte är att orientera signalskyddschefer och övriga företrädare för signalskyddstjänsten om de viktigaste händelserna under året. Årsrapporten riktar sig även till övrig signalskyddspersonal inom totalförsvaret.

## Sammanfattning signalskydd

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

Såsom verkställande organ för Försvarsmaktens ledning och samordning av signalskyddstjänsten har 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, aktiva kort och certifikat.

Året har präglats av ökat antal åtaganden inom det internationella området, framförallt inom EU-samarbetet. Kunskaper har inhämtats för att möjliggöra interoperabilitet



för våra förband inför kommande internationella uppdrag.

Signalskyddssystem finns idag förutom i Försvarsmakten, inom regeringskansliet och vid ca 50 statliga myndigheter och verk samt vid ca 40 företag, företrädesvis inom försvarsindustrin. Många av de statliga myndigheterna har även signalskyddsverksamhet vid respektive ”regionala och lokala” enheter.

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 2003 med det centrala signalskyddsmötet i Sundsvall som under 1:a kvartalet 2004 följdes upp med fyra 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 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 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 i syfte att planera framtida utveckling. Vid dialogerna har representant från FMV och i några fall KBM och KRI LED deltagit.

Det centrala signalskyddsmötet 2004 genomfördes i Visby. Till mötet var signalskyddschefer och företrädare för signalskyddstjänsten vid centrala myndigheter och organisationsenheter samt Försvarsmaktens centrala och regionala ledningsorgan inbjudna.

## Ledning

En översyn av Försvarsmaktens funktionsledning av signalskyddstjänsten har genomförts. Totalförsvarets signalskyddssamordning (TSA) kommer fr o m 2005-02-01 att ingå som en funktion i Militära underrättelse- och säkerhetstjänstens Säkerhetskontor (MUST SÄKK).

### Regelverk

Översyn av Försvarsmaktens (FM) föreskrifter om signalskyddstjänsten inom totalförsvaret har under året genomförts. Vissa mindre justeringar återstår innan föreskrifterna kan fastställas. Fastställandet planeras att genomföras under 1:a kvartalet 2005. Arbetet med översyn av Försvarsmakten interna bestämmelser har på på grund av Försvarsmaktens pågående omstrukturering legat nere. Arbetet kommer att återupptas så snart Försvarsmaktens framtida ledning och organisation är fastställd.

Följande instruktioner har fastställts och givits ut under 2004:

- I TST MGK 2003
- I TST MGMI 2004 (Eng version)
- I TST MGWI 2004 (Eng version)
- I TST MGV 2004

Instruktion för hantering av aktiva kort, certifikat och kortterminaler I TST AKT har under året fastställts och kommer att ges ut under första kvartalet 2005.

Revidering av Handbok Totalförsvarets Signalskyddstjänst (H TST Grunder 2001) har under året påbörjats. Ny utgåva beräknas fastställas och ges ut under tredje kvartalet 2005.

### Pågående utvecklingsprojekt

Under året har sju kryptosystem verifierats och godkänts varav två efter modifiering. Ett av dessa system är det första utvecklat för signalskyddsgrad Restricted som även skall kunna användas för att skydda information klassad EU-restricted.

Utveckling av Mobilt Taktiskt Talkrypto MTT för användning tillsammans med truppradion har påbörjats. Utan det miljöskydd som erfordras för truppradiomiljö skall MTT även kunna användas som ett Talkrypto för restricted med en förenklad nyckelhantering.

I ett samarbete med NL NCSA har NL beställt utveckling av ett mobilt krypto avsett för SG Secret och Försvarsmakten har beställt utveckling av en kryptomodul för mobilt krypto som också planeras godkännas för SG S.

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. Kryptomodulen skall ha en gemensam arkitektur som kan anpassas för en svensk och en NL-variant.

Utveckling av nästa generation av kryptomoduler har påbörjats. Målet är en snabb kryptomodul som skall klara mer än 2.5 Gbit/s och kunna användas i FTN och vid kommunikation mellan servrar.

Fortsatt arbete har bedrivits under året med aktiva kort och nya kortterminaler som skall driftsättas första halvåret 2005.

Under året har arbete bedrivits med att få fram det KryptoAPI som skall möjliggöra anrop till alla kryptokomponenter i form av både hård och mjukvara. Detta har presenterats vid två tillfällen på KP inforum där

alla totalförsvarsmyndigheter som utvecklar IT-system med kryptografiska funktioner har kunnat deltaga.

Fortsatt utveckling har skett av krypto-modem och VPN-krypto.

Ett nytt system för beställning av mjuka certifikat ”Cert-Order” har driftsatts.

TSA har påbörjat en ”second evaluation” av ett engelskt krypto. Denna process är ett krav för att få använda ett krypto som EU-godkänd produkt.

TSA har deltagit i fem internationella konferenser om krypto och deltagit i flera kryptosamarbeten inom G5 samt gjort studiebesök vid NSM i Norge för att få underlag till elektronisk nyckelförsörjning.

### Kryptonycklar

Produktion och distribution av kryptonycklar och Totalförsvarets aktiva kort (TAK) har genomförts enligt plan.

Två nya CA-system har driftsats. Ett system kommer 2005 att ersätta det nuvarande systemet för utgivning av TAK, det andra systemet är avsett för produktion av TEID (Totalförsvarets Elektroniska ID-kort)

Utredning av totalförsvarets framtida försörjning av kryptonycklar, med hänsyn till organisation och framtida tekniska möjligheter, har fortsatt under året. Resultatet skall ligga till grund för framtagning av ett nytt elektroniskt nyckelförsörjningssystem (eNFÖ).

### Nyckelincidenter

Antalet incidenter är konstant i förhållande till tidigare år. Nivån är godtagbar med hänsyn till det stora antal nycklar som dagligen hanteras inom totalförsvaret.

### Administrativa kontroller

Uppföljning och kontroll av signalskyddstjänsten har under året genomförts vid 15 centrala myndigheter, ett förband, fyra försvarsavdelningar samt i samband med detta givit respektive ambassad stöd inom sakområdet. Vidare har utlandsstyrkan kontrollerats två gånger. Generellt kan sägas att resultatet, med några undantag, varit gott.

### Signalkontroll

Avancerad ny materiel har under året installerats och personalen har därmed erhållit utbildning i Tyskland, England och USA.

Signalkontroll har genomförts vid utlandsstyrkan samt vid större övningar och prov- och försöksverksamhet inom landet. Kontrollmätningar av eventuell förekomst av röjande signaler, RÖS, vid myndigheter och förband har också genomförts.

# Bilaga 1
# Det nya Säkerhetskontoret

Med anledning av Försvarsmaktens omstrukturering, behovet av ett mera processinriktat arbetssätt och upplevda brister i den militära säkerhetstjänstens måluppfyllnad har C MUST beslutat att förändra MUST organisation. Från och med 2005-02-01 består MUST av ett Säkerhetskontor, ett Underrättelsekontor, en Administrativ avdelning och en Ledningsavdelning.

Säkerhetskontorets organisation innefattar den verksamhet som tidigare genomförts på Säkerhets- och IT-säkerhetsavdelningarna.

Världen har förändrats och det ställer krav på att Säkerhetskontoret anpassas utefter dessa förändringar. Ökade internationella insatser och internationalisering ställer andra krav på förmågan att klarlägga säkerhetshotande verksamhet och högre krav på säkerhetslägesuppfattning. Den ökande användningen av informationsteknik innebär att säkerhetsskyddet måste hanteras med informationssäkerhet och signalskydd i samverkan inom systemen. Detta i sin tur ställer högre krav på utveckling av skyddsmekanismer inom IT-säkerhets- och kryptoområdet. Behovet av att arbeta förebyggande inom säkerhetstjänsten är tydlig, då stor kraft måste läggas på att rätta till misstag som begåtts på grund av att befattningshavare inte är tillräckligt utbildade eller informerade. Informations- och utbildningsinsatser skall genomföras för att i förebyggande syfte minimera misstag och i värsta fall brott mot gällande regelverk.

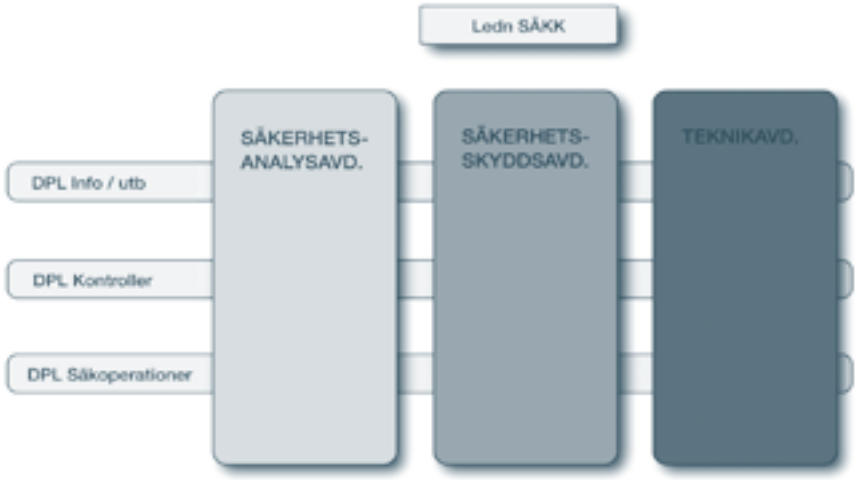
## Organisation

### Syfte

Syftet med Säkerhetskontorets nya organisation är dels att bättre kunna lösa dagens uppgifter, bl a genom utökat samarbete och tydligare ansvar dels bli bättre inom följande områden:

- Upprätthålla en klar bedömning av säkerhetsläget

### Säkerhetskontorets organisation



- Klarlägga den säkerhetshotande verksamheten
- Att utveckla system, teknik och metoder inom säkerhetsområdet
- Planering och genomförande av kontroller
- Utbildning och information

### Organisation

Säkerhetskontorets organisation utgörs av ledning, säkerhetsanalysavdelning, säkerhetsskyddsavdelning och teknikavdelning, samt delprocessledare vilka är ansvariga för information/utbildning, kontroller och säkoperationer (se organisationsbild). Avdelningscheferna är också delprocessledare för respektive avdelningsprocess. De sex delprocessledarna har alla resultatansvar och avdelningscheferna har dessutom personalansvar.

### Intressenter/kunder

Säkerhetskontoret har många intressenter/kunder inom totalförsvaret, vilket har påverkat utformningen av organisationen. Prioriterade intressenter/kunder är sådana som Säkerhetskontoret levererar underlag till. Övriga intressenter är medel för att kunna leverera underlag till prioriterade intressenter/kunder.

Det nya Säkerhetskontoret skall arbeta processinriktat med intressenternas och kundernas behov i fokus. Tidigare uppbyggda och väl fungerande nätverk skall bibehållas och utvecklas. Det nya Säkerhetskontoret skall leda och samordna den militära säkerhetstjänsten och signalskyddstjänsten där strävan är att ansvar och rollspel skall vara tydligt.