Årsrapport Säkerhetstjänst 2007

HÖGKVARTERET

Militära underrättelse- och säkerhetstjänsten MUST

Årsrapport säkerhetstjänst 2007

Militära underrättelse- och säkerhetstjänsten, MUST

FÖRSVARSMAKTEN

Denna årsredovisning publiceras även på Försvarsmaktens hemsida
på internet www.mil.se.

Omslaget är tryckt på 250 gr Multiart Gloss och inlagan på 115 gr Multiart Silk.

Grafisk form: FMLOG TryckE, Grafiska ateljén, Stockholm.
Tryckeri: Åtta.45 Tryckeri AB.

Återigen ger säkerhetskontoret vid den militära underrättelse- och säkerhetstjänsten (MUST) ut en årsrapport. Vår ambition är att ge dig som läsare en översiktlig bild av den militära säkerhetstjänstens verksamhet under det gångna året. Genom att orientera om de säkerhetshot som finns i vår omvärld hoppas vi också att rapporten ska bidra till ett ökat säkerhetsmedvetande.

De säkerhetshot som riktas mot Försvarsmaktens verksamheter och intressen är mångfacetterade. Traditionella hot som främmande underrättelseverksamhet ligger fortsatt kvar på en förvånansvärt hög nivå och har det gångna året tom ökat något i Försvarsmaktens internationella insatser. Den allt snabbare teknikutvecklingen medför nya typer av hot och ställer krav på en modern säkerhetstjänst som förmår att utveckla kompetenser och metoder för att möta en omvärld i förändring.

Internationella insatser utgör en allt större del av Försvarsmaktens verksamhet. Dessa skiljer sig från den nationella verksamheten såväl när det gäller förutsättningar som behov av säkerhetsskydd. Förmågan att rätt bedöma säkerhetshot för att därigenom kunna vidta rätt skyddsåtgärder är en utmaning för säkerhetstjänsten.

En god förmåga att bemöta yttre hot spelar marginell roll om problemen, så att säga, finns på insidan. Säkerhetsprövningen av Försvarsmaktens anställda har utvecklats med syfte att säkerställa att all personal uppfyller kraven på pålitlighet och lojalitet.

Många allvarliga incidenter är onödiga och har sin grund i bristande kunskap och/eller slarv. Ett gott ledarskap och riktade utbildnings- och informationsinsatser är den bästa metoden för att skapa ett brett säkerhetsmedvetande och arbetssätt där den skyddsvärda verksamheten ges ett tillräckligt skydd. De kommande åren skall vi tillsammans arbeta för en smartare och vassare säkerhetstjänst.

Stockholm i mars 2008

John Daniels
Chef Säkerhetskontoret

Militära underrättelse- och säkerhetstjänsten MUST

Fotografer

Omslagsbild	Andreas Karlsson, FBB
Sid 7	Andreas Karrlsson, FBB
Sida 13	Michael Moriatis, U.S. Navy
Sida 14	Andreas Karlsson, FBB
Sida 16	Jimmie Adamsson, FBB
Sida 17	Andreas Karlsson, FBB
Sida 18	FS13/FBB
Sida 20	Lasse Sjögren, FBB
Sida 22	Lasse Sjögren, FBB
Sida 23	Andreas Karlsson, FBB
Sida 25	Combat Camera, FBB
Sida 29	Jörgen Welter, FBB
Sida 32	Kristofer Sandberg, FBB
Sida 34	Ronnie Hammar, FBB
Sida 35	FBB
Sida 37	Combat Camera, FBB
Sida 43	Steffanie Müller, FBB
Sida 47	Johan Lundahl, Combat Camera, FBB
Sida 49	Combat Camera, FBB
Sida 52	FBB
Sida 53	Andreas Karlsson, FBB

Innehållsförteckning

Årsrapport säkerhetstjänst 2007

Säkerhet handlar om att ha kontroll

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

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

När man förlorat kontrollen

En viktig dimension av kontroll är strävan efter få att veta när man förlorar kontrollen dvs att få en indikation på att kontrollen runt objektet är kompromett-erad. Detta är naturligtvis i många fall svårt, speciellt avseende personers pålitlighet och lojalitet men också vad gäller sekretess- och informationsförluster. Då uppstår oftast inga spår förrän det är för sent. Ambitionen måste dock alltid vara att så långt det är möjligt skapa arbetssätt, metoder och system som kan ge indikationer på att kontrollen är på väg att förloras. Exempel på detta kan vara larmsystem, logganalyser, löpande uppföljning av personalen, inventering av information, kontroller av säkerhetsskyddet osv.

Att återfå kontrollen

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

Organisation och ledning av den militära säkerhetstjänsten

Den militära säkerhetstjänstens uppgift är att tillvarata de säkerhetsintressen som berör Försvarsmakten och dess tillsynsområde enligt säkerhetsskyddslagstiftningen. Den militära säkerhetstjänsten har tillsynsansvar över följande myndigheter; Försvarets radioanstalt, FRA, Försvarets materielverk, FMV, Fortifikationsverket, FortV, Totalförsvarets forskningsinstitut, FOI, Totalförsvarets Pliktverk, TPV, Försvarshögskolan, FHS och Försvarets underrättelsenämnd, FUN.

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

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

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

Operativ chef i Högkvarteret, OPS J2, leder säkerhetstjänsten i utlandsstyrkan samt den territoriella säkerhetstjänsten i Försvarsmakten med stöd av s.k. säkerhets- och samverkanssektioner, Säksam, i Malmö, Göteborg, Stockholm och Boden.

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

områden med Försvarsmaktens säkerhetsorganisation.

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

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

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

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

Den militära säkerhetstjänsten är organiserad i 7 delprocesser:

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

Omvärlden är i ständigt förändring och säkerhetstjänsten försöker ligga i framkant när det gäller att utveckla den egna verksamheten. Kompetenser och metoder inom den militära säkerhetstjänsten är och skall vara på en kvalitativt hög nivå. Våra motståndare är av världsklass och det sätter nivån på kraven på oss.

Ökade internationella insatser och globaliseringen ställer högre krav på säkerhetslägesuppfattning och förmågan att klarlägga säkerhetshotande verksamhet. Den alltmer omfattande användningen av informationsteknik ställer nya krav på utveckling av skyddsmekanismer inom IT-säkerhets- och kryptoområdet.

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

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

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

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

Syfte med Årsrapport Säkerhetstjänst

Årsrapporten gör inte anspråk på att vara en heltäckande beskrivning av den verksamhet som den militära säkerhetstjänsten bedrivit under året. Genom att beskriva hotbilden och ett urval av inträffade incidenter och vidtagna säkerhetsskyddsåtgärder bör rapporten ändå kunna ge en god överblick.

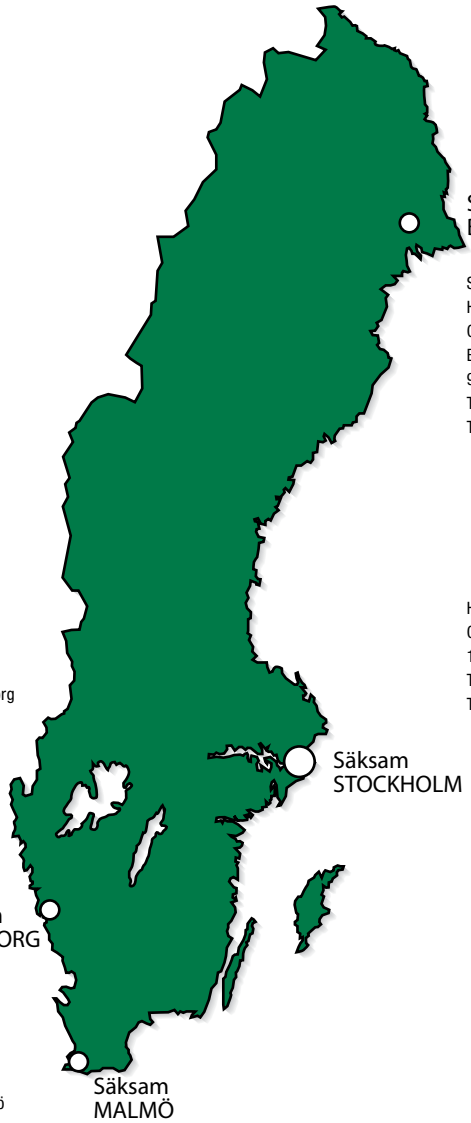
Årsrapporten är ett öppet dokument. Detta begränsar givetvis vad som kan sägas. Ambitionen har varit att vara så öppen med information som det är möjligt med hänsyn till sekretesslagen m.m. De uppgifter som inte kan anges i denna rapport återfinns i en hemlig årsrapport. ■

Här finns den militära säkerhets-tjänsten

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
OPS J2
107 85 Stockholm
Telefon: 08-788 75 00
Telefax: 08-788 72 31



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

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

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

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

Säkerhetshotande verksamhet

Den militära säkerhetsunderrättelsetjänsten syftar till att klarlägga säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess intressen inom och utom landet. Med säkerhetshot avses främmande underrättelseverksamhet, kriminalitet, terrorism, sabotage och subversion. Säkerhetsunderrättelsetjänsten ska främst producera underlag för beslut om säkerhetsskyddsåtgärder men även underlag för fortsatt säkerhetsunderrättelseinhämtning. För att genomföra denna verksamhet nationellt krävs en god kännedom om regionala och lokala förhållanden och i den internationella verksamheten ett väl fungerande samarbete med andra organisationer. Nationellt har säkerhetskontoret och OPS J2 under 2007 fortsatt att utveckla samverkansformer inom ramen för säkerhetsunderrätteletjänsten för att följa upp säkerhetsläget, verksamheter och säkerhetshot som sträcker sig över flera delar av Sverige.

Den skyddsvärda verksamheten har varit något mer omfattande 2007 jämfört med 2005 och 2006. Med skyddsvärd verksamhet avses verksamhet som pga sekretess eller av andra skäl behöver ett säkerhetsskydd. Den verksamhet som kan lyftas fram under 2007 är samträ-

ning och slutövning för Nordic Battle Group , NBG, samt övningarna Cold Response, Combined Challenge, Open Spirit, Baltops och Noble Mariner. Flera av verksamheterna har varit multinationella vilket ställer högre krav på säkerhetshotsbedömningar än nationell verksamhet. Ett exempel är övning Noble Mariner som genomfördes under försommaren 2007 och som bla innehöll ett örlogsbesök i Göteborg med fartyg från flera nationer. Särskilda utmaningar finns kopplade till denna typ av verksamhet, främst avseende överförda hot från terrorism. Konsekvensen av bristande säkerhetsrutiner och ansvar kan innebära att Försvarsmakten avslöjar unika prestanda och utsätter personal och materiel för hot från främmande underrättelseverksamhet, kriminalitet och värsta fall även hot från terrorgrupper eller andra extremistiska grupperingar.

Försvarsmakten har under 2007 fortsatt sitt engagemang i Kosovo, ökat truppbidraget och fått ett utökat ansvar i Afghanistan samt genomfört en insats med ett sjöoperativt förband i medelhavet inom ramen för en FN-operation. Den främre bas som upprättats i Abu-Dhabi med transportflygdivisionen för trupp- och materieltransporter till och från Afghanistan har under 2007 fortsatt verka. Marinen har haft en ubåt baserad i San Diego, USA. De två sistnämnda är en särskild utmaning för säkerhetstjänsten eftersom de är en utskjuten del av ett militärt förband grupperat utanför Sverige under lång tid. Försvarsmaktens personal finns därutöver grupperad på många platser runt om i världen, i enskilda missioner eller stabsbefattningar, men där har Försvarsmakten ett begränsat säkerhetsskyddsansvar.

Vid de internationella insatserna ställs ökade krav på identifiering av angripare och aktörer. Därför är det viktigt att den militära säkerhetsunderrättelsetjänsten, samordnat med den militära underrättelsetjänsten, kan inhämta, bearbeta, analysera och delge underlag inför pågående- och potentiella insatser. I dessa sammanhang bör det påpekas att en svensk insats kan komma att utgöra ett säkerhetshot mot de parter som förekommer i insatsområdet, vilket ställer krav på förmågan när det gäller kontraverksamhet.

Omfattande prov- och försöksverksamhet har genomförts under 2007, främst vid provplatsen i Vidsel. Den ökade internationella efterfrågan som kunde konstateras år 2006 har på intet sätt minskat. Tvärtom är det nu fler aktörer som vill utnyttja de utmärkta förhållanden som finns för flyg, UAV och robotprov. En ökning av internationellt samarbete och insatser tillsammans med andra nationer ställer andra krav än tidigare på verksamhetsägaren och dennes skyldighet att identifiera vad som är skyddsvärt i respektive verksamhet.

År 2006 uppdagades brister i rapporteringen av skyddsvärd verksamhet vilket resulterade i en allvarlig säkerhetsincident där främmande makt hade möjlighet att inhämta underrättelser. Detsamma har dessvärre inträffat även under 2007. Verksamhetsägare har brustit i identifiering och delgivning av planerad skyddsvärd verksamhet och uppföljning av andra nationers plattformar för underrättelseinhämtning. Detta medförde att säkerhetshotande verksamhet bedöms ha genomförts riktat mot minst en av dessa verksamheter.

Inriktning för 2008

Under 2008 kommer den militära säkerhetsunderrättelsetjänsten att prioritera stöd till Nordic Battle Group och pågående internationella insatser. I fokus står också säkerhetshot och sårbarheter inom Försvarsmaktens verksamhet nationellt och då främst inom Försvarsmaktens Logistiks, FMLOG, verksamhetsområden. Det är inom denna som den skyddsvärda materielen hanteras, materiel som är eftertraktad i kriminella kretsar. En nära samverkan mellan säkerhetstjänstens olika delar är en förutsättning för ett effektivt resursutnyttjande och för möjligheterna att kunna verka proaktivt.

Vidare kommer säkerhetsunderrättelsetjänsten fortsatt arbeta med att förbättra rapporteringsrutinerna avseende säkerhetshotande verksamhet, säkerhetsincidenter och den skyddsvärda verksamheten. Utan relevant underlag blir inte lägesbilden tillförlitlig och därigenom försvåras möjligheterna att lämna beslutsunderlag och vidta säkerhetsskyddsåtgärder.

Övergripande säkerhetshotbild

De främsta säkerhetshoten som riktas mot Försvarsmakten nationellt är alltjämt främmande underrättelseinhämtning och kriminalitet. Även terrorism måste medräknas mot bakgrund av de konsekvenser som ett angrepp sannolikt skulle få. Vidare kan Försvarsmaktens internationella insatser medföra ett överfört hot mot Försvarsmakten i Sverige. Vid

de internationella insatserna varierar säkerhetshoten med förutsättningarna för det specifika insatsområdet. Hotbilden var t.ex. inte densamma för korvetten Gävle i medelhavet som den är för den svenska insatsen i Afghanistan. Utgångsläget och situationerna är ofta komplexa med olika konfliktparter, koalitionspartners, värdlandets förutsättningar och dess förhållande till annan stat m.m.

Nedan följer en övergripande beskrivning av respektive säkerhetshot och vad som inträffat nationellt och internationellt inom ramen för Försvarsmaktens verksamhet. En utförligare beskrivning av den säkerhetshotande verksamheten redovisas i den hemliga årsredovisningen.

Främmande underrättelsetjänst

Hotet från främmande underrättelseverksamhet riktad mot Försvarsmakten i Sverige är oförändrat, däremot har hotet ökat mot Försvarsmaktens internationella insatser. Under året har det inkommit rapporter som bekräftar att det finns ett stort intresse från främmande makt för Försvarsmaktens kvalificerade vapensystem, främst sjö- och luftstridskrafter. Till viss del har intresset även riktats mot NBG och den svenska förmågan att ansvara för en Battle Group inom EU:s ram. Däremot har intresset minskat för vissa utvecklingsprojekt som t.ex. Nätverksbaserat Försvar (NBF). Orsaken till detta är för tidigt att uttala sig om eftersom den uppfattade minskningen möjligen kan förklaras av ett ökat fokus på NBG och hur Försvarsmakten omsätter NBF i praktiken. Minskningen kan också ha sin grund i bristande säkerhetsrapportering.

Under 2007 har det förekommit underrättelseinhämtning från främmande makt mot vissa förband. Officerare och anställda har närmats på ett för dem

oskyldigt sätt men där beteendet tyder på en avsikt att eftersöka information som är skyddsvärd ur ett svenskt perspektiv. Försvarsmakten har unika kompetenser, både vad gäller förband och personal, som av naturliga skäl tilldrar sig intresse. Signalspaning från flygande och sjögående plattformar har riktats mot Försvarsmaktens skyddsvärda verksamhet från flera nationer.

När det gäller främmande underrättelseverksamhet riktat mot svenska förband i Försvarsmaktens insatsområden ökade rapporteringen av incidenter under 2006 och trenden har hållit i sig även under 2007. En förklaring kan vara att Sveriges truppbidrag har enheter som verkar inom underrättelsefunktionen och därmed tilldrar sig ett intresse från både samarbetspartners och aktörer i insatsområdet. I Kosovo har ett flertal fall av misstänkt övervakning rapporterats där svensk personal blivit förföljda under patrullering. I Afghanistan har lokalanställd personal i ett flertal fall bedrivit underrättelseinhämtning åt tredje part i insatsområdet. Det är ingen nyhet för den militära säkerhetstjänsten att detta sker men det kan i många fall vara svårt att upptäcka.

Det finns ett generellt problem med lokalanställd personal. Försvarsmakten är i många fall beroende av denna typ av personal samtidigt som de utgör en sårbarhet i kontingentens verksamhet genom att de får kunskap, både direkt och indirekt, om när t.ex. verksamhet planeras. Personal i utlandsstyrkan byts normalt var sjätte månad men lokalanställda blir kvar vilket innebär att de vet mer om normalbilden inne på baser, sk camper, än den svenska kontingenten. I både Kosovo och Afghanistan har detta uppdagats och åtgärder vidtagits genom att personerna i fråga har avskedats eller omplacerats.

Ytterligare underrättelseinhämtning har genomförts mot den svenska kontingenten i Afghanistan. Ett problem tycks vara aningslöshet bland svenska soldater och officerare, särskilt i missioner som är etablerade. Säkerhetshoten verkar inte tas riktigt på allvar och ytterligare utbildningsinsatser måste genomföras under 2008 både inför och under en mission.

Terrorism

Under det gångna året utsattes inte Försvarsmakten för några terroristrelaterade incidenter nationellt. Tidigare gjorda bedömningar avseende säkerhetshotet från terrorism riktat mot Försvarsmaktens verksamhet och intressen har därmed visats sig stämma med utfallet under året.

Hotbilden är högre i Försvarsmaktens insatsområden än den är nationellt. I Afghanistan har en markant ökning av antalet terrorattacker riktade mot den internationella närvaron konstaterats under 2007. Det gäller även i den norra regionen där det svenska truppbidraget Provinsional Reconstruction Team, PRT, är grupperat i Mazar-e-Sharif, MeS. Angreppen riktades både mot den internationella militära insatsen International Security Assistance Force, ISAF, den civila närvaron och lokala afghanska myndigheter. Under 2007 har det förekommit attentat med improviserade sprängladdningar s.k. Improvised Explosive Devices, IED, riktade mot svenska soldater på patrull i provinsområdena och inne i MeS. Attackerna i PRT MeS genomfördes i huvudsak av regeringsfientliga grupper eller genom bulvaner i form av krimi-

nella grupperingar som betalats för att utföra dessa. Inga hot har dock riktats mot Sverige som nation eller svenska intressen, men då svenska förband ingår som en del i den internationella närvaron har den svenska kontingenten en liknande hotbild som övriga i ISAF ingående länder. Detta har föranlett att skyddsåtgärder för den svenska kontingenten i ISAF har vidtagits under året.

I övriga insatsområden har inga incidenter inträffat under det gångna året. Dock verkar svenska förband i områden där hotbilden mycket snabbt kan förändras. En förändring kan orsakas både av egen genomförd verksamhet men också genom överförd hotbild från samarbetsländer som verkar inom samma område. En förändrad hotbild kan eventuellt ge överspridningseffekter från ett insatsområde till Sverige eller annat geografiskt område där svenska intressen finns. Även nationella politiska och militärstrategiska ställningstaganden påverkar säkerhets-hoten mot Försvarsmakten, såväl nationellt som internationellt. Ett exempel som belyser detta är publiceringen av en bild i Nerikes Allehanda föreställande profeten Muhammed som rondellhund. Detta fick den svenska regeringen att mycket snabbt agera utifrån erfarenheter av hur Danmark och Tyskland hanterade sina kriser 2005 och 2006. Lyckligtvis föranledde inte detta några våldsyttringar annat än mindre demonstrationer vid svenska beskickningar etc.

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

Kriminalitet

Säkerhetshotet från kriminalitet riktad mot Försvarsmakten, såväl i Sverige som i de internationella insatser där Försvarsmakten deltar, ligger kvar på oförändrad nivå. Antalet inrapporterade säkerhetshändelser under 2007 har uppgått till 1.316 st. De klassificeringar av incidenter som gjorts visar att inbrott och inbrottsförsök tillsammans med informations- och materielförluster toppar statistiken om man bortser från larmbortfall som beror på handhavandefel.

Hot mot personer i Försvarsmakten och otillbörlig påverkan på beslutsfattare inom Försvarsmaktens högsta ledning har uppdagats under året. Händelserna är mycket komplexa och kräver nära samverkan mellan organisationsenheter inom Försvarsmakten, polis samt säkerhetsföretag. Det främsta hotet mot Försvarsmakten i Sverige utgörs dock av tillgreppsbrott. De säkerhetsrapporter som är av störst intresse att bearbeta är tillgrepp och försök till tillgrepp av vapen och ammunition samt avancerad skyddsutrustning såsom kroppsskydd, skyddsmasker och hjälmar. Under 2007 har ett antal vapen rapporterats saknade och skyddsutrustning försvunnit eller kan inte återfinnas i Försvarsmaktens redovisningssystem.

Försvarsmakten drabbades under 2007 av metallstölder på en nivå som motsvarar 2006. Tillgreppen har skett mot koppar som finns på en mängd platser i Försvarsmakten, främst kring skyddsobjekt. I huvudsak rör det sig om extern brottslighet som riktar sig mot flera samhällssektorer. Det finns tecken som tyder på att

verksamheten är organiserad i någon form men ingen aktör har kunnat identifieras.

Även drivmedelstölderna har fortsatt under 2007. Denna verksamhet har fortgått under flera år, främst i norra Sverige. Dock har tillvägagångssätten förändrats efter det att skyddsåtgärder vidtagits och nu är det fordon i olika typer av förråd och uppställningsplatser som främst är utsatta. Några av dessa stölder har kunnat klaras upp. Det finns tecken som tyder på att det rör sig om både extern och intern kriminalitet. Under 2008 kommer särskilda åtgärder vidtas mot detta.

Antalet larmincidenter ökade kraftigt under 2006 vilket bedömdes främst bero på en ökad rapporteringsbenägenhet vid några förband. Ökningen har dock fortsatt under 2007. Ett stort antal av incidenterna kan konstateras vara orsakade av handhavandefel från personal som har haft att hantera larmanläggningarna. Detta är otillfredsställande då det kan leda till bristande förtroende för vidtagna säkerhetsskyddsåtgärder, en minskad benägenhet att göra insats och ett minskat säkerhetsmedvetande vid insats.

Under 2006 ökade rapporteringen om illegal försäljning av försvarsmaktsmateriel. Bloggar och andra forum på internet var då en förhållandevis ny arena för möjlig brottslig verksamhet riktad mot Försvarsmakten och trenden har fortsatt under 2007. Det har bl.a. förekommit att sekretessbelagd information om anläggningar publicerats på olika websidor och internetforum samt att privatpersoner sålt Försvarsmaktsmateriel på auktions- och försäljningssidor på internet. Det pågår ett arbete för att minska detta problem under 2008.

I Försvarsmaktens insatsområden har det under 2007 inte uppdagats några större fall av kriminalitet där den militära säkerhetstjänsten behövt vidta åtgärder. Under 2006 var fallet det omvända. Det bör dock påpekas att kriminella grupper är högst påtagliga aktörer både på Balkan och i Afghanistan. Nationsgränser är betydelselösa för den organiserade kriminaliteten och det är stora värden som hotas när ISAF respektive KFOR försöker påverka ”trafficking” m.m. inom ramen för sina operationer. I Afghanistan har hotbilden ökat lokalt efter det att svensk personal understött afghansk polis och militär vid olika gripanden och andra åtgärder.

Subversion

Under året har inga säkerhetsrapporter inkommit som kan bedömas peka på att någon aktör bedriver subversiv verksamhet riktad mot Försvarsmaktens nationella verksamhet eller intressen. Internationellt så förekommer det informationsoperationer som skulle kunna liknas vid någon form av subversiv verksamhet inom Försvarsmaktens insatsområden. I Afghanistan har detta kunnat konstaterats vid två tillfällen. I det ena fallet har svenska försvarsmaktsanställda använts för att påverka opinionen och synen på den svenska insatsen. I det andra fallet så användes svensk personal ovetandes av en aktör i insatsområdet som ville påvisa sin goda samarbetsförmåga med ISAF, vilket denne i själva verket inte hade. Det är tydligt att svensk personal oavsett kategori måste bli mer uppmärksam på just detta hot eftersom det så påtagligt används av olika aktörer för att vinna egna fördelar eller splittra sammanhållningen inom t.ex. ISAF.

Sabotage

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

IT-säkerhetsrelaterade incidenter

FM Computer Emergency Response Team, FM CERT, är Försvarsmaktens resurs på militärstrategisk nivå vad gäller IT-säkerhet. FM CERT har två huvuduppgifter, incidenthantering och lägesbild. Incidenthantering innebär insamling och sammanställning av IT-säkerhetsrelaterade incidenter. Statistik sammanställs, analyseras och erfarenheter delges. Vid mindre allvarliga incidenter har FM CERT normalt endast en rådgivande och stödjande funktion. Vid allvarligare incidenter kan FM CERT koordinera incidenthanteringen. Den andra huvudupp-giften innebär att sammanställa och delge en lägesbild rörande säkerhetsläget i Försvarsmaktens IT-system. Denna syftar ytterst till att skapa beslutsunderlag för Försvarsmaktens insatschef och försvarsmaktsledningen. Till grund för lägesbilden ligger framförallt incidentrapportering och omvärldsbevakning. Omvärldsbevakningen tjänar också till att informera driftägare om hot, sårbarheter och nya trender.

Arbetet med att utveckla förbandet FM CERT fortsätter. Vid sidan av den operativa verksamheten har under 2007 stor vikt lagts på förbandsutveckling och rekrytering. Antalet inrapporterade incidenter ligger på en nivå motsvarande tidigare år.

Ofta rör det sig om felaktig hantering av sekretessbelagd information i IT-system eller otillåtna sammankopplingar av system. Otillåten användning av trådlösa nätverk har också förekommit.

Skadlig kod

Inga allvarliga utbrott av skadlig kod drabbade Försvarsmakten under 2007. Detta tack vare en god nätarkitektur samt en strikt policy avseende behörigheter. Trenden mot mer riktade attacker fortsätter. Hackare världen över har insett att de kan tjäna pengar på sina kunskaper. Försvarsmakten är en tänkbar måltavla, framförallt när det gäller teknisk information. En angripare kan t.ex. utnyttja det faktum att en anställd med tillgång till känsliga uppgifter om militär teknik också med stor sannolikhet besöker webbplatser, läser e-post, följer länkar etc. i aktuellt ämne. Genom att förfalska sin identitet kan en angripare förleda den anställde att besöka webbplatser eller öppna e-postbilagor som är preparerade med skadlig kod som samlar information och därefter skickar denna vidare till angriparen.

Datorer som ansluts till internet blir nu inom några minuter utsatta för angreppsförsök med syfte att ta över datorn och skapa en så kallad ”bot” eller ”zombie”. Denna kan sedan utnyttjas tillsammans med andra i koordinerade angrepp eller spridning av spam. Ett exempel på denna typ av angrepp är när Estland i slutet av april utsattes för en Denial Of Service attack (DOS-attack). Man skall därför dagligen uppdatera sitt operativsystem, antivirusprogram och viktiga applikationer.

SPAM

Spam är ett ökande problem och många i Försvarsmakten har upplevt det som en stor börda. Driftsättningen av det planerade spamfiltret har inte kunnat genomföras som planerat. Anledningen är att det saknas ett fastställt regelverk för hur förvaltning och granskning av filtrerad e-post skall genomföras. Problemet har dock kunnat minskas genom andra åtgärder. ”Spammare” finner emellertid ständigt nya tekniker för att komma runt de åtgärder som vidtas. Detta gör att vi troligtvis aldrig helt blir av med problemet. De som är varsamma med att sprida sin adress till sändlistor och webbplatser har i regel mindre problem med spam. Detta gäller även publicering av e-postadresser på www.mil.se

Signalkontroll

Sektionen för teknisk inhämtning genomför signalkontroll i Totalförsvarets telekommunikations- och informationssystem. Syftet är att klarlägga:

- riskerna för obehörig åtkomst
- störande eller manipulering av data
- att systemen används enligt gällande regler
- förekomst av röjande signaler (RÖS)

Signalkontrollens uppgift är också att delta vid olika operationer för att t.ex. klarlägga närvaro av obehörig personal vid skyddsvärd verksamhet.

Signalkontrollen inriktas mot olika verksamheter som kräver hög eller långvarig sekretess. Detta genomförs bland annat genom avlyssning i syfte att klarlägga vilken information som främmande underrättelsetjänst kan få ut genom signalspaning.

Under 2007 har signalkontroll genomförts i anslutning till:

- Prov och försök
- Militära övningar såsom Combined Challenge 07 (CC07) och NBG Finex (NR07)
- Säkerhetsoperationer inom landet
- Tekniska utredningar (RÖS) samt planering av radiolänkförbindelser

Vid signalkontroll i samband med övningar har konstaterats att deltagande personal vid ett flertal tillfällen har pratat hemlig information på oskyddade och ej krypterade telefoner. Detta beteende är allvarligt och särskilda insatser kommer därför att vidtas under 2008

Detaljerad redovisning av resultat från genomförda verksamheter sker i den hemliga årsredovisningen.

Teknisk IT-kontroll

Teknisk IT-kontroll kontrollerar Försvarsmaktens IP-nät och IT-system. Syftet är att detektera otillbörligt nyttjande. Detta görs genom att studera loggar och datatrafik, både i realtid och i efterhand. Kontroller sker dels under begränsad tid, som till exempel vid övningar, dels kontinuerligt. Mönster kartläggs för att anomalier ska kunna upptäckas.

Sårbarheter söks även genom kontrollerade intrångsförsök, så kallade penetrationstester. Till viss del utförs arbetet automatiskt av datorer, men ett stort mått manuellt arbete krävs. Detta gäller framförallt logganalys och konfigurering av de automatiska systemen. Tonvikt har under året lagts vid kontroll av de system som hanterar hemlig information.

Tekniska Utredningar

Under 2007 har ett tjugotal tekniska utredningar genomförts. Antalet utredningar är relativt konstant över tiden, däremot ökar mängden data i varje utredning kraftigt. Anledningen till detta är den ökande lagringskapaciteten på olika minnesmedia och överföringshastigheten i näten.

Under 2007 har stor vikt lagts på metodutveckling, ett arbete som kommer fortgå under 2008. Målsättningen är att säkerställa forensiska metoder som bättre överensstämmer med de civila myndigheternas. Den ökande mängden data gör att utredningarna blir allt mer tids- och resurskrävande.

Utredningsmaterial har bland annat varit hårddiskar, mobiltelefoner, andra typer av minnesmedia samt systemloggar. Syftet har varit att upptäcka sekretessförluster. Uppdragen har kommit från den centrala ledningen, lokala förband och andra myndigheter. ■

Säkerhetsskydd

Säkerhetsskyddstjänsten syftar till att hindra eller försvåra säkerhetshotande verksamhet samt förlust av skyddsvärd information. Säkerhetsskyddstjänsten arbetar bl.a. med informationssäkerhet, säkerhetsprövning, säkerhetsskyddad upphandling samt med internationella säkerhetsskyddsavtal.

Försvarsmaktens ledningssystemutveckling

Den militära säkerhetstjänsten har under 2007 gett stöd för framtagning av policy och riktlinjer för informationssäkerhet vid utveckling av Försvarsmaktens ledningssystem, vilket engagerar flera myndigheter samt industri både inom och utom landet.

Komponenter från ledningssystemutvecklingen används idag i ledningssystem inom ramen för skarpa insatser. Eventuella sårbarheter i sådana komponenter kan, om de röjs, av obehöriga användas i syfte att störa eller hindra genomförandet av en insats. Av den anledningen är det viktigt att det på en övergripande nivå finns en styrning så att Försvarsmaktens säkerhetsintressen i utvecklingen av ledningssystem omhändertas, såväl inom som utom myndigheten.

Stöd till projekt PRIO

PRIO är Försvarsmaktens projekt för att införa ett integrerat resurs- och ekonomiledningssystem. Den militära säkerhetstjänsten har under 2007 gett stöd till PRIO bland annat genom kompetens rörande klassificering av information.

I samband med utvecklingen av ett IT-system är det viktigt att identifiera vilka uppgifter i systemet som omfattas av sekretess. Detta för att kunna utforma säkerhetsskyddsåtgärder.

I de fall uppgifterna rör rikets säkerhet ska även det men uppgifterna kan ge om de röjs identifieras. Klassificeringen av den information som ska ingå i de IT-system som blir följden av projekt PRIO är komplext då ett stort antal IT-system skall ersättas.

Medförande av hemlig handling

2007 infördes nya föreskrifter om medförande av hemlig handling utanför Försvarsmaktens områden. Föreskrifterna innebär att chefen för en organisationsenhet i Försvarsmakten ska fatta beslut före medförandet av en hemlig handling som är placerad i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre. Chefen kan delegera beslutsrätten och beslutet kan vara generellt så att det inte krävs ett beslut för varje enskild hemlig handling som behöver medföras. Ett beslut om medförande krävs även vid medförande från ett militärt fartyg, luftfartyg eller fordon som befinner sig utanför Försvarsmaktens lokaler eller områden.

Syftet med de nya föreskrifterna är att det inom varje organisationsenhet i Försvarsmakten skall tydliggöras i vilka sammanhang en hemlig handling får medföras. Finns inte ett beslut om medförande får sådana hemliga handlingar inte medföras. De nya föreskrifterna innebär även att en hemlig handling som medförts snarast möjligt ska återföras eller överlämnas till en annan organisationsenhet inom Försvarsmakten.

Föreskrifterna om medförande av hemlig handling ska även tillämpas för lagrings-

HEMLIG/CONFIDENTIAL

HEMLIG/TOP SECRET

medium som är avsett för eller innehåller hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/ CONFIDENTIAL eller högre.

Gemensam användning av hemlig handling

Inom Försvarsmakten förekommer verksamheter där flera personer har behov av att gemensamt använda hemliga handlingar. Exempel på sådan verksamhet är ledningscentraler och drift- och underhållsverksamhet i Försvarsmaktens anläggningar. I dessa fall är det inte alltid möjligt att låta varje person ha ett exemplar var av varje hemlig handling eller låta personerna kvittera de hemliga handlingarna mellan sig.

En ändring 2007 av Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel gör det möjligt för en grupp personer att gemensamt använda hemliga handlingar. Personer som ingår i en sådan grupp får utan inbördes kvittenser använda de hemliga handlingarna.

Gemensam användning av hemlig handling ska tillämpas restriktivt då grundregeln fortfarande är att hemliga allmänna handlingar som är placerade i informationssäkerhetsklass HEMLIG/ CONFIDENTIAL eller högre ska kvitteras av mottagaren. Gemensam användning av hemliga handlingar gäller även för hemlig materiel samt lagringsmedium som är avsedda för eller innehåller hemliga uppgifter.

Skydd av landskapsinformation

Skydd av landskapsinformation skall uppmärksamma sekretessen för lägesbestämd information som kan orsaka skador för Sveriges förberedelser för krig om de återger förhållanden som är av betydelse för totalförsvaret och sprids. I takt med att Försvarsmakten har förändrats från ett invasionsförsvar till ett insatsförsvar har behovet av skydd för landskapsinformation minskat. Fortfarande finns det dock av människan skapade förhållanden i naturen och naturgivna förhållanden som om uppgifter om dessa röjs kan skada våra förberedelser för krig.

Under 2007 har den militära säkerhetstjänsten tillsammans med Lantmäteriverket och Säkerhetspolisen genomfört ett seminarium på konferensen GeoInfo 2007 i Gävle. Det gemensamma seminariet syftade till att ge kunskap om det fortsatta sekretessbehovet för landskapsinformation och gällande lagstiftning. Frågor om upprättande och spridning av landskapsinformation är ett aktuellt område, bland annat till följd av intresset för havsmiljöfrågor och effektivisering av offentlig förvaltning.

Försvarsmakten har 2007 föreslagit regeringen att frågor som rör tillämpning av lagen om skydd för landskapsinformation samt förordningen skall utredas. Senast detta skedde var i utredningen om tillträdesskydd med betänkandet Sekretess för landskapsinformation.

Förstöring av lagringsmedium

Den militära säkerhetstjänsten har i ett direktiv gett anvisningar för hur digitala lagringsmedier skall förstöras inom Försvarsmakten så att uppgifter som lagrats inte längre kan läsas eller återskapas. Direktivet anger detaljerade krav på metoder för förstöring av

- optiska lagringsmedier
- hårddiskar
- mjuka magnetiska lagringsmedier
- elektroniska minnen (t.ex. USB-minnen)

De metoder som används för förstöring av lagringsmedier som innehåller hemliga uppgifter måste ta hänsyn till att underrättelseaktörer kan ha utvecklat metoder för återskapande av information som vi inte känner till, den framtida tekniska utvecklingen vad avser återskapande av information samt sekretesstiden för hemliga uppgifter som i vissa fall uppgår till 150 år.

Förstöring av lagringsmedium kan ske genom mekanisk påverkan (tuggning, perforering, slipning, sandblästring, krossning och klippning), förbränning, nedsmältning eller avmagnetisering. Direktivet anger krav på förstöringsmetoder (bl.a. regler för fragmentens storlek) och nödvändiga säkerhetsåtgärder i samband med förstöring av lagringsmedier.

Miljörelaterad säkerhet

Vid kontroller under de senaste åren har den militära säkerhetstjänsten konstaterat att driftmiljön inte är godtagbar ur säkerhetssynpunkt för flera av Försvarsmaktens IT-system. Det är skyddet mot kyla, brand, vattenläckage, klimatlarm, åskskydd, tekniska försörjningssystem, kontinuerlig strömförsörjning och nedsmutsning som brister. En av konsekvenserna kan bli att information inte är tillgänglig när den behövs, information som kan vara verksamhetskritisk.

En effekt av att t.ex. klimatlarm saknas kan vara att ingen indikation av att temperaturen stiger fås vid ett eventuellt haveri av luftkonditioneringen. När temperaturen blir för hög havererar utrustning i IT-systemet och först då blir användarna och driftpersonalen uppmärksammade på incidenten.

Styrande direktiv i form av regelverk och handböcker gällande tillgänglighet kommer att tas fram av säkerhetskontoret för att ge produktägarna riktlinjer för att dessa skall kunna tillse att skyddet i och kring ett IT-system är tillfredsställande. Även mallar i Metod- och utbildningsstöd för Auktorisation och Ackrediteringsprocesserna inom Försvarsmakten (MAACK) kommer att uppdateras.

Säkerhetsprövning

Säkerhetsprövning skall göras innan en person anställs. Detta gäller även för personer som på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet eller som anlitas för sysslor som är viktiga

för skyddet mot terrorism. Prövningen skall klarlägga om personen kan antas vara lojal mot de intressen som skyddas i säkerhetsskyddslagen och i övrigt är pålitlig ur säkerhetssynpunkt.

Att en person inte bedöms vara pålitlig ur säkerhetssynpunkt behöver i och för sig inte alltid utgöra ett negativt omdöme om vederbörande. Det kan vara så att en person är särskilt sårbar i det att han eller hon på grund av dubbla lojaliteter riskerar hamna i en intressekonflikt eller genom sin livsföring eller levnadssätt kan utsättas för påtryckningar.

Under 2007 har fortsatt samordning och utveckling av Försvarsmaktens säkerhetsprövningsverksamhet genomförts. Antalet genomförda registerkontroller ligger omkring 20.000 och mer än hälften av dessa beror på förnyade kontroller av hemvärnspersonal och frivillig avtalspersonal.

Förekommer det uppgifter om en person i polisens register och uppgifterna lämnas ut till Försvarsmakten så avslås normalt en ansökan om anställning som yrkes- eller reservofficer. Detsamma gäller för befattningar i utlandsstyrkan, inom hemvärns- eller frivilligverksamhet och vid mönstring av värnpliktiga. Är individen redan ianspråktagen av Försvarsmakten görs en personutredning av säkerhetskontoret på grundval av inkomna uppgifter eller noteringar. Säkerhetsskyddsbeslut i personärende fattas enbart av MUST.

Antalet personärenden som krävt utredning med påföljande säkerhetsskyddsbeslut ligger på en oförändrad nivå vilket innebär cirka 500 fall per år. Vanliga utredningsskäl är uppgifter om rattfylleri, misshandel, snatteri, stöld och olaga vapeninnehav. Missbruk av alkohol är ofta en orsak till att personal begår brott som innebär att uppgifter lämnas ut från

Rikspolisstyrelsen (RPS). Även uppgifter från RPS rörande misstanke eller belastning om smuggling, förargelseväckande beteende, olaga hot, olovligt förfogande, häleri, brott mot knivlagen, olovlig körning, osant intygande, föregivande av allmän ställning, undandräkt, bokföringsbrott, bedrägeri, urkundsförfalskning, förskingring, hemfridsbrott, våld mot tjänsteman, brott mot besöksförbud, kvinnofridskränkning, sexuellt ofredande, våldtäkt, narkotika brott, rån, mordförsök och mord har förekommit. Uppgifter om misstanke om terroristbrott har varit väldigt få under året, likaså uppgifter om vårdslöshet eller obehörig befattning med hemlig uppgift.

Vid några tillfällen har den förnyade kontrollen av hemvärns- och frivilligpersonalen inneburit uppseendeväckande resultat. Det finns exempel på personer som dömts för brott, i några fall med fängelsestraff som påföljd, men som fortfarande är kvar i verksamheten. Säksamsektionerna har mot bakgrund av detta av fått i uppdrag att utreda vad i säkerhetsprövningen och uppföljande kontroller som brustit. Detta visar på betydelsen av att på lokal nivå genomföra en grundlig säkerhetsprövning inför anställning samt att följa upp personal kontinuerligt. Försvarsmakten har för närvarande inte rätt att begära registerkontroll av personal i de frivilligrörelser som inte har avtal med Försvarsmakten.

Lämplighetsprövning av värnpliktiga genomförs av Pliktverket vid mönstring. Försvarsmakten ansvarar för och genomför säkerhetsprövning under tjänstgöringstiden. Ett antal personärenden har under året rört värnpliktiga som av säkerhetsskyddsskäl inte bör få fortsätta sin tjänstgöring. Aktuellt förband ska noggrant utreda händelsen och om säkerhetsskäl anförs ska utredningen överlämnas till säkerhetskontoret för prövning. Säkerhetskontoret beslutar om den värnpliktige av säkerhetsskyddsskäl inte får vara kvar på sin befattning och hemställer sedan hos Pliktverket att inskrivningsbeslutet ska ändras. Överklagar den värnpliktige det ändrade inskrivningsbeslutet så kommer förbandets utredning att granskas av Statens överklagandenämnd. I syfte att förbättra säkerhetsprövningen av värnpliktiga kommer samtliga värnpliktiga att placeras i säkerhetsklass fr.o.m. 2009.

Uppföljning av anställda ska genomföras lokalt och vid behov med stöd från säkerhetskontoret. Vid t.ex. misstanke om alkoholproblem hos en individ får dennes förbandschef i uppgift av säkerhetskontoret att genomföra ett säkerhetssamtal. Utifrån vad som framkommer vid detta beslutar förbandschefen om individen skall placeras eller inte. När det gäller anställda förtjänar det att påpekas att ett säkerhetsskyddsbeslut normalt inte är grund för avsked men kan innebära en omplacering eller restriktion för individen. Exempel på restriktioner kan vara att individen:

- inte får delges hemlig uppgift
- inte får hantera Försvarsmaktens vapen eller ammunition
- inte får ianspråktas för internationell tjänst

Förbandschef ska skriftligen återrapportera till säkerhetskontoret vidtagna åtgärder och resultat av uppföljning.

För placering i den högsta säkerhetsklassen (SK 1) genomförs särskild säkerhetsprövning. Under 2007 har ett drygt sextiotal individer har genomgått särskild säkerhetsprövning för eventuell befordran och placering i Försvarsmaktens chefskrets. Denna särskilda säkerhetsprövning är tidsödande och resurskrävande. Samtliga prövade till chefskretsen har godkänts ur säkerhetssynpunkt. Personer med alkoholproblem ska inte vara placerade i de högsta säkerhetsklasserna och inte heller tas i anspråk för internationell tjänst. En särskild inriktning under 2009 är att följa upp personal för att tidigt uppmärksamma faktorer som kan utvecklas till säkerhetsproblem.

Säkerhetskontoret har i flera fall under året nekat individer att delta i internationell tjänst på grund av alkoholrelaterade problem eller kriminell belastning. En grundläggande säkerhetsprövning av personal med etnisk bakgrund från aktuellt insatsområde inför anställning i utlandsstyrkan är komplicerad. Under 2008 kommer införandet av en uttagningskommission förbättra rekrytering och säkerhetsprövning av personal till vissa befattningar i utlandsstyrkan.

Administrationen av registerkontroller och intyg om genomförd säkerhetsprövning (Personnel Security Clearance, PSC), har effektiviserats genom utveckling och införande av nya rutiner i underrättelse- och säkerhetstjänstens IT-system, IS UNDSÄK. Utveckling och driftsättning av datakommunikation med RPS under har inneburit kortare ledtider och minskade kostnader. MUST har utfärdat 2.159 stycken säkerhetsintyg av vilka cirka 200 har föregåtts av särskild utredning beroende på utlämnade uppgifter från RPS eller till följd av säkerhetskontorets restriktioner.

SUA

När det gäller säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA) har i några fall anställda vid företag nekats delta i verksamhet med Försvarsmakten på grund av resultatet av genomförd säkerhetsprövning. Omfattningen av antalet registerkontroller med kontrollorsak SUA har ökat. Även säkerhetsskyddskraven har ökat på grund av att Försvarsmakten upphandlar alltmer kvalificerade tjänster, både ur säkerhetsskydds- och kompetensperspektiv.

SUA innebär att företag, som inte omfattas av säkerhetsskyddslagstiftningen, inför en upphandling som rör verksamhet som erfordrar skydd med hänsyn till rikets säkerhet skall förbindas att följa motsvarande säkerhetsskyddsbestämmelser som gäller för den upphandlande myndigheten. Denna förbindelse tecknas i ett säkerhetsskyddsavtal. Avtalet skall reglera samtliga säkerhetsskyddsåtgärder som säkerhetsanalysen/säkerhetsplanen anger. Affärsavtalet får tecknas först då säkerhetsskyddsavtalet ingåtts.

Försvarsmakten löser alltfler uppgifter inom stödverksamhetsområdet genom upphandlade tjänster och allt oftare

krävs SUA. Exempel på detta är tillverkning av legitimationshandlingar, bevaknings- och receptionstjänster, telefonväxeltjänster, posthantering, drift och underhåll inom IT-området och stöd vid auktorisations- och ackrediteringsprocesser avseende IT. Säkerhetsskyddsansvaret åvilar den organisationsenhet som ansvarar för verksamheten som skall genomföras.

Idag är det cirka 300 företag med säte i Sverige som har ett eller flera säkerhetsskyddsavtal med Försvarsmakten. Endast ett fåtal företag har uppdrag med SUA-avtal nivå 1 vilket innebär att leverantören hanterar och förvarar hemliga uppgifter i egna lokaler. Fördelningen mellan SUA-avtal nivå 2 (leverantören hanterar och förvarar hemliga uppgifter i av Försvarsmakten anvisade och godkända lokaler) och SUA-avtal nivå 3 (leverantören kan komma att få ta del av hemliga uppgifter) är ungefär lika. Säkerhetsskyddskraven för respektive uppdrag styrs av resultatet av genomförd säkerhetsanalys. Säkerhetsprövningen av företag med säkerhetsskyddsavtal kommer att bli föremål för särskild uppföljning under 2009.

Vapen och ammunition

Eftersom det alltjämnt blir svårare att tillgripa skjutvapen och ammunition ur förråd kan det befaras att hot kan komma att riktas mot personal som arbetar vid förråd eller som har nycklar till dessa. Särskilt sårbara är förråd som finns utanför inhägnat och bevakat område. Det

Förlust av vapen

Sammanställning av förkomna vapen 1998-2007

Typ/ År	Pistol	Kpist	Gevär	Ak 4	Ak 5	Totalt
1998	0	1	2	8	18	29
1999	8	3	7	12	1	31
2000	3	4	4	11	4	26
2001	3	4	3	8	2	20
2002	0	1	0	9	0	10
2003	1	2	0	11	1	15
2004	1	1	6	6	0	14
2005	2	0	0	6	8	16
2006	10	1	3	1	0	15
2007	9	3	0	2	0	14

kan dock inte uteslutas att även områden och platser innanför bevakat och inhägnat område kan utgöra ett mål för en angripare. Detta understryker vikten av att avdela personal för bevakning och skydd vid arbete i vapen- och ammunitionsförråd samt att transporter av skjutvapen och ammunition genomförs som skyddade transporter. Regler för detta anges bla i H SÄK Vap Am som utkom i reviderad version under 2007.

Trots en nedåtgående trend avseende vapenförluster återstår en del innan nollvisionen är uppnådd. Förluster under 2007 har främst drabbat militärförråd och militärförläggningar samt vapen tillhörande hemvärnsmän. Flertalet av de förekomna vapnen är av typen enhandsvapen.

Hemvärnsmännens vapen bedöms vara försedda med patronlägeslås och bör därför vara obrukbara, dock kan förlust av vapen med patronlägeslås innebära att kriminella kan skaffa sig kunskap om hur man forcerar det skydd som patronlägeslåset utgör. Beträffande ammunitionsförluster så uppgår dessa till en ringa förlust, främst i form av övningsammunition.

Mot bakgrund av erfarenheter från tidigare år är det väsentligt att alla organisationsenheter ser över tillämpningen av gällande bestämmelser avseende vapen och ammunitionshanteringen och att omedelbara åtgärder vidtas om hotbilden förändras.

Betydelsen av en aktuell säkerhetsanalys inför varje momenten i arbete med skjutvapen, ammunition samt skyddsvärd materiel, kan inte nog understrykas. Säkerhetsanalysen skall utgöra en viktigt underlag när det gäller att anpassa rätt skyddsåtgärder i form av bevakning och insatsberedda skyddsstyrkor mot rådande hotbild.

Skyddade transporter

I syfte att minska behoven av att ta värnpliktiga i anspråk för transportskydd och bevakning vid arbeten i förråd beslöt Högkvarteret 2003 att pröva att nyttja civila bevakningsföretag. FMLOG gavs uppdraget att upphandla tjänsten. Upphandlingen avslutades hösten 2005 varvid ett avtal slöts med Falck Security AB (nuvarande G4S).

Rikspolisstyrelsen beslutade senare under året att avslå en ansökan från bevakningsföretaget G4S om att få utrusta väktare med skjutvapen. Därmed kunde inte G4S uppfylla de krav som Försvarsmakten ställde avseende bevakning av säkerhetsskyddade transporter (dock kan G4S även fortsättningsvis nyttjas för bevakning vid arbete i förråd).

Om en lösning inte kommer till stånd som medger ett nyttjande av säkerhetsföretag i samband med skyddade transporter kan en eventuell lösning vara att under tidsbegränsad period anställa personal för uppgiften. Beslut ifrågan väntas under våren 2008.

Bevakningsutredningen

I januari 2006 fick chefen för Försvarsmaktens tekniska skola, C FMTS, i uppdrag av Högkvarteret att utreda Försvarsmaktens bevakning och transportskyddstjänst. Utredningen skulle bl.a. ta fram förslag på dimensionering, utrustning och metoder samt förslag till rationaliseringar.

Under hösten 2007 har utredningens slutsatser och förslag bearbetats och resulterat i att Högkvarteret har fattat beslut om ansvarsfördelning och uppgifter för det fortsatta arbetet.

Sammanfattningvis så innebär detta att Arméinspektören ges i uppdrag att funktionsutveckla bevakningsverksamheten, operativ chef skall insatsleda bevakningstjänsten och att övriga enheter inom Högkvarteret skall ge riktlinjer och styrningar för verksamheten. Senast 2010 skall ett nytt koncept för bevakning och transportskydd vara implementerat i Försvarsmakten.

Internationella säkerhetsskyddsavtal

Sverige är beroende av att ha giltiga och uppdaterade säkerhetsskyddsavtal med flera länder och organisationer. Syftet är att svenska myndigheter och företag

på ett säkert sätt skall kunna utbyta hemlig information med myndigheter och företag i andra länder och 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 av JAS 39 Gripen och deltagande i operationer som KFOR och ISAF.

Den militära säkerhetstjänsten förhandlar fram dessa avtal efter bemyndigande från regeringen, till vilken även förhandlingsresultaten redovisas. Avtalen bygger på de deltagande ländernas nationella lagstiftning på området och avtalstexten anpassas efter dessa förhållanden. Avtalen ingås normalt av regeringen och publiceras i serien Sveriges Överenskommelser, SÖ, som ges ut av Utrikesdepartementet.

Under året har förhandlingar om bi- och multilaterala säkerhetsskyddsavtal genomförts med ett flertal länder. Den militära säkerhetstjänsten bemyndigades under året att inleda förhandlingar med Bulgarien, Kroatien, Irland och Singapore. Avtalen med Bulgarien och Polen signerades under 2007 och det som avser Bulgarien har även trätt ikraft.

Den militära säkerhetstjänsten deltar också kontinuerligt i säkerhetsarbetet inom samarbetsavtalet rörande den europeiska försvarsindustrins omstrukturering, vilket också berör bilaterala säkerhetsfrågor med de deltagande länderna

– Storbritannien, Spanien, Frankrike, Tyskland och Italien.

Genom att Sverige är den ledande nationen i den nordiska snabbinsatsstyrkan Nordic Battle Group har den militära säkerhetstjänsten fått en samordnande roll gentemot de övriga deltagarländernas säkerhetstjänster. Detta arbete kommer att pågå tills dess att beredskapstiden är över.

Under 2008 är arbetet med säkerhetsfrågorna för försvarsmaterielsamverkan, främst rörande exportsatsningar för JAS 39 Gripensystemet, högst prioriterat. I övrigt kommer förhandlingsarbetet avseende internationella säkerhetsavtal att fortgå och i några fall avslutas under 2008. Några avtal bedöms också träda i kraft. Deltagandet i säkerhetssamarbetet inom EDIR FA förväntas också att fortskrida i samma omfattning som tidigare. ■

Signalskyddstjänst

Försvarsmakten har uppgiften att leda och samordna signalskyddstjänsten inom hela totalförsvaret. Uppgiften inkluderar även utveckling och framtagning av nationellt godkända kryptografiska funktioner som syftar till att skydda skyddsvärd information.

Inom totalförsvaret ansvarar säkerhetskontoret för utveckling och granskning av kryptografiska metoder och signalskyddssystem, framtagning av regelverk samt försörjning av kryptonycklar, certifikat och aktiva kort.

Till grund för verksamheten ligger en årlig plan för signalskydds- och kontrollverksamheten. Planerna ger en god grund för dialogbaserad utveckling av signalskyddsverksamheten i syfte att säkerställa ett fullgott signalskydd inom totalförsvaret.

Utvecklingsarbetet beskrivs i kapitlet Teknikutveckling.

NCSA

Rollen som National Communications Security Authority (NCSA) utövas av säkerhetskontoret. Rollen innebär att inom

kryptoområdet stödja regeringskansliet i kryptofrågor som rör internationell verksamhet.

Året har präglats av stöd till följande arbetsgrupper:

- Galileo-projetet (satellitnavigeringssystem)
- ITTF (Implementation Tempest Task Force)
- BICES (Battlefield Information Collection Exploitation System)
- SESAME-projektet (EU:s nästa system för nivån EU SECRET)

I rollen som NCSA har ett antal godkännandeskrivelser för utländska kryptosystem (t.ex. Link 16) utfärdats. Dessa system har anskaffats för att möjliggöra interoperabilitet i de olika internationella uppgifter som Sverige åtagit sig, men det finns vissa begränsningar för systemens användande. T.ex. får kryptosystemen endast användas för skydd av information som är delgivningsbar (”releasable”) till de länder som har tillgång till samma kryptonycklar. Systemen är ej godkända för hantering av övriga hemliga uppgifter som omfattas av sekretess enligt sekretesslagen och som rör rikets säkerhet.

Flera s.k. COMSEC-avtal har förhandlats fram och fastställts under året, bl.a. med de i EU:s snabbinsatsstyrka NBG deltagande nationerna. COMSEC-avtal utarbetas vid tillfällen då svenska signalskyddssystem tillhandahålls åt annan nation eller internationell organisation eller då Sverige tillhandahålls annan nations eller internationell organisations kryptosystem.

Inom det internationella området har fokus bl.a. legat på NBG genom att flera avdelningar inom säkerhetskontoret under året har stöttat med signalskyddskompetens. Fler utländska system har under året införskaffats (bl.a. till NBG) och ett tätare samarbete med EU och NATO har inletts avseende kryptonycklar till flertalet system.

För att kunna informera om nyheter inom signalskyddstjänsten och möjliggöra för erfarenhetsutbyte mellan signalskyddstjänstens olika företrädare, genomförs årligen ett antal signalskyddsmöten. Dessa möten riktar sig till signalskyddschefer och företrädare för signalskyddstjänsten vid centrala, regionala och lokala myndigheter samt till organisationsenheter inom Försvarsmakten. Deltagande i mötena är också ett sätt att bibehålla aktuell signalskyddsbehörighet.

Under våren genomfördes tre regionala signalskyddsmöten (i Stockholm, Umeå och Göteborg). Dessa planerades och genomfördes av Säksamsektionerna i samverkan med Krisberedskapsmyndigheten, KBM.

Under hösten genomfördes dialoger mellan säkerhetskontoret och myndigheter/organisationer inom totalförsvaret. Dialogerna syftar dels till ett ömsesidigt informationsutbyte och dels till att klarlägga respektive myndighets framtida behov av kryptoprodukter.

I samarbete med KBM arrangerades i december det årliga centrala signalskyddsmötet. Till mötet inbjöds signalskyddschefer och företrädare för signalskyddstjänsten vid centrala myndigheter och organisationsenheter samt Försvarsmaktens centrala och regionala ledningsorgan. Mötet samlade ca 120 deltagare under två dagar.

Regelverk

Arbetet med en genomgripande översyn och revidering av Försvarsmaktens interna bestämmelser om signalskyddstjänsten har under året fortsatt. Den tidigare genomförda utredning som behandlade ledningen av Försvarsmaktens signalskyddstjänst har lagt grunden till reviderade interna bestämmelserna. Arbetet har bedrivits i nära samarbete med berörda delar inom Försvarsmaktens högkvarter.

Handbok Totalförsvarets Signalskyddstjänst, H TST Grunder 2001 har under året reviderats i samarbete med totalförsvarets signalskyddsskola, TSS. Handboken innehåller bl.a. allmänna råd och föreskrifter för signalskyddstjänsten inom totalförsvaret och riktar sig till personal som:

- planlägger, leder och samordnar signalskyddstjänsten inom totalförsvaret
- nyttjar betjänar eller på annat sätt handhar signalskyddssystem
- utvecklar, anskaffar, underhåller, förrådshåller och avvecklar signalskyddsmateriel

Under året har också följande instruktioner tagits fram:

- I TST MGB and I TST MGBI CSO Interim v. 2.0
- I TST MGB and I TST MGBI LSO Interim v. 2.0
- I TST MGZI 2007

Kundanpassad Produktion (KaP)

Utvecklingen av Kundanpassad Produktion, KaP, har fortsatt enligt plan. KaP syftar till att ur kryptonyckelmottagarens synvinkel förenkla dagens produktion och distribution av kryptonycklar. Detta genom att samtliga kryptonycklar distribueras direkt till respektive organisationsenhet. På så sätt kortas ledtider från beställning till slutlig leverans. Konceptet KaP bedöms kunna ersätta dagens produktionsmetod under 2008. Under året har en referensgrupp för KaP påbörjat sitt arbete. Referensgruppen är brett och representativt sammansatt med deltagare från de delar av totalförsvaret som berörs av utvecklingen av KaP. Samma referensgrupp kommer även att bistå i utvecklingen av eNFÖ.

Elektronisk Nyckelförsörjning (eNFÖ)

Elektronisk nyckelförsörjning är ett projekt inom signalskyddstjänsten som syftar till att framtidsanpassa och modernisera signalskyddsverksamheten vad gäller säkerhet, användningsområden och teknik. Det innebär bl.a. att kryptonycklar (vilka i dag distribueras i pappersform) i huvudsak skall kunna distribueras på ett säkert

sätt i elektronisk form, direkt varifrån produktionen av kryptonycklar sker, till slutanvändaren (enskild kryptoapparat). För att uppnå detta krävs djupgående tekniska och administrativa kunskaper, tid för utveckling samt hållbara rutiner.

I syfte att skapa underlag inför eNFÖ har liknande system studerats och målsättningsarbetet påbörjats. Referensgruppen för eNFÖ har påbörjat sitt arbete och studier startats för när en övergång till eNFÖ kan ske. Utvecklingen av KaP och eNFÖ samordnas för att utvecklingen skall vara så sammanhållen som möjligt.

Kryptonycklar, certifikat och totalförsvarets aktiva kort

Aktiva kort tas fram av Försvarsmakten för användning inom totalförsvarets olika system som kräver säker identifiering av användare vid behörighetskontroll (autentisering). Vissa aktiva kort (TAK och TEID) är dessutom avsedda att användas för signering av information (digital signatur) samt som bärare av data (främst kryptonycklar). Korten kan även användas för kryptering.

Om ett meddelande skall krypteras använder avsändaren mottagarens publika nyckel för att kryptera meddelandet och mottagaren dekrypterar det med sin privata nyckel. För att en mottagare skall kunna lita på att en publik nyckel hör till rätt avsändare sprids den i form av ett certifikat. Certifikatet är ett signerat intyg från Certification Authority, CA, vilket anger att en publik nyckel hör till en viss avsändare. Systemet bygger på tilltro till CA och därmed även tilltro till de certifikat som CA signerat. Första steget i kedjan måste alltid vara att användaren har tillgång till och kan lita på CA:s publika nyckel för att kunna verifiera mottagna certifikat.

För servrar eller datorer med behov av att kunna utföra många autentiseringar eller signaturer per tidsenhet räcker inte kapaciteten hos ett aktivt kort till. För vissa av dessa servrar/datorer är det heller inte enkelt att ansluta en kortterminal. I sådant fall används RSA-nyckelpar och certifikat levererade på en CD i form av en fil skyddad med ett lösenord som läses in i servern/datorn. Eftersom dessa certifikat levereras i form av mjukvara kallas de mjuka certifikat.

Produktion och distribution av kryptonycklar, certifikat och totalförsvarets aktiva kort har genomförts enligt plan. Certification Authority-tjänsten för totalförsvarets aktiva kort generation 1 (t.ex. TAK/Pers) har avvecklats och ersatts av totalförsvarets aktiva kort generation 2 (t.ex. TAK, NBK och TEID). Efterfrågan på CA-tjänsten har ökat avsevärt under 2007. Bland annat har FMV tillkommit som kund.

Signalskyddsincidenter

Det totala antalet incidenter är ungefär likvärdigt med föregående år. Omfattningen av antalet signalskyddsincidenter är godtagbar med hänsyn till det stora antalet nycklar som dagligen hanteras inom totalförsvaret, men generellt ej godtagbar vad gäller hanteringen av Försvarsmaktens signalskyddsmateriel.

Nyckelincidenter

Antalet anmälda nyckelincidenter under året har legat på samma nivå som tidigare år. Under 2007 har dock fördelningen mellan olika typer av rapporterade incidenter till viss del avvikit från den traditionella bilden. Anledningen till detta är att ett ovanligt stort antal incidenter bestått i inläsningsproblem på grund av felaktigt tillverkade nycklar. Denna typ av fel brukar annars normalt förekomma i högst ett eller några enstaka fall per år. Även några fall av saknad nyckel till följd av distributionsproblem har uppmärksammats. Antalet incidenter med aktiva kort och certifikat är fortsatt lågt i antal.

Kryptofunktion för skyddsvärda uppgifter

Försvarsmakten ansvarar för att leda och samordna arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information. Inom signalskyddstjänsten har ett arbete påbörjats med att definiera vad säkra kryptografiska funktioner innebär. Säkra kryptografiska funktioner syftar till att få ett väl fungerande skydd av information och uppgifter som omfattas av sekretess, samt även skydd för annan information enligt respektive organisationsenhets bedömande. Med anledning av detta har Säkerhetskontoret under 2007 påbörjat utveckling av Kryptofunktion för Skyddsvärda Uppgifter, KSU, samt ett regelverk för KSU. Viktigt att framhålla är dock att KSU under inga omständigheter får användas för skydd av information som är hemlig och rör rikets säkerhet. Det första system som avses godkännas för KSU är ett program för kryptering av filer, ett s.k. filkrypto. ■

Teknikutveckling

Teknikutveckling inom säkerhetstjänsten består av utveckling av signalskyddssystem och kryptosystem för skyddsvärda uppgifter samt utveckling av generella IT-säkerhetsprodukter och komponenter. Med utveckling avses kravställning, verifiering och godkännande medan själva utvecklingen görs av industrin efter upphandling av Försvarets Materielverk, FMV. Även tekniska granskningar och bedömningar av system och säkerhetslösning ingår i teknikutvecklingen.

Säkerhetsgranskningar

Sektionen för IT-säkerhetsutveckling har under året genomfört en mängd tekniska granskningar av system och säkerhetsprodukter. I flertalet fall har allvarliga brister hittats som medfört att driftsatta system tagits ur drift och att utvecklingsprojekt blivit försenade. För att komma tillrätta med problemet har ett arbete påbörjats för att revidera Försvarsmaktens krav på IT-säkerhetsfunktioner. Under året togs bland annat en granskningsmetodik för kommersiella IT-produkter fram. Ett samarbete med Sveriges Certifieringsorgan för IT-säkerhet, FMV/CSEC, har inletts i syfte

att studera metoder för granskningar av IT-säkerhet i produkter och system.

Säkerhetskontoret fortsätter att stödja Försvarsmaktens chief information officer, CIO, i auktorisations- och ackrediteringsprocesserna. Under året omorganiserades stödet i syfte att bland annat skapa en sammanhållen kontaktyta gentemot utvecklingsprojekten. Säkerhetskontoret har uppgiften att godkänna säkerhetsfunktioner och avge yttrande angående säkerheten innan driftsättning. Ett 50-tal auktorisationsärenden och ett 20-tal ackrediteringsärenden handlades under 2007. Stora resurser har lagts på att säkerställa att system som skall användas i NBG haft en tillräcklig säkerhetsnivå. Andra prioriterade projekt har varit PRIO, NBF och IS UNDSÄK.

Utveckling av gemensamma säkerhetsprodukter

Sektionen för IT-säkerhetsutveckling har ett nära samarbete med FMV för att ta utveckla och anskaffa gemensamma IT-säkerhetsprodukter för integrering i olika utvecklingsprojekt inom Försvarsmakten och FMV. Under året utveckades och granskades bland annat filterapparaten GARM. GARM kan användas när system som hanterar hemliga uppgifter behöver ansluta till olika typer av öppna nät. GARM skall användas av bl.a. stridsledningscentraler.

Under framtagning är också komponenter för att använda aktiva kort (TAK och TEID) vid inloggning i Windowssystem, produkter för skydd mot okänd kod (SMOK) och okända externa enheter (Deviceblocker), kontrollvertyg samt säker radering av lagringsmedia.

Strategi för säkerhetsloggning

I samarbete med FMV har säkerhetskontoret påbörjat ett arbete med att ta fram en gemensam strategi för säkerhetsloggning. Arbetet syftar till att ta fram syfte och mål med säkerhetsloggning, riktlinjer (däribland minsta gemensamma loggmängd) samt verktyg inom områdena insamling, analys, och arkivering.

Kryptoutveckling

Under 2007 har fem nya signalskyddssystem godkänts för användning:

- Signalskyddssystem MGB/MGBI, vilket är ett nytt krypto för Virtuella Privata Nätverk (VPN) för överföring av sekretessbelagd information mellan slutna IP-baserade nätverk. MGB/MGBI har godkänts för signalskyddsgrad Top Secret (SG TS). Godkännandet gäller för användning inom hela totalförsvaret.

- Signalskyddsystem MGFI, Telefonkrypto 7301 även kallat Mobilt krypto Secret, är avsett för kryptering av tal/data och har

godkänts för signalskyddsgrad Secret, SG S. Systemet består bl.a. av en handhållen terminal för kryptering och dekryptering av tal i flertalet kommunikationsnät såsom det fasta telenätet, GSM-nätet och via satellit. Den första versionen av systemet finns endast i begränsat antal och är anpassad för NBG:s behov. Nästa version av Mobilt krypto Secret beräknas godkännas under första halvåret 2008 och kommer att användas inom hela totalförsvaret.

- Signalskyddsystem MAEI, Mobilt Taktiskt Talkrypto, för kryptering av tal/data över Truppradio 180 och Digitaltelefon 9000. MAEI har godkänts för signalskyddsgrad Restricted (SG R). Systemet används inom NBG och inom de förband och enheter som har behov av att kommunicera säkert med NBG.

- Signalskyddssystem MFFI, är en radiolänk för JAS39 Gripen som godkänts för signalskyddsgrad Restricted (SG R).

- Signalskyddsystem MSSI, är ett flygburet telemetrikrypto som godkänts för signalskyddsgrad Secret (SG S).

Dessutom har nya versioner av signalskyddssystem MGS/MGSI FKA (Filkrypto för SG S) och PGAI (Restricted-Färist) godkänts.

Följande system är planerade att godkännas under 2008:

- Signalskyddssystem PGBI, vilket är ett filkrypto för signalskyddsgrad Restricted (SG R).

- Signalskyddssystem PGCI, vilket är ett hårddiskkrypto för signalskyddsgrad Restricted (SG R). ■

Säkerhets- och signalskyddskontroll-verksamheten

För att Försvarsmakten ska kunna uppfylla aktuella säkerhetsbestämmelser till skydd för rikets säkerhet, skydd mot terrorism samt för att motverka kriminalitet riktad mot Försvarsmakten och dess tillsynsområde genomförs årligen ett stort antal säkerhetskontroller. Den militära säkerhetstjänsten har funktionsansvar för all säkerhetskontrollverksamhet som genomförs i Sverige och utomlands. En säkerhetskontroll består av hotbildskontroll, säkerhetsskyddskontroll och kontroll av signalskyddstjänsten.

Försvarsmakten genomför säkerhetskontrollerna med stöd av säkerhetsskyddslagen och säkerhetsskyddsförordningen vad avser Försvarsmakten och dess tillsynsmyndigheter. Säkerhetskontoret ansvarar och genomför dessutom ett stort antal kontroller av signalskyddstjänsten vid myndigheter inom totalförsvaret som har signalskyddsutrustningar med kryptonycklar från Försvarsmakten.

Kontrollerna inom Sverige genomförs av säkerhetskontoret eller OPS J2 genom sina fyra säkerhets- och samverkanssektioner lokaliserade till Malmö, Göteborg, Stockholm och Boden. OPS J2 har ansvaret för huvuddelen av Försvarsmaktens nationella kontroll-

objekt. Undantagna är Försvarsmaktens och FMLOG:s centrala ledning samt vissa centra, som utgör säkerhetskontorets kontrollansvar. Utöver dessa har säkerhetskontoret säkerhetskontrollansvar för Försvarsmaktens tillsynsmyndigheter (FRA, FMV, FOI, FortV, TPV, FHS och FUN) och för kontroller utomlands. Dessa genomförs på de platser där Försvarsmakten löser uppgifter inom utlandsstyrkan, vid våra försvarsavdelningar och vid vissa ambassader.

Målet för kontrollverksamheten är att ständigt ligga i takt med och helst före hot- och riskutvecklingen. Viktigt i kontrollverksamheten är att i dialog med myndigheternas/förbandens säkerhetsföreträdare klarlägga om organisationen uppfattat och följer gällande säkerhetsbestämmelser. Vidare kontrolleras alltid hur kontrollerad myndighet/förband uppfattar hotläget och risksituationen för att bedöma om särskilda utbildningsinsatser behöver vidtas.

På detta sätt utgör kontrollprocessen ett stöd till den lokala säkerhetstjänsten i syfte att myndigheten eller förbandet ständigt ska kunna göra korrekta hotbedömningar samt vidta rätt säkerhetsskyddsåtgärder.

Försvarsmaktens kontrolläge

FM kontrolläge är en metod för att snabbt ge Försvarsmaktens ledning information om säkerhetsbrister och upptäckta hot inom och mot Försvarsmakten, samt vid de myndigheter där Försvarsmakten har tillsynsansvar.

Kontrolläget i såväl Sverige som i utlandsstyrkan sammanställs veckovis. Operativ ledare för säkerhetskontoret beslutar därefter vad i underlaget som skall bifogas till Försvarsmaktens gemensamma lägesbild (FMGL). Kontrolläget som redovisas i FMGL ska belysa de viktigaste bristerna i säkerhetsskyddet och nya hot som uppdagats vid de senaste säkerhets- och signalskyddskontrollerna. Därmed möjliggör FMGL Kontrolläge att säkerhetsbrister uppmärksammas på bredd inom Försvarsmakten samt att Försvarsmaktens högsta ledning omedelbart orienteras om viktigare delar av aktuellt säkerhetsskyddsläge.

Utlandskontrollverksamheten

Under 2007 har kontrollverksamheten haft ett fortsatt tydligt fokus på utlandsstyrkan. Säkerhetskontoret har vid dessa kontroller haft ett nära samarbete med OPS J2 samt Armé- och Marintaktiska staberna, vilket gjort att upptäckta säkerhetsbrister förhållandevis snabbt kunnat åtgärdas. Kontroller har genomförts vid de svenska truppmissionerna i Afghanistan och Kosovo samt vid den marina insatsen i medelhavet. Kontrollerna har inriktats på att kunna nå även de geografiskt yttersta delarna av förbanden, vilket visat sig nödvändigt för att få en relevant uppfattning om det verkliga säkerhetsläget.

Strävan är att genomföra en säkerhetskontroll så tidigt som möjligt efter att ett förband anlänt till missionsområdet. Detta för att tidigt i missionen ge förbandets säkerhetsorganisation stöd inför kommande tjänst. På så sätt kan också

brister i säkerhetsskyddet upptäckas tidigt och åtgärdas.

Säkerhetskontorets kontroller utomlands har, utöver utlandsstyrkan, genomförts vid försvarsavdelningarna i:

- Tallin, Estland
- Budapest, Ungern
- Rom, Italien
- Ankara, Turkiet
- Tel Aviv, Israel
- Samt vid den framskjutna flygbasenheten i Förenade Arabemiraten, FOB FAE.

Vid förbandet i Bosnien har en uppföljningskontroll genomförts under hösten beroende på upptäckta brister under vårens periodiska kontroll vid förbandet.

Den internationella dimensionen inom kontrollverksamheten kommer fortsätta att vara prioriterad. I de delar av utlandsstyrkan som har ett gott säkerhetsläge och som bedöms som stabila kommer dock antalet kontroller att reduceras från två till en per år.

Grundkontroll av FRA

Under 2007 genomfördes en stor planerad grundkontroll vid Försvarets radioanstalt, FRA. Under en veckas tid kontrollerades den centrala ledningen och verksamheten på Lovön. Den senaste kontrollen genomfördes för fem år sedan. Detta i kombination med den

snabba utvecklingen inom informationsteknikområdet gjorde det nödvändigt med en ny grundkontroll. Resultatet av kontrollen är sekretessbelagt men i detta fall, såväl som i de flesta, så finns utrymme för förbättringar av säkerhets- och signalskyddet.

Operativ chefs kontrollansvar

OPS J2 har genom sina Säksamsektioner under 2007 kontrollerat ett antal garnisoner, centra och skolor. Kontrollresultaten har varierat på samma sätt som tidigare år men vissa brister tycks vara generella. Exempel på dessa är brister i säkerhetsplaneringen och internkontrollverksamheten. Liksom tidigare år har respektive Säksamsektion lämnat de kontrollerade värdefullt stöd genom att tillse att adekvata åtgärder snabbt sätts in för att stärka säkerhetsskyddet, då väsentliga brister har upptäckts.

Kontroll av signalskyddstjänsten vid civila myndigheter

Uppföljning och kontroll av signalskyddstjänsten har under året genomförts vid 36 enheter inom Jämtlands-, Stockholms-, Uppsala- och Västernorrlands län. Detta innebär kontroller av såväl statliga och landstingskommunala myndigheter och institutioner som av statliga bolag. Brister förekommer men överlag är resultaten generellt sett goda vid de myndigheter etc. som kontrollerats.

Utveckling av kontrollverksamheten

Under året har säkerhetskontoret bedrivit ett utvecklingsarbete av kontrollverksamheten. Tolv arbetsgrupper har skapats för att förbättra och effektivisera olika delområden inom kontrollverksamheten.

Gruppernas utvecklingsarbete har bl.a. berört:

- Utvärdering och analys av kontrollresultaten
- Långsiktig planering av kontrollverksamheten
- Nya protokoll och delområdesmallar
- Ny kontrollportal i IS UNDSÄK
- FM kontrolläge

Mängder av säkerhetskontroller har genomförts under åren men någon systematisk granskning och utvärdering av resultaten har inte genomförts. Det är mycket angeläget att detta område utvecklas för att förbättra möjligheterna att inrikta framtida kontrollverksamhet.

Den långsiktiga kontrollplaneringen innefattar alla delar av säkerhetskontrollverksamheten inom Försvarsmakten. Kontrollcykeln som idag är femårig förändras till att bli sjuårig. Förändringen innebär att det får dröja högst sju år mellan två planlagda grundkontroller. Mellan grundkontrollerna genomförs en uppföljningskontroll och ett begränsat säkerhetsskyddsbesök. De resurser som därigenom kan frigöras ska främst användas till att öka antalet särskilda kontroller av överraskande natur.

En av arbetsgrupperna har tagit fram nya kontrollmallar för nio delområden inom kontrollverksamheten för att förenkla, snabba upp och kvalitetssäkra protokollskrivningsarbetet. Brister har tidigare funnits när det gäller efterarbetet av en kontroll samt att kunna distribuera ut protokollen i rimlig tid. Under 2008 kommer dessa mallar att prövas och ytterligare förbättras.

Vid årsskiftet infördes en försvarsmaktsgemensam kontrollportal i IS UNDSÄK. Varje enskild kontroll får inom ramen för portalen en egen mapp där samtliga dokument och handlingar kopplade till kontrollen samlas och sparas på ett strukturerat sätt. Den som deltar i en kontroll får tillgång till aktuell mapp, dock i varierad grad. Behörigheten att ta del av materialet i mapparna styrs av individens befattning och organisatorisk tillhörighet.

FM Kontrolläge har utvecklats ytterligare genom att det införts s.k. förhandsrapporter.

I dessa presenteras övergripande de viktigaste slutsatserna av varje kontroll. Viktigare åtgärdskrav följs upp och presenteras i FM Kontrolläge tillsammans med beslutade tider för remissvar och åtgärdsplaner.

Upptäckta fel och brister

Protokollen från de två senaste kontrollåren har utvärderats. Slutsatsen är att kontrollverksamheten fyller en viktig funktion för att upptäcka och komma till rätta med de brister som finns. Här bredvid beskrivs ett antal generella och allvarliga brister som har åtgärdats eller är på väg att åtgärdas.

Ledning, säkerhetsutbildning och internkontroll
Det kan konstateras att brister i säkerhetsplaneringen är genomgående, såväl inom som utom Försvarsmakten. Med säkerhetsplanering avses främst säkerhetsanalyser, säkerhetsskyddsplaner, signalskyddsinstruktioner, IT-säkerhets- och förstöringsplaner. Bristerna kan gälla avsaknad av ett eller flera av ovanstående dokument alternativt att vissa av dessa inte håller tillräckligt god kvalitet.

Vanligt förekommande fel är brister i säkerhetsutbildning och internkontroll dvs. områden som är av stor vikt för det allmänna säkerhetsmedvetande och förmågan att hantera uppkomna säkerhetsproblem på rätt sätt.

Personalproblem inom säkerhetstjänsten medför ofta för svaga organisationer med ingen eller liten flexibilitet. Det förekommer även att personer får ansvar för flera tunga befattningar inom säkerhetstjänsten samtidigt t.ex. säkerhetschef, IT-säkerhetschef, signalskyddschef. Även dubbelbefattningar med jävsrisker förekommer såsom IT-säkerhetschef och IT-chef.

Hotbildsuppfattning
Kunskaperna om hot och risker varierar starkt liksom hur man använder erhållet hotbildsunderlag i det egna säkerhetsanalysarbetet.

Informationssäkerhet
Brister finns regelmässigt i hanteringen av

sekretessbelagda handlingar, främst inom landet. Det handlar ofta om fel i kvittering och utformning av hemliga handlingar, brister i registrering och förekomst av s.k. ”svartkopior”. Hemligstämpling på felaktiga grunder förekommer också inom många delar av tillsynsområdet.

IT-säkerhet
Lättåtkomliga server- och korskopplingsutrymmen samt oskyddade kablage ger påtagliga risker för IT-driften i händelse av beskjutning eller brand. Brister förekommer också när det gäller ackrediteringar och säkerhetsmålsättningar.

Tillträdesbegränsning
Nationellt så bedöms huvuddelen av tidigare problem vara åtgärdade men fortfarande finns problem med låssystem. Exempel finns på låssystem där alla nycklar inte har kunnat redovisas. Inom utlandsstyrkan förekommer dock ofta brister inom detta område, främst beroende på logistiska och tekniska problem.

Brister har konstaterats i perimeterskyddet av våra ”camper” i utlandsstyrkan. Med perimeterskydd avses områdesskyddet (staket, inkörningshinder, vakttorn, chikaner, strålkastare, larmanläggningar, murar, beskjutningsskydd) och rätt rutiner för bevakning, rondering och insats. Åtgärder har vidtagits eller pågår för närvarande.

Avsaknad av splitterskyddade förläggningar i områden som utan föregående varning kan utsättas för granatbeskjutning, är normen för närvarande. Detta avser inte tillfälliga fältförläggningar utan platser som vi använder under lång tid och som motståndare lätt kan nå med olika vapen.

För vapen- och ammunitionsförvaring i utlandsstyrkan ges ofta avsteg från regelverket på grund av svårigheter att få fram lämpliga kassuner samt beroende på att personal alltid finns i tjänst som kan övervaka och skydda vapen och ammunition. Detta innebär dock risker vid t.ex. beskjutning av plats med ammunitionsförvaring med bristande splitter- och brandskydd.

Säkerhetsprövning och SUA
Inom området säkerhetsprövning har konstaterats några fall med bristande kontroll av referenser inför anställning samt att kontinuerlig uppföljning under anställningen inte gjorts på ett önskvärt sätt.

När det gäller SUA förekommer brister främst på grund av okunskap om när SUA-upphandling skall genomföras. Undermåliga säkerhetsanalyser är ofta grunden till felaktigt hanterande. Vidare bedrivs inte alltid den uppföljning som krävs av upphandlade företag i form av säkerhetskontroller och besök. Dokumentationen kring SUA bedöms generellt som bristfällig.

Signalskydd och signalkontroll
Inom signalskyddsområdet har det förekommit att utländsk personal använt svenska signalskyddssystem utan avtal och utbildning. Brister i signalskyddsutbildningen är relativt vanligt och det är inte ovanligt att man fått utbildningen av någon icke signalskyddslärarutbildad.

Brister i förvaringen för kryptonycklar har konstaterats. Dessa har främst bestått i att kryptoapparater, med inlästa nycklar, inte förvarats på rätt sätt eller att många obehöriga har haft tillträde till utrymmen med signalskyddsutrustning.

Övrigt
Brister i utbildningen inför missioner är vanliga när det gäller säkerhetstjänst och angränsande områden såsom Force Protection, åtgärder vid förhöjd hotbild och insatsrutiner av olika slag.

Brister i kraftförsörjning och kylanläggningar är vanligt förekommande och kan generera omfattande säkerhetsproblem då nästan all verksamhet bygger på fungerande IT-system.

Anläggningar för eldfarliga vätskor, inom utlandsstyrkan, ligger ofta på utsatta platser med ringa eller inget skydd, med såväl sabotage- som stöldrisker som följd. ■

FÖRSVARSMAKTEN

107 85 Stockholm Telefon: 08-788 75 00 Fax: 08-788 77 78 www.mil.se