Årsrapport Säkerhetstjänst 2008

HÖGKVARTERET

Militära underrättelse- och säkerhetstjänsten MUST

Årsrapport säkerhetstjänst 2008

Militära underrättelse- och säkerhetstjänsten, MUST

FÖRSVARSMAKTEN

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

Omslaget är tryckt på 300 gr Multiart Gloss och inlagan på 115 gr Multiart Silk.

© Försvarsmakten
Grafisk form: FMLOG APSE, Grafiska ateljén, Stockholm.
Tryckeri: Alfa Print AB

Förord

För sjunde året i rad ger säkerhetskontoret vid den militära underrättelse- och säkerhetstjänsten, MUST, ut en årsrapport. Syftet är att övergripande beskriva den verksamhet som bedrivits under året samt vilka slutsatser och erfarenheter som den genererat. Genom att informera om aktuella säkerhetshot är ambitionen att rapporten också ska bidra till ett ökat säkerhetsmedvetande.

De säkerhetshot som riktas mot Försvarsmaktens verksamheter och intressen är mångfacetterade. Hotet från främmande underrättelseverksamhet ligger kvar på en anmärkningsvärt hög nivå, både nationellt och internationellt. Försvarsmaktens materiel och kompetens tilldrar sig också intresse från den organiserade brottsligheten och radikala grupperingar. Viljan till ökad öppenhet måste därför ur flera avseende kombineras med en förståelse för behovet av att värna våra skyddsvärda tillgångar.

Vidare ställer Sveriges medverkan i internationell krishantering särskilda krav på säkerhetstjänsten. Förmågan att rätt bedöma säkerhetshot är avgörande för att kunna vidta adekvata skyddsåtgärder, inte minst då hotbilden snabbt kan förändras.

En god kapacitet att möta yttre hot kompenserar inte säkerhetsskyddet om problemen finns på insidan. Säkerhetsprövningen av Försvarsmaktens anställda har därför fortsatt att utvecklas. Erfarenheter från kontrollverksamheten visar dock att den löpande uppföljningen måste bli bättre.

Den moderna informationsteknologin förenklar vårt arbete men medför också nya sårbarheter. Brister har konstaterats när det gäller vilken information som överförs på öppna och okrypterade sambandsmedel samt i hanteringen av digitala lagringsmedia, främst USB-minnen. Förtroendet för Försvarsmakten som aktör är bland annat beroende av vår förmåga att hantera sekretessbelagd information. En enskild medarbetares slarv kan snabbt rasera ett förtroende som tagit lång tid att bygga upp. För att komma till rätta med detta genomförs särskilda informations- och utbildningsinsatser under innevarande år.

Säkerhetstjänsten måste ha ett lärande arbetssätt. Slutsatser från kontrollverksamheten och ny kunskap är viktiga beståndsdelar för att utveckla arbetsformer och metoder. Därigenom skapas en smart och vass säkerhetstjänst med en god förmåga till att arbeta förebyggande

Stockholm i juni 2009

Stefan Kristiansson
Generalmajor
Chef för den militära underrättelse- och säkerhetstjänsten, MUST

Fotografer

Sida 13	Peter Liander, FBB
Sida 14	Johan Lundahl, Combat Camera/FBB
Sida 15	Peter Nilsson, FBB
Sida 17	Richard Wissman, FBB
Sida 18	Combat Camera/FBB
Sida 20	Lasse Sjögren, FBB
Sida 21	Andreas Karlsson, FBB
Sida 23	Kjell Lindqvist, FBB
Sida 24	Kim Svensson, Combat Camera/FBB
Sida 27	Andreas Karlsson, FBB
Sida 29	Rickard Bergius, MUST
Sida 30	Andreas Karlsson, FBB
Sida 33	Peter Liander, FBB
Sida 35	Lasse Sjögren, FBB
Sida 37	Nicklas Ehlén, FBB
Sida 38	Nicklas Ehlén, FBB
Sida 41	Bertil Almqvist. Publiceras med tillstånd av Beredskapsmuseet

Innehållsförteckning

Årsrapport säkerhetstjänst 2008

Säkerhet handlar om kontroll

I botten finns alltid ett skyddsvärde, ett objekt. Det kan till exempel vara ett geografiskt område, en byggnad, ett vapensystem, en informationsmängd eller en individ som behöver skyddas. Runt det skyddsvärda objektet etablerar man 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 säkerställa 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 och integritetsaspekter så bestäms omfattningen av kontrollen runt objektet. 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 vanligt att prioritera tekniska kontrollmetoder framför att djupgående granska personers pålitlighet och lojalitet.

När man förlorat kontrollen

En viktig dimension av kontroll är strävan efter att få veta när den går förlorad. Att finna system och metoder som indikerar när kontrollen runt objektet är komprometterad. Vanligtvis är detta ganska svårt, inte minst när det gäller personers pålitlighet och lojalitet men även vid risk för 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 personal, inventering av information, kontroller av säkerhetsskyddet och så vidare.

Att återfå kontrollen

Oavsett skyddsåtgärder kommer man vid vissa tillfällen förlora kontrollen över sitt skyddsvärda objekt. Förmågan att återfå kontrollen måste vara lika god som förmågan till kontroll. Resurser för att utreda och återställa samt planer och förberedelser för att återfå kontrollen i händelse av incidenter är viktiga beståndsdelar.

Organisation och ledning av den militära säkerhetstjänsten

Den militära säkerhetstjänstens uppgift är att tillvarata de säkerhetsintressen som berör Försvarsmakten och dess tillsynsområde enligt säkerhetsskyddslagstiftningen. Säkerhetsintressena omfattar eller kan hänföras till personal, materiel, information, förtroende, anläggningar och verksamhet.

Den militära säkerhetstjänsten har tillsynsansvar över Försvarets radioanstalt, Försvarets materielverk, Fortifikationsverket, Totalförsvarets forskningsinstitut, Totalförsvarets Pliktverk och Inspektionen för Försvarsunderrättelseverksamhet. Dessa myndigheter har också en egen säker-

hetsorganisation som i flera avseende samverkar med Försvarsmaktens säkerhetsorganisation.

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

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

Insatschefen i Högkvarteret leder säkerhetstjänsten i utlandsstyrkan samt den territoriella säkerhetstjänsten i Försvarsmakten med stöd av fyra säkerhets- och samverkanssektioner, Säksamsektioner, i Malmö, Göteborg, Stockholm och Boden.

Säkerhetsunderrättelsetjänsten syftar till att bedöma vilka säkerhetshot som riktas mot Försvarsmakten och dess intressen inom och utom landet. Bedömningen utgör underlag för beslut om skyddsåtgärder. Säkerhetsskyddstjänsten har till uppgift att hindra eller försvåra säkerhetshotande verksamhet samt förlust av skyddsvärd information. Signalskyddstjänsten skall förhindra obehörig insyn i och påverkan av totalförsvarets informations- och kommunikationssystem, samt ansvarar för 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 sju delprocesser:

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

Omvärlden är i ständig förändring och säkerhetstjänsten försöker ligga i framkant när det gäller att utveckla metoder och arbetssätt. Kompetensen inom den militära säkerhetstjänsten är och skall vara på en kvalitativt hög nivå. Våra motståndare är av världsklass och vi skall stå oss väl i konkurrensen.

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 genom informations- och utbildningsinsatser är tydligt då stora resurser måste läggas på att rätta till misstag som begåtts på grund av att medarbetare inte är rätt utbildade och har för lågt säkerhetsmedvetande.

Genom såväl föranmälda, överraskande som särskilda kontroller erhålles bekräftelse 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 den verksamhet som bedrivits bör rapporten ändå kunna ge en god överblick.

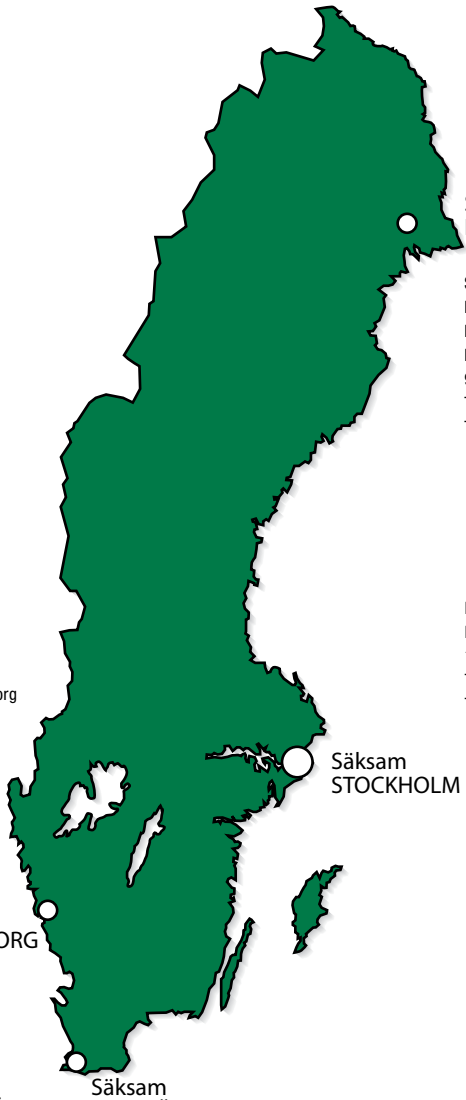
Årsrapporten är ett öppet dokument. Detta begränsar givetvis innehållet. Ambitionen har varit att vara så öppen med information som det är möjligt med hänsyn till sekretesslagen med mera. De uppgifter som inte kan anges i denna rapport återfinns i en hemlig årsrapport.

Här finns den militära säkerhetstjänsten

Centralt

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

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



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

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

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

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

Säkerhetshotande verksamhet

Allmänt om verksamheten 2008

Den militära säkerhetsunderrättelsetjänsten syftar till att klarlägga säkerhetshotande verksamhet som riktas mot Försvarsmakten i Sverige och utomlands. Med säkerhetshot avses främmande underrättelseverksamhet (spionerі och signalspaning), kriminalitet, terrorism, sabotage och subversion. Säkerhetsunderrättelsetjänsten ska främst producera underlag för beslut om säkerhetsskyddsåtgärder men även för fortsatt säkerhetsunderrättelseinhämtning.

Den skyddsvärda verksamheten har under året ökat. Med skyddsvärd verksamhet menas verksamheter som av sekretesskäl eller andra orsaker behöver ett säkerhetsskydd. Exempel på sådana verksamheter är flygvapnets deltagande i den amerikanska övningen Red Flag och marinens deltagande i NATO-övningen Northern Coasts 08. Vidare har övning Viking 08 och ett antal ledningsövningar genomförts som också är att betrakta som skyddsvärd verksamhet. Dessutom upprätthöll Nordic Battle Group beredskap under första halvåret 2008 för att därefter avrustas som förband. Särskilda utmaningar finns kopplade till denna typ av verksamhet främst avseende överförda hot från terrorism.

Försvarsmakten har under 2008 bland annat fortsatt sitt engagemang i Kosovo, ökat sitt truppbidrag i Afghanistan samt genomfört en insats i Tchad. Den främre bas som upprättats i Abu-Dhabi för transportflygdivisionen har fortsatt verka. Inom ramen för exportstöd och samarbeten med andra nationer finns Försvarsmaktens personal och materiel på många platser runt om i världen. Exempel på detta är den personal som tjänstgör i Ungern i ett gemensamt förband för transportflyg.

Försvarsmaktens personal finns därutöver på många platser i världen i enskilda missioner eller stabsbefattningar. I dessa fall har Försvarsmakten dock ett begränsat säkerhetsskyddsansvar. Vid de internationella insatserna ställs ökade krav på identifiering av potentiella angripare och aktörer. En svensk insats kan komma att utgöra ett säkerhetshot mot de parter som förekommer i insatsområdet vilket ställer krav på vår förmåga till kontraverksamhet.

Omfattande prov- och försöksverksamhet har under året genomförts, till exempel vid provplatsen i Vidsel. Den internationella efterfrågan har inte minskat. Tvärtom är det nu allt fler aktörer som vill utnyttja de utmärkta förhållanden som finns för flyg-, UAV- och robotprov.

2006 och 2007 konstaterades brister i rapporteringen av skyddsvärd verksamhet. Detta hade utmynnat i två allvarliga säkerhetsincidenter där främmande makt har haft möjlighet att inhämta underrättelser. De åtgärder som därefter har vidtagits har haft avsedd effekt och bedömningen är att inget liknande har inträffat under 2008.

Övergripande säkerhetshotbild

De främsta säkerhetshoten som riktas mot Försvarsmakten nationellt är främmande underrättelseinhämtning (spioneri och signalspaning) och kriminalitet. Även terrorism måste medräknas med tanke på

de konsekvenser som ett angrepp sannolikt skulle få. Vidare kan Försvarsmaktens övningsverksamhet och insatser nationellt och internationellt medföra ett överfört hot från terrorism mot Försvarsmakten i Sverige beroende på vilka länder eller aktörer som deltar i verksamheten. Vid de internationella insatserna varierar säkerhetshoten med de specifika förutsättningar som finns i insatsområdet. En utförligare beskrivning av den säkerhetshotande verksamheten redovisas i den hemliga årsredovisningen.

Främmande underrättelsetjänst

Hotet från främmande underrättelseverksamhet riktad mot Försvarsmakten är oförändrat högt. Rapporter bekräftar att det finns ett stort intresse från främmande makt för Försvarsmaktens kvalificerade vapensystem. Intresset riktar sig i första hand mot sjö- och luftstridskrafters förmåga och verksamhet.

2008 har det, precis som under 2007, förekommit underrättelseinhämtning, bland annat genom kontakttagning. Officerare och anställda har närmats på ett för dem oskyldigt sätt men där beteendet tyder på en avsikt att eftersöka information som är skyddsvärd. Hur arbetar då en underrättelseagent som har ambition att rekrytera en insider? Metoden och tillvägagångssättet är på inget sätt nytt utan följer en klassisk modell som närmast kan beskrivas som universell.

Inledningsvis söker underrättelseagenten efter personer som är möjliga att närma sig och som har tillgång till den typ av information som han önskar komma över. När agenten funnit en person som motsvarar kraven kartläggs denna varefter nästa steg tas. Agenten närmar sig sin målperson och börjar bygga en relation. Detta kan pågå under en längre tid utan att det sker något konspiratoriskt. Sakta men säkert utvecklas relationen och förtroendet mellan personerna byggs

stegvis upp. Om målpersonen visar sig lämplig och bedöms vara möjlig att rekrytera inleds den sista fasen, rekryteringsfasen. Till att börja med kan agenten be sin målperson ta fram information som inte är hemlig. Steg för steg ökas graden av sekretess på den information som agenten önskar få ta del av, i utbyte mot betalning och gåvor.

Signalspaning från flygande och sjögående plattformar är också en realitet och ett ständigt närvarande hot från flera nationer. Som tidigare redovisats har detta under 2008 dock inte resulterat i någon känd informationsförlust.

När det gäller främmande underrättelseverksamhet riktat mot svenska förband i Försvarsmaktens insatsområden så ligger antalet inrapporterade händelser på samma höga nivå som under 2007. Det finns flera aktörer i ett insatsområde som bedriver underrättelseinhämtning. Statliga aktörer, regionala och lokala makthavare, kriminella och de som aktivt motverkar eller bekämpar de internationella insatserna. Utmaningen ligger i att söka rätt på de indikatorer som kan visa på att informationsinhämtning genomförs då metoderna spänner från personbaserad inhämtning till utnyttjande av informationsteknologi och avancerade spaningssystem.

Även om vaksamheten bland svenska officerare och soldater har förbättrats så finns alltjämt en viss aningslöshet inför det reella hot som föreligger mot en svensk internationell militär insats. Detsamma gäller för de internationella utbyten och samarbeten som Försvarsmakten är inblandad i. Ytterligare utbildningsinsatser måste därför genomföras under 2009 både inför och under planerade missioner.

Terrorism

Under det gångna året utsattes inte Försvarsmakten för några terroristrelaterade incidenter nationellt. De gjorda bedömningarna avseende säkerhetshotet från terrorism riktat mot Försvarsmaktens verksamhet och intressen visade sig därmed överensstämma med utvecklingen under året. Hotbilden är högre i Försvarsmaktens insatsområden än den är nationellt. I Afghanistan har antalet terrorattacker riktade mot den internationella närvaron ökat även om den norra regionen, där huvuddelen av det svenska truppbidraget finns, inte är lika hårt drabbat.

Under 2008 har attentat med improviserade sprängladdningar (Improvised Explosive Device, IED) genomförts men dessa har primärt varit riktade mot lokalbefolkningen eller mot de aktörer som samarbetar med ISAF. Det har förekommit att svenska förband hamnat i strid när förbandets lämnat stöd till Afghansk polis eller militär i deras operationer. I övriga insatsområden har inga incidenter inträffat under det gångna året som direkt kan härledas till terrorism. Dock verkar svenska förband i områden där hotbilden mycket snabbt kan förändras. En förändring kan orsakas såväl av egen genomförd verksamhet eller som överförd hotbild från samarbetsländer.

En förändrad hotbild kan eventuellt ge överspridningseffekter från ett insatsområde till Sverige eller annat geografiskt område där svenska intressen finns. Nationella politiska och militärstrategiska ställningstaganden kan förändra säkerhetshotet mot Försvarsmakten och dess verksamheter. Enskilda missioner och försvarsavdelningar är generellt mer utsatta för denna typ av hot eftersom skyddsnivån där inte är lika hög som i Försvarsmaktens insatsområden. Under 2008 har effekten av bland annat Muhammedkarikatyrer och rondellhundar inte kunnat märkas lika påtagligt som under 2007 men den överförda hotbilden gör att viss vaksamhet bör iakttas eftersom vissa aktörer inte skiljer på svenskar eller till exempel danskar. Hotutvecklingen följs kontinuerligt för att beslut om nya skyddsåtgärder snabbt skall kunna fattas om hotbilden förändras.

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 har dock minskat något och uppgick 2008 totalt till 1062 st. Det kan finnas flera orsaker till detta men sannolikt beror det bland annat på att den vaksamhet och aktivitet som fanns i samband med Nordic Battle Group (NBG) under 2007 med naturlighet har minskat då NBG avvecklats. Inbrott och inbrottsförsök tillsammans med informations- och materielförluster toppar statistiken.

Hot mot personer i Försvarsmakten har förekommit under 2008. Händelserna är mycket komplexa och kräver nära samverkan mellan Försvarsmakten och polis. Kriminella grupper utgör det främsta hotet mot Försvarsmakten i Sverige där tillgreppsbrott eller försök därtill är det vanligaste. I första hand är det vapen, ammunition samt avancerad skyddsutrustning (kroppsskydd, skyddsmask och hjälm) som är eftertraktat att komma över. Under 2008 har ett antal vapen rapporterats saknade och skyddsutrustning har försvunnit eller inte kunnat återfinnas i Försvarsmaktens redovisningssystem. Inventeringsförluster är ett stort problem eftersom det inte kan uteslutas att materielen faktiskt har försvunnit. Försvarsmakten arbetar aktivt med att rätta till dessa brister.

Metallstölder som utgjort ett stort problem för under 2006-2007 har avtagit under 2008. I huvudsak har det rört sig om extern organiserad brottslighet som även drabbat andra än Försvarsmakten. En kombination av effektivt polisarbete och myndighetssamverkan har tillsammans med vidtagna säkerhetsskyddsåtgärder försvårat för aktörerna verka. En bidragande orsak kan också vara att världsmarknadspriset på metaller har sjunkit kraftigt under andra halvåret 2008.

Drivmedelstölder inom Försvarsmakten har under 2008 minskat avsevärt, detta främst i norra Sverige där verksamhet tidigare varit omfattande. Det är sannolikt att de skyddsåtgärder som vidtagits ligger bakom minskningen men det finns behov av fortsatta åtgärder. Tillgreppen sker alltjämt ur fordon i olika typer av förråd

och uppställningsplatser. Det finns tecken som tyder på att det rör sig om både extern och intern kriminalitet.

Internet som arena för spridning av information och försäljning av materiel utgör ett stort problem för säkerhetstjänsten. Antalet inrapporterade händelser under 2008 har ökat jämfört med 2007. Det handlar om sekretessbelagd information om anläggningar som publiceras på olika webbsidor och internetforum samt olika privatpersoners försäljning av Försvarsmaktens egendom genom auktions- och försäljningssidor på internet. Allt som bjuds ut är förvisso inte försvarsmaktsmateriel även om det ser så ut. Vidare finns det även en viss aningslöshet hos Försvarsmaktens anställda. I flera fall har information som lagts ut på mil.se eller förbandshemsidor avslöjat onödig information som i fel händer utgör målsökningsinformation för ett närmande. Det har också förekommit att sårbarheter i olika system har avslöjas.

I Försvarsmaktens insatsområden har det under 2008 inte kunnat uppdagas några större fall av kriminalitet. Hotet från kriminella har till del redovisats under terrorism. Den organiserade brottsligheten också en högst påtaglig aktör såväl på Balkan som i Afghanistan. I Afghanistan har hotbilden lokalt ökat som en effekt av att svensk personal bistått afghansk polis och militär vid olika gripanden. I det svenska området har det uppdagats att en lokal entreprenör bedrivit kriminell verksamhet inom logistikområdet på den svenska campen. Skyddsåtgärder har vidtagits och den säkerhetshotande verksamheten har avbrutits tack vare uppmärksam personal och ett snabbt ingripande.

Subversion

I de internationella miljöer där Försvarsmakten verkar förekommer informationsoperationer som skulle kunna liknas vid subversiv verksamhet. I Afghanistan har detta exempelvis skett då västerländska utbildningsteam genomfört utbildning av afghansk polis där en man tvingats till ett för honom förödmjukande beteende. När detta senare uppdagades var uppfattningen att det var svenska rådgivare som genomfört detta, vilket inte var fallet. Denna typ av händelser påverkar den lokala opinionen negativt och i sin förlängning även säkerheten för svenska soldater. Det är tydligt att svensk personal måste bli mer uppmärksam på detta hot eftersom det så påtagligt används av olika aktörer för att vinna egna fördelar eller splittra sammanhållningen inom till exempel ISAF.

Sabotage

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

IT-säkerhetsrelaterade incidenter

Sektionen för teknisk inhämtning har under 2008 genomfört ett 50-tal tekniska utredningar samt tekniska kontroller av organisationsenheter och informationssystem. 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. Lagring av presentationer eller liknande från internationella insatser eller samarbeten där sekretess förekommer har ökat och måste uppmärksammas särskilt eftersom detta kan få konsekvenser för Försvarsmaktens trovärdighet och ytterst säkerhetsskyddet i våra insatser.

Användandet av USB-minnen för att överföra information mellan olika informationssystem ökar såväl nationellt som internationellt. Denna informationshantering ökar risken för informationsförlust och spridning av skadlig kod vilket bland annat visar sig i antalet förlorade digitala lagringsmedia ökar.

Försvarsmaktens insatser i områden med tuff miljö och begränsade möjligheter att ge informationssystemen bra skydd medför att nya krav ställs på lokal drift och underhåll för att säkerställa tillgänglighet till informationssystemen.

Signalkontroll

Signalkontrollsektionen är ett verktyg för chefen för MUST i uppgiften att bedömma om signalskyddet är tillräckligt.

Syftet med en signalkontroll är bland annat att försvåra eller om möjligt förhindra främmande signalunderrättelsetjänst eller annan obehörig att komma åt information i Totalförsvarets telekommunikations- och IT-system.

Kontrollerna inriktas mot verksamheter som kräver hög eller långvarig sekretess

och genomförs för att konstatera vilken information som kan förloras genom främmande signalspaning.

Under 2008 har bland annat följande aktiviteter genomförts av Signalkontrollsektionen:

- Signalkontroll av Försvarsmaktens högkvarter. Mer än 10.000 telefonsamtal från nyckelbefattningar har kontrollerats. Dessutom har radiotrafik övervakats och analyserats.

- Ett flertal dämpningsmätningar på militära enheter i syfte att klarlägga riskerna för informationsförluster genom röjande signaler (RÖS).

- Ett flertal utbildningsinsatser om signalunderrättelsehotet. Målgrupp för utbildningarna har bland annat varit signalskydds- och IT-säkerhetschefer.

- Deltagande vid prov- och försöksverksamhet med skyddsvärda materielsystem.

- Sårbarhetsanalyser av IT- och telekommunikationssystem.

En negativ tendens avseende signalskyddet har kunnat konstateras under flera år. Ett exempel på information som förmedlats i öppna system är inriktning och tidpunkter för hemlig prov- och försöksverksamhet med skyddsvärda materielsystem. Genom att främmande signalunderrättelsetjänst kan ta del av sådan typ av information i god tid före genomförandet kan förberedelser vidtas för att följa vår skyddsvärda verksamhet. Ett annat exempel är hur säkerhetsskyddade transporter med vapen avhandlats på förbindelser som enkelt kan avlyssnas av obehöriga, exempelvis kriminella grupperingar.

Som ett resultat av konstaterade brister i signalskyddet initierades under 2008 särskilda åtgärder för att säkerställa att skyddsvärd information inte förmedlas på öppna sambandsmedel. Exempel på åtgärder är utbildnings- och informationsinsatser. Dessutom kommer felaktiga beteenden och överträdelser av bestämmelser att följas upp och nödvändiga säkerhetsskyddsåtgärder vidtas.

Detaljerade resultat från kontrollerna framgår i den hemliga årsredovisningen.

Säkerhetsprövning av personal

Säkerhetsprövning ska göras innan en person anställs i Försvarsmakten och därefter löpande följas upp. Detta gäller även för personer som på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet eller som anlitas för uppgifter som är viktiga i skyddet mot terrorism. Den som gör en säkerhetsprövning ska ta ställning till om det finns något som kan ge anledning till osäkerhet om att den person prövningen avser är lojal mot de intressen som säkerhetsskyddslagen ska skydda. Med detta avses i första hand en bedömning av om det till exempel på grund av bindningar med en främmande makt eller en terroristorganisation finns en risk för att personen begår brottsliga handlingar. Personen i fråga kan emellertid utgöra en säkerhetsrisk även om han eller hon är lojal med de intressen som säkerhetsskyddslagen ska skydda. Detta kan vara fallet om vederbörande på grund av sin livsföring eller bakgrund löper risk att bli utsatt för utpressning (sårbarhet) eller om det finns risk för att personen genom oaktsamhet (slarv eller oavsiktligt) avslöjar sekretessbelagd information. Säkerhetsprövningen ska därför omfatta både en bedömning av den prövades lojalitet och dennes pålitlighet från säkerhetssynpunkt. Det är vanligtvis graverande för en prövad individ om det förekommer

uppgifter om denne i polisens register. Normalt avslås då en ansökan om anställning. Är individen redan ianspråktagen av Försvarsmakten görs en personutredning av säkerhetskontoret på grundval av den tillgängliga informationen.

Antalet personärenden som krävt utredning med påföljande säkerhetsskyddsbeslut har under året legat på ungefär samma nivå som 2007, vilket innebär cirka 500 fall. Vanliga anledningar till utredning är utlämnade uppgifter från polisen om rattfylleri, misshandel, stöld och olaga vapeninnehav. Bruk av alkohol är den främst bidragande orsaken till att personal begår brott. Säkerhetskontoret har i flera fall under 2008 nekat individer att delta i internationell tjänst på grund av alkoholrelaterade problem eller kriminell belastning.

Även utlämnade uppgifter från polisen rörande misstanke eller belastning om smuggling, förargelseväckande beteende, olaga hot, olovligt förfogande, häleri, brott mot knivlagen, olovlig körning, osant intygande, bokföringsbrott, bedrägeri, urkundsförfalskning, förskingring, hemfridsbrott, våld mot tjänsteman, brott mot besöksförbud, kvinnofridskränkning, sexuellt ofredande, våldtäkt, narkotikabrott, rån och mord har förekommit. Uppgifter om misstanke om terroristbrott samt vårdslöshet eller obehörig befattning med hemlig uppgift har varit väldigt få under året.

Ett hypotetiskt personärende skulle kunna gestalta sig på följande sätt:
Klockan är halv ett på natten när Anders och Bertil kliver ut på gatan. De har varit hos sin kompis Cesar och invigt hans nya 52-tums platt-tv. Stämningen har varit hög under kvällen tack vare två mål av Zlatan. Några starköl var har de druckit vilket också gjort sitt till för att de ska känna sig på topp. De har kommit överens om att lämna Anders bil på Cesars garageuppfart och göra sällskap på nattbussen eftersom de bor åt samma håll. Men turen är inte med dem. Då de närmar sig busshållplatsen ser de bakljusen på bussen och inser snabbt att de missat den. Efter några mindre väl valda ord säger Anders att det är en timme till nästa buss så det får nog ändå bli så att han tar bilen hem. Han menar att tre starköl tidigare på kvällen inte kan sitta i så länge. Han borde klara gränsen för att

få köra. Bertil är mera tveksam men hans protester är rätt svaga, kanske beroende på att han fryser så han skakar i februarinattens kalla snålblåst.

De är strax på väg ut ur stan i Anders bil. När han svänger ut på huvudleden missar Anders att stanna vid en stoppskylt. I mörkret går det dock inte att missa de kraftiga blåljus som strax därefter börjar blinka bakom bilen. Anders kör ut på vägrenen och stannar samtidigt som han förebrår Bertil varför denne inte hindrade honom från att ta bilen. Polisen som kommer fram säger att hon heter Doris och kommer från trafikpolisen. Hon ber att få se Anders körkort och frågar samtidigt om inte Anders uppmärksammade stoppskylten på Västerleden. Anders svarar lite tafatt att han inte hade sett den. Doris frågar också om Anders druckit någon alkohol under kvällen. I ögonvrån ser Anders att polisinspektören håller en alkometer i handen. Anders förstår att han inte kommer att slippa undan ett alkoholutandningsprov och inser samtidigt att kvällen som började så bra kommer att sluta illa. Och mycket riktigt. När han med viss möda blåst i alkometern visade denna positivt utslag. Anders fick nu följa med till en polisbuss och där blåsa ytterligare en gång, nu i en så kallad Evidencer. Denna visade att alkoholkoncentrationen i hans utandningsluft var 0,27 mg/l, vilket var klart över gränsen för rattfylleri. Det var bara för Anders att lämna bilen på plats. Han och Bertil fick ta sig hem i taxi.

Efter fem veckor får Anders ett brev från åklagarmyndigheten. Det innehåller ett strafföreläggande. Av detta framgår att Anders fått 60 dagsböter á 120 kronor för rattfylleriet. Han inser att det inte är så mycket annat att göra än att bita i det sura äpplet och betala. Den nya datorn han tänkt köpa ser han gå upp i rök. Några djupare tankar om att han gjort något dumt och riskerat andra människors väl och ve har han inte.

En liten oro börjar Anders dock känna för framtiden. Han hade nämligen i början av januari 2008 sökt utlandstjänstgöring i Försvarsmakten. Han hade sökt som stridsfordonsförare eftersom han hade gjort sin värnplikt i den befattningen. Han hoppades verkligen att han skulle bli antagen och få åka iväg till Afghanistan. I början av maj 2008 hade han blivit uppringd av sin blivande plutonchef i missionen. Anders hade fått svara på en rad frågor och även blivit uppmanad att fylla i de blanketter som han strax skulle få hemsända. Han hade också fått redan på att i säkerhetsprövningen inför uttagningen ingick registerkontroll. Plutonchefen hade förklarat att i stora drag gick den ut på att Anders kontrollerades i polisens register. En olustkänsla infann sig direkt hos Anders. Varken till plutonchefen eller i de blanketter han fyllde i nämnde han något om det han varit med om den där eländiga februarinatten. Inte heller det i hans ögon lilla missödet från året före, då han råkat i slagsmål med en gammal skolkamrat i ett öltält under stadsfestivalen, nämnde han. Trots att han i tingsrätten dömdes för misshandel till villkorlig dom med samhällstjänst i fyrtio timmar, höll han tyst om detta. Han bestämde sig för att chansa på att det inte skulle komma fram, det fick bära eller brista.

Men det kom fram. Registerkontrollen avseende Anders inför dennes utlandstjänstgöring resulterade i juni 2008 i en utlämning beslutad av Registerkontrolldelegationen. Den sändes med stöd av säkerhetsskyddslagen till säkerhetsprövningssektionen vid säkerhetskontoret. I svart på vitt stod i utlämningen att läsa att Anders i juni 2007 gjort sig skyldig till misshandel och för detta dömts till villkorlig dom med samhällstjänst fyrtio timmar, och att om fängelse i stället dömts ut hade det blivit en månad. Vidare stod det att Anders godkänt ett strafföreläggande gällande rattfylleri i februari 2008. För detta hade han fått 60 dagsböter á 120 kronor.

I fallet Anders fattades beslut om att han inte fick placeras i säkerhetsklass 3, det vill säga den säkerhetsklass i vilken huvuddelen av de utlandstjänstgörande placeras. Grunden för beslutet var de brott Anders gjort sig skyldig till. Misshandeln pekade på att Anders hade problem med att hantera konflikter på ett acceptabelt och bra sätt. Rattfylleriet gav en indikation på att Anders inte var problemfri vad gällde sin relation till alkohol. Graverande för Anders var också att han vid ansökan till utlandstjänstgöringen varken vid frågor från sin plutonchef eller när han fyllde i blanketterna nämnde de två brott han begått. Han brast i och med detta i pålitlighet från säkerhetssynpunkt. Det fattade säkerhetsskyddsbeslutet fick som en självklar följd att Anders inte kom i fråga för den utlandstjänstgöring han sökt.

För Anders var det med all sannolikhet ett inte välkommet beslut. Ur Försvarsmaktens perspektiv var det beklagligt att en individ som uttryckt vilja att tjänstgöra utomlands inte fick denna möjlighet, men också ett tydligt exempel på hur säkerhetsprövning fungerar och att den fungerar.

Krypto för skyddsvärda uppgifter

Försvarsmakten har sedan länge regeringens uppdrag att kravställa och godkänna signalskyddssystem (kryptosystem) för skydd av hemliga uppgifter som rör rikets säkerhet. Säkerhetskontoret är den enhet inom Försvarsmakten som har denna uppgift. Sedan en tid tillbaka har Försvarsmakten även uppdraget att kravställa och godkänna system för att skydda annan sekretess än sådan som rör rikets säkerhet, till exempel känsliga personuppgifter. Denna typ av system benämns Krypto för Skyddsvärda Uppgifter (KSU). Med skyddsvärda uppgifter menas i detta sammanhang bland annat uppgifter som omfattas av sekretess enligt sekretesslagen men som inte rör rikets säkerhet. Även uppgifter som inte omfattas av sekretess men som myndigheten vill skydda av annan anledning inkluderas i begreppet skyddsvärda uppgifter.

Som ett led i arbetet med KSU har säkerhetskontoret tagit fram ett regelverk. I detta regleras vilka krav som ställs på en myndighet eller organisation som vill använda KSU. Regelverket anger hur kryptonycklar och materiel skall hanteras, vilken utbildning som krävs för att hantera KSU med mera. Till viss del fattar den enskilda myndigheten själv beslut om formerna för användning av KSU varför

tillämpningen av regelverket variera något beroende på vilken typ av information myndigheten vill skydda. Instruktionen är provisorisk och den slutliga versionen beräknas vara klar i slutet av 2009.

Det första systemet för KSU som säkerhetskontoret kravställt och godkänt är en filkryptoapplikation (FKA), som har tagits fram på uppdrag av dåvarande Krisberedskapsmyndigheten. FKA-KSU är en programvara för Windowsmiljö som både kan producera kryptonycklar och kryptera/dekryptera filer. De krypterade filerna kan sedan distribueras över öppna kommunikationsnät som till exempel Internet utan risk för att någon obehörig kan läsa informationen.

Programvaran för FKA-KSU är för en användaren mycket enkel att använda och installera. En stor del av handhavandet sker genom visuella och enkla handgrepp av typen ”dra och släpp” (eng. drag and drop). FKA-KSU förväntas på sikt täcka ett stort uppdämt behov vid svenska myndigheter att på ett enkelt och säkert sätt kunna skydda olika sorters information. Ett tänkbart användningsområdet är inom hälso- och sjukvården där KSU kan nyttjas för att skydda uppgifter som rör enskilda patienters hälsotillstånd eller andra personliga förhållanden, så kallad patientsekretess.

USB-fallet

Bakgrund

I januari 2008 kontaktas Högkvarterets informationsstab av tidningen Aftonbladet. En icke namngiven person har till tidningen lämnat in ett USB-minne innehållande militära handlingar. USB-minnet har personen i fråga funnit i biblioteket på Stockholms universitet. Journalisten uppger att det finns hemliga handlingar på USB-minnet och överlämnar det till Försvarsmakten. Ärendets karaktär gör att det faller på säkerhetskontoret att ansvara för den fortsatta handläggningen.

Vid en genomgång av USB-minnet visar det sig innehålla information rörande Improvised Explosive Device (IED). Ett par handlingar innehåller sekretessbelagda uppgifter och en av de sekretessbelagda handlingarna är utländsk. Ägaren till USB-minnet identifieras genom tekniska undersökningar och en polisanmälan görs. Som underlag till den påföljande förundersökningen gör säkerhetskontoret en så kallad menbedömning, det vill säga en utvärdering och bedömning av vilken skada informationsförlusten kan eller har medfört. Resultatet av denna är att konsekvenserna av det inträffade är att betrakta som ett icke obetydligt men. Detta underlag används senare i åklagarens skriftliga bevisning då åtal väcks mot ägaren till USB-minnet.

Händelseförlopp

Men hur kunde hemliga handlingar hamna på Stockholms universitet? Bakgrunden är följande.

I slutet på april 2006 åkte den åtalade till Afghanistan. Det var hans tredje utlands-

tjänstgöring och han var där som expert på min- och ammunitionsröjning.

Någon gång i augusti 2006 lyssnade han tillsammans med omkring 40 andra soldater och civilanställda på ett föredrag om hotet från IED. Föredraget hölls av en major från ett Natoland engagerat i insatsen i Afghanistan. Hotet hade uppmärksammats alltmer sedan bland annat två svenska soldater dödats i en attack året innan. Alla intresserade fick lyssna på föredraget. Anställda ur lokalbefolkningen fick dock inte var med av säkerhetsskäl. Den åtalade gick efter föredragningen fram till majoren och frågade om han kunde få ta del av det bildmaterial som förevisats för att använda när han skulle utbilda soldater i sin pluton. Majoren var mycket positiv till det och lämnade ut en kopia på en CD-skiva. Denna innehöll i huvudsak det förevisade materialet utan att ange några särskilda restriktioner. Han använde materialet i interna utbildningar inom plutonen. När han skulle åka hem tog han med en fil med bildmaterialet som han lagrade på ett USB-minne, ett minne han även använde för andra dokument. Han var medveten om att bildmaterialet hade beteckningen Secret. Majoren hade enligt den åtalade dock inte gett intryck av att materialet var särskilt känslig ur säkerhetssynpunkt.

I samband med jul- och nyårshelgen 2007 befann sig den åtalade i Stockholm. Eftersom han inte hade någon egen dator behövde han nyttja en dator som han hade tillgång till på universitet. I samband med detta kom han att använda det tidigare nämna USB-minnet. Medan han använde datorn ringde telefonen. Han fick bråttom iväg och kom att glömma kvar minnet i datorn. Han upptäckte förlusten

av USB-minnet först senare och kunde inte hitta det trots att han åkte tillbaka till universitetsområdet. Han visste inte exakt var han hade förlorat minnet. Universitet var stängt och USB-minnet fortfarande inte återfunnet. Något senare fick han höra i media att någon hittat minnet i datorn och lämnat det till en tidning. Han anmälde till sin chef i att det var han som tappat USB-minnet. Den åtalade ansåg att material som är likvärdigt med det han hade på USB-minnet kan hämtas av vem som helst på Internet.

Av den menbedömning som Försvarsmakten gjort står det klart att materialet på filen i orätta händer är känsligt främst i två avseenden. Den ger en motståndare underlag för att anpassa sin taktik/vapenanvändning så att motmedel mot vissa typer av IED till viss del blir overksamma men också att effekten av vissa IED kan ökas. I båda fallen kan de svenska, och samverkande ländernas, förluster i människoliv och materiel komma att öka.

Förundersökningen ledde fram till ett åtal och den 19 november 2008 dömdes den åtalade av Stockholms tingsrätt för vårdslöshet med hemlig uppgift i enlighet med åklagarens ansvarspåstående.

Användning av digitala lagringsmedia

Inom Försvarsmakten har i likhet med samhället i övrigt användningen av digitala lagringsmedia ökat markant i takt med teknikutvecklingen. Digitala lagringsmedia i form av bland annat USB-minnen, externa hårddiskar, bärbara datorer, handdatorer (PDA), minneskort och mobiltelefoner utnyttjas i den dagliga verksamheten i Försvarsmakten.

Tillgången till små bärbara lagringsenheter har inneburit att den enskilde anpassat sitt beteende till de tekniska möjligheterna. I stället för att nyttja bärbara lagringsmedia för att i första hand överföra information mellan olika former av IT-system, vilket var fallet tidigare, har lågt pris och stor lagringskapacitet inneburit att den enskilde numera bär med sig ett digitalt arkiv, med kapacitet att lagra många tusen dokument eller andra filer. En möjlighet som utan tvekan kan underlätta det dagliga arbetet, men som samtidigt innebär påtagliga risker.

Förlust av information är en av de mest påtagliga riskerna när det gäller digitala lagringsmedia. Det aktuella USB-fallet är bara ett exempel på informationsförlust orsakad genom förlust av digitala lagringsmedia. Under 2006 uppmärksammades att digitala lagringsmedia tillhörande den amerikanska krigsmakten var till försäljning på den lokala marknaden utanför den amerikanska militärbasen vid Bagram i Afghanistan. Hårddiskar och andra bärbara lagringsmedia, innehållande bland annat uppgifter om måldata, personuppgifter och samverkande parter, hade enligt uppgift i amerikanska medier stulits på den amerikanska basen.

I Storbritannien har flera uppmärksammade förluster av bland annat bärbara datorer med koppling till den brittiska krigsmakten ägt rum de senaste åren. I ett av de mer uppmärksammade fallen innehöll en stulen bärbar dator

tusentals personuppgifter om brittisk militär personal.

Även inom Försvarsmakten ökar användningen av bärbara datorer och därigenom även informationsförlusterna. Detta ställer i sin tur krav på att skyddsåtgärder i form av exempelvis hårddiskkryptering utvecklas och implementeras.

I det aktuella fallet med USB-minnet var det ett privat USB-minne som användes. Inom Försvarsmakten finns regelverk för vilka IT-system och lagringsmedia som är godkända för användning i Försvarsmakten tillsammans med regler för hur denna typ av utrustning ska auktoriseras och ackrediteras innan de får tas i bruk. Privat utrustning är i regel inte godkänd att använda utan särskilt tillstånd.

Vid användning av digitala bärbara lagringsmedia måste även andra risker uppmärksammas utöver rena informationsförluster. Risken att skadlig kod överförs till Försvarsmaktens system är påtaglig. Likaså att digitala lagringsmedia innehållande ej godkända programvaror exekveras på Försvarsmaktens system med risk att skada tillgängligheten i Försvarsmaktens system.

Åtgärder med anledning av USB-fallet

Den militära säkerhetstjänsten utreder riskerna kopplat till hantering av digitala lagringsmedia och utarbetar löpande förslag till skyddsåtgärder. Dels skyddsåtgärder för att minska risken för informationsförluster, dels hantering av hemliga uppgifter på digitala lagringsmedia.

Skyddsåtgärderna omfattar både tekniska som administrativa moment. Vidare pågår arbeten med att ta fram skyddsåtgärder för att minska riskerna för överföring av skadlig kod och exekvering av ej godkända programvaror vid hantering av digitala lagringsmedia i Försvarsmaktens system.

I samband med de utredningar den militära säkerhetstjänsten genomfört har vid upprepade tillfällen konstaterats brister rörande den enskildes säkerhetsmedvetande, bland annat när det gäller hantering av digitala lagringsmedia. För att komma till rätta med detta krävs omfattande utbildnings- och informationsinsatser. Rätt kunskap och rätt attityd är grundläggande för att kunna minska risken för att medarbetare begår misstag.

Den militära säkerhetstjänsten har under 2008 genomfört flera riktade utbildningsinsatser för Försvarsmaktens säkerhetschefer, IT-säkerhetschefer och annan personal med säkerhetsansvar.

Under innevarande år fortsätter arbetet genom att ett grundläggande utbildningspaket i säkerhetstjänst för all personal i Försvarsmakten tas fram samt inom ramen för ett informationsprojekt kallat Ekeby 2.0.

Radering av digitala lagringsmedia

Av samma anledning som man inte bör slänga hemliga handlingar i papperskorgen så krävs särskilda metoder när man önskar radera en digital fil på ett säkert sätt. En fil som lagras på ett lagringsmedium, exempelvis en hårddisk, består av en sekvens av ettor och nollor som tillsammans representerar filens innehåll. När en fil raderas via datorns operativsystem är det normalt endast en markör som ställs om för att indikera att filen inte längre finns. Det utrymme som filen använde på lagringsmedias markeras därefter som ledigt och kan användas för lagring av nya filer. Den här typen av radering är mycket snabb och används i alla vanliga operativsystem med tillhörande filsystem. Problemet är dock att de ettor och nollor som representerade filens innehåll finns kvar oförändrade och kan fortfarande läsas ut med hjälp av speciella verktyg.

När det gäller vanliga hårddiskar finns det i princip tre metoder för att säkerställa att den information som lagrats på hårddisken inte kan läsas av obehöriga. De första är att fysiskt förstöra disken på ett sådant sätt så att återläsning blir omöjlig. Det andra är att utsätta hårddisken för ett starkt magnetfält så att alla informationsbärande bitar nollställs. Båda dessa

metoder gör att hårddisken blir obrukbar. Det tredje sättet är att använda en särskild programvara för att aktivt skriva över filerna så att ingen tidigare lagrad information kan läsas ut. Denna typ av metod gör att hårddisken kan återanvändas samtidigt som den gamla informationen inte kan återläsas.

För att ett programvara för överskrivning skall vara säker behöver den uppfylla vissa krav. Den behöver kunna identifiera vilken typ av media det är, hur mycket information mediet kan lagra samt kunna skriva över samliga bitar oavsett om de för tillfället används eller inte. I vissa typer av lagringsmedia, däribland vanliga hårddiskar med magnetiska roterande skivor, finns det risk att det finns kvar restinformation efter en överskrivning som skulle kunna utläsas med speciella verktyg om man får fysisk tillgång till lagringsmediet. En programvara för överskrivning behöver därför kunna skriva över flera gånger för att minimera risken för att restinformation finns kvar. Vidare behöver den kunna hantera sektorer på mediet som är gömda eller trasiga. Slutligen behöver den genom verifiering kunna säkerställa att överskrivningen lyckats.

Säkerhetskontoret har under 2008 genomfört interna och externa granskningar för att säkerställa både funktion och tilltro till hos produkter för säker överskrivning. I slutet av året godkändes Överskrivningsverktyg 2.0 som får användas för att radera hårddiskar med hemliga uppgifter. Verktyget består av programvaran Blancco Pro 4.8 med tillhörande direktiv. Blancco Pro 4.8 har upphandlats av Försvarets materielverk med ett licensavtal som medger obegränsad användning för myndigheter inom Försvarsdepartementets verksamhetsområde under den avtalade licensperioden.

Överskrivningsverktyget kan användas i en vanlig fristående PC med den aktuella hårddisken inkopplad. Efter slutförd överskrivning ges en rapport om status för överskrivningen. Rapporten kan sedan skrivas ut på en lokal skrivare eller sparas på externt media.

När Överskrivningsverktyg 2.0 används på hårddiskar som innehåller uppgifter upp till informationssäkerhetsklass HEMLIG/CONFIDENTIAL kan hårddisken efter en lyckad överskrivning betrakta som öppen. För hårddiskar som innehåller uppgifter med högre informationssäkerhetsklasser får hårddisken endast återanvändas i system med samma säkerhetsnivå och måste även fortsatt hanteras som hemlig.

Säkerhetskontroll av Högkvarteret

Säkerhetsskyddslagen anger att all verksamhet som kan få konsekvenser för rikets säkerhet skall kontrolleras. Säkerhetsskyddsförordningen anger att Försvarsmakten har ansvaret för kontrollverksamheten inom den egna myndigheten samt mot ett antal andra myndigheter tillhörande Försvarsdepartementet. Ansvaret för säkerhetskontroller har fördelats mellan säkerhetskontoret och insatsstabens säkerhets- och samverkanssektioner.

En grundkontroll omfattar samtliga säkerhetstjänstens delområden och bör regelmässigt genomföras omkring vart femte, sjätte år. Senast en sådan genomfördes vid Högkvarteret var 1999. Då Högkvarteret genomgått många organisationsförändringar de senaste åren har grundkontrollen skjutits på framtiden. 2007 påbörjades dock planeringsarbetet för att möjliggöra för en förnyad kontroll. Då en grundkontroll av Högkvarteret är ett stort projekt kom den att genomföras inte bara av personal från Säkerhetskontoret utan också av personal från Insatsstaben samt Försvarsmaktens Underrättelse- och säkerhetscentrum. Totalt kom kontrollgruppen att bestå av drygt 30 personer.

Kontrollen hade bland annat till syfte att kontrollera, bedöma och utvärdera:

- grundskyddet i form av vakt, bevakning, larm med mera
- chefers och nyckelpersonals hotbildsuppfattning
- säkerhetsplaneringens innehåll och utformning
- bestämmelsers och policys efterlevnad
- infiltrationsskyddet genom granskning av säkerhetsprövningsområdet och säkerhetsskyddade upphandlingar
- säkerhetsorganisationen ur såväl hotbilds- som skyddsperspektiv
- internkontrollverksamhetens omfattning, genomförande och dokumentation
- säkerhetsutbildningens omfattning, genomförande och dokumentation
- informationssäkerhets- och IT-säkerhetsarbetet
- signalskyddet genom administrativ signalskyddskontroll samt signalkontroll

Kontrollen inleddes med en genomgång av kontrollens upplägg och innehåll för alla chefer samt för de anställda som arbetar med frågor som rör säkerhetstjänst. Under inledningsgenomgången gavs också information om aktuell hotbild. I steg två intervjuades ett flertal av Försvarsmaktens högsta chefer parallellt med att den direkta kontrollverksamheten påbörjades. Den personal som ingick i kontrollgruppen var uppdelad i ett antal mindre grupper som granskade de olika delmoment som kontrollen syftade till att utvärdera. Totalt tog kontrollen mer än 300 mandagar att genomföra, exklusive tid för förberedelser och efterarbete.

Genom kontrollen utvärderades vilka sårbarheter som finns och hur säkerhetsskyddet vid Högkvarteret behöver utvecklas och förstärkas. Mot bakgrund av detta så är detaljresultatet av kontrollen hemligt men likt alla andra förband finns behov av åtgärder för att säkerställa ett fullgott säkerhetsskydd. Kontrollen medför också i sig att säkerhetsmedvetandet och kompetensen ökar.

Utveckling av kontrollprocessen

Under 2008 har Säkerhetskontoret tillsammans med Insatsstabens Säksamsektioner genomfört en granskning av kontrollresultaten från samtliga genomförda säkerhetskontroller under åren 2006-2008. Syftet med arbetet har varit att finna eventuella generella och signifikanta brister och tendenser. Utvärderingen av kontrollprotokollen är inte en engångsföreteelse utan kommer fortsättningsvis vara ett årligen återkommande projekt. Resultaten kommer bland annat nyttjas till att inrikta kommande års kontroller, ligga till grund för säkerhetsskyddsåtgärder, prioritering av resurser inom säkerhetstjänsten med mera.

Under år 2008 har säkerhetskontoret och insatsstaben tillsammans genomfört 17 grundkontroller, sju uppföljningskontroller, ett omfattande säkerhetsskyddsbesök, två signalkontroller samt 32 särskilda signalskyddskontroller inom totalförsvaret. Genomsnittsomdömet har varit ett godtagbart resultat. Några verksamheter, som inte är av ringa betydelse, haft fått ett underkänt omdöme gällande sitt säkerhetsskydd. De allvarligaste bristerna har rört säkerhetsplanering, internkontrollverksamhet samt hur de lokala säkerhetsorganisationerna varit organiserade och utbildade. Brister har också konstaterats när det gäller säkerhetsskyddade upphandlingar och IT-säkerhet.

Inom verksamheten ledning av säkerhetstjänsten utgör de största bristerna avsaknad av säkerhetsanalyser och säkerhetsplaner. Likaså saknas påfallande ofta internkontrollplaner och internutbildningsplaner. På många verksamhetsställen är säkerhetsorganisationen också underdimensionerad. Det är vanligt förekommande att de viktigaste säkerhetsbefattningarna (säkerhetschef, IT-säkerhetschef och signalskyddschef) endera upprätthålls av en person eller är tillikabefattningar med befattningar inom andra huvudområden vilket ibland försvårat ett förebyggande säkerhetsskyddsarbete.

När det gäller kunskapen om aktuell säkerhetshotbild så är den högst varierande vid de kontrollerade verksamhetsställena. Rapporteringen brister överlag, såväl vad avser rapportering av skyddsvärd verksamhet och säkerhetsrapportering

som kontaktrapporter och underrättelserapporter.

Det råder stor aningslöshet när det gäller nyttjandet av teknisk apparatur såsom radioapparater, telefoner, datorer, handdatorer, digitalkameror och inte minst elektroniska lagringsmedia, främst USB-minnen. Dessutom avhandlas påfallande ofta sekretessbelagd information på öppna och okrypterade sambandsmedel, framförallt mobiltelefoni. Detta sker trots att förutsättningar ofta finns till krypterade samtal. Särskilda åtgärder vidtas därför under 2009 för att komma till rätta med dessa problem.

Inom området informationssäkerhet och IT-säkerhet har sekretessbelagda uppgifter funnits i öppna IT-system. Ofta har detta berott på låg tillgång på IT-system för bearbetning av hemlig information. Bristerna har också medfört att en del information inte informationssäkerhetsklassats på rätt sätt. Skyddet mot obehörig avlyssning i lokaler som är avsedda för informationsutbyte av information i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre klass är bristfälligt.

Inom delområdet tillträdesbegränsning är de största bristerna funna avseende nyckelhantering av fysiska nycklar där spårbarhet och historik ofta är otillräcklig.

Förvaring av vapen och ammunition samt hemliga handlingar är i huvudsak bra men kan fortsatt bli bättre. Rutiner för besökshantering behöver dock på många platser ses över.

När det gäller säkerhetsskyddad upphandling genom säkerhetsskyddsavtal har stora brister uppdagats, i första hand när det gäller den grundläggande säkerhetsanalys som skall avgöra om upphandlingen skall göras med säkerhetsskyddsavtal eller inte.

Inom många verksamhetsställen likställs säkerhetsprövning med registerkontroll. Alldeles för lite tid ägnas åt intervjuer, granskning av betyg/intyg samt referenstagning. Uppföljning av personal ur säkerhetssynpunkt varierar starkt mellan olika verksamhetsställen.

Genom den utvärdering och granskning av de senaste årens kontrollresultat som genomförts har ett antal övergripande och generella slutsatser kunnat dras. Utifrån detta kommer säkerhetskontoret vidta åtgärder för att förbättra säkerhetsskyddet inom Försvarsmakten samt vid de myndigheter som Försvarsmakten utövar tillsyn över. Några generella råd kan dock redan nu ges.

Samtliga chefer bör se över aktuell säkerhetsplanering samt utformningen av och kompetensen inom den egna säkerhetsorganisationen. Är säkerhetsorganisationen anpassad efter den verksamhet som bedrivs? Kan utsedd säkerhetspersonal avsätta tillräcklig tid för säkerhetsarbetet och har de relevant utbildning för uppgiften? Har säkerhetsorganisationen möjlighet att agera förebyggande och bedrivs ett systematisk internkontrollarbete?

Brister som framkommit och som beror på enskilda individers beteende kan enkelt åtgärdas. Som enskild bör man i förväg tänka över vad som kan avhandlas på öppna sambandsmedel och då sekretessbelagda uppgifter skall diskuteras endast använda sig av krypterade förbindelser. Detsamma gäller i våra IT-system. Hanteringen av digitala lagringsmedia såsom USB-minnen och liknande behöver avsevärt förbättras.

Avslutnings bör varje anställd tillse att i ökad utsträckning rapportera incidenter och vilken skyddsvärd verksamhet som bedrivs. Det är endast genom ett bra grundmaterial som rätt säkerhetsskyddsåtgärder kan vidtas.

Tigern lämnade Försvarsmakten

Till följd av andra världskrigets utbrott inrättades den så kallade tremannanämnden. Denna skulle fungera som ett statligt organ för informationsfrågor till följd av krigsutbrottet. Organisationen blev dock kortvarig. Redan ett knappt år senare ersattes tremannanämnden av Statens Informationsstyrelse (SIS). Uppgiften var dock fortsatt att bedriva informations- och opinionsarbete.

Ett år efter SIS bildande tillskrevs myndigheten av den ställföreträdande chefen för försvarsstaben. Det fanns ett behov av att få allmänhet och militär personal att iaktta försiktighet beträffande sitt sätt att hantera information och försvarsstaben önskade SIS hjälp med en informationskampanj. Under det följande halvåret arbetades formerna för en vaksamhetskampanj fram. Det var inom ramen för denna som journalisten, författaren och tecknaren Bertil Almqvist skapade verket En svensk tiger.

Vaksamhetskampanjen inleddes i november 1941. Sven Tunberg som var ordförande för SIS vid tiden höll ett radioanförande som avslutades med orden:

”Tig med vad du vet – tig med vad du inte vet – blir alltså vår menings dubbla paroll. Var på din vakt mot allt vad pratmakare heter. Hjälp inte spionen lösa pussel. Slå vakt om ditt land.”

Informationsgivningen drog nu igång på bred front. En svensk tiger som på ett enkelt och tydligt sätt sammanfattade essensen i kampanjen kom att pryda allt från prylar av olika slag till väggar i offentliga miljöer.

Strax efter krigsslutet lades SIS ner och behovet av vaksamhet var inte längre lika tydligt.

Under de efterföljande årtiondena kom ”En svensk tiger” att bli en symbol för den militära säkerhetstjänsten. Mot bakgrund av detta ansökte Försvarsmakten om att få verket registrerat som varumärke, vilket beviljades i oktober 1981.

I maj 2007 beslutade Svea Hovrätt att Försvarsmakten och den militära underrättelse- och säkerhetstjänsten, MUST, inte längre äger rätten att nyttja symbolen i sin verksamhet. Detta då Bertil Almqvist efterlevande några år tidigare hade överlåtit nyttjanderätten till Beredskapsmuseet i Helsingborg.

Under våren 2008 lämnades en stämningsansökan in gällande det belopp som Försvarsmakten skall erlägga för den tid man använt verket i sin verksamhet. Under sensommaren förlikades dock Försvarsmakten och Beredskapsmuseet och stämningsansökan togs tillbaka. Uppgörelsen innebar också att Försvarsmaktens nyttjande av verket En svensk tiger avslutats.

FÖRSVARSMAKTEN

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