Årsrapport säkerhetstjänst 2009

Militära underrättelse- och säkerhetstjänsten MUST

FÖRSVARSMAKTEN

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

Omslaget är tryckt på 270 gr Multiart Gloss och inlagan på 120 gr 4CC.

Grafisk form: FMLOG APSA, Grafiska ateljén, Stockholm.
Tryckeri: FMLOG, APSA, Grafisk Produktion, Stockholm

Förord

För åttonde året ger säkerhetskontoret vid den militära underrättelse- och säkerhetstjänsten ut en årsrapport. Syftet är att övergripande beskriva de säkerhetshot som riktas mot Försvarsmakten men också att till del beskriva den verksamhet som bedrivits under året. Genom att öppet beskriva aktuella säkerhetshot är förhoppningen att rapporten aktivt kan 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, förmågor och verksamheter tilldrar sig inte bara intressen från statsaktörer utan även från den organiserade brottsligheten och radikala grupper. De IT-relaterade hoten ökar i omfattning precis som antalet aktörer. Den tekniska utvecklingen är snabb och med den skapas nya sårbarheter.

Sveriges medverkan i internationell krishantering ställer 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 utvecklats ytterligare för att säkerställa att all personal är pålitlig och lojal ur säkerhetssynpunkt. Under året har också ett särskilt informations- och utbildningsprojekt genomförts i syfte att öka säkerhetsmedvetandet och förändra attityder bland Försvarsmaktens medarbetare.

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.

Säkerhetstjänsten måste alltid ha ett lärande arbetssätt. Genom öppenhet för ny kunskap, erfarenheter från kontrollverksamheten samt en kontinuerlig utvärdering av den egna verksamheten skapas möjligheter att utveckla arbetsformer och metoder. Därigenom skapas en smart och vass säkerhetstjänst med en god förmåga till proaktivitet.

Stockholm i juni 2010

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

Fotografer

Sida 7	Andreas Karlsson, FBB
Sida 13	Andreas Karlsson, FBB
Sida 14	Marco Nilsson, FBB
Sida 15	Ulf Fabiansson, FBB
Sida 17	Alexander Karlsson/FBB
Sida 18	Andreas Karlsson, FBB
Sida 19	Andreas Karlsson, FBB
Sida 21	Alexander Karlsson, FBB
Sida 22	Andreas Karlsson, FBB
Sida 23	Christian Lövgren, FBB
Sida 25	Johan Lundahl, FBB
Sida 26	Marco Olsson, FBB
Sida 29	Lennart Andersson, FBB
Sida 30	Fredrik Forsman, FBB
Sida 31	Torbjörn F Gustafsson, FBB
Sida 32	Håkan Brandt, FBB
Sida 33	Torgeir Haugaard, Norska försvarsdepartementet
Sida 34	Per körnefeldt, FBB

De personer som förekommer på bilderna har ingen koppling till innehållet i respektive artikel.

Innehållsförteckning

Årsrapport säkerhetstjänst 2009

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 kompromitterad. 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 Statens Inspektion för Försvarsunderrättelseverksamhet samt Försvarsunderrättelsesdomstolen. Dessa myndigheter har också en egen säkerhetsorganisation 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.

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. 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
FMTM/Säksamsektion Boden
Box 9101
961 19 Boden
Telefon: 0921-34 80 00 (vx)
Telefax: 0921-34 81 22

Säksam Stockholm
FMTM/Säksamsektion Stockholm
107 85 STOCKHOLM
Telefon: 08-788 75 00 (vx)
Telefax: 08-788 91 26

Säksam Göteborg
FMTM/Säksamsektion Göteborg
Box 5155
426 05 Västra Frölunda
Telefon: 031-69 20 00 (vx)
Telefax: 031-69 20 49

Säksam Malmö
FMTM/Säksamsektion Malmö
247 82 Södra Sandby
Telefon: 046-36 80 00
Telefax: 046-36 89 18

Rapportera alltid hot, incidenter och misstänkta händelser till din närmaste chef, säkerhetschefen eller direkt till säkerhetstjänsten. Även om en enskild händelse kan verka harmlös kan den i ett större perspektiv ha betydelse.

Dina rapporter ger viktig information om potentiella sårbarheter inom Försvarsmakten som kan utgöra ett hot mot våra skyddsvärda tillgångar och din personliga säkerhet. Informationen ger oss möjlighet att vidta motåtgärder.

Om du som enskild finner något som du tror kan vara av intresse för den militära säkerhetstjänsten så rapportera alltid. Vi tar hellre emot en rapport för mycket än en för lite.

Underrättelsehotet mot Försvarsmakten nationellt

I Sverige förekommer idag underrättelseinhämtning mot flera myndigheter. Försvarsmakten är inget undantag inte minst då förmågan att möta ett väpnat angrepp med naturlighet främst återfinns i Försvarsmakten. Främmande makt har ett intresse av att inhämta underrättelser avseende svensk operativ förmåga i både Östersjön och Nordkalotten, men också internationellt. Underrättelseinhämtningen syftar till att kunna göra bedömningar av Försvarsmaktens förmåga till förvarning och kapacitet att möta och avvisa kränkningar av olika slag. Svensk industri med kopplingar till försvarsrelaterade verksamheter är i vissa segment världsledande vilket också tilldrar sig intresse från främmande makt och konkurrerande företag.

Hotet från främmande underrättelseverksamhet riktar sig i första hand mot Försvarsmaktens kvalificerade vapensystem och operativa förmåga. Intresset riktar sig främst mot sjö- och luftstridskrafternas förmåga och verksamhet. Försvarsmaktens förband och verksamheter följs noggrant av andra stater bland annat genom försvarsattachéer och den information som publiceras på Försvarsmaktens hemsida. För att komma över sekretessbelagd information krävs dock vanligtvis ett insteg i organisationen

genom till exempel en insider eller en informationslämnare som inte förstår vem som är mottagare av informationen. Under de senaste åren har det förekommit underrättelseinhämtning riktad mot Försvarsmaktens personal genom så kallad 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.

Omfattningen av målsökning av personal och kontakttagning ligger kvar på ungefär samma nivå som 2008. Den information som eftersöks rör bland annat utveckling av svensk militärteknolog samt Försvarsmaktens operativa förmåga och ledningssystemutveckling. Tyvärr kan konstateras att många av Försvarsmaktens medarbetare är oförsiktiga med vilken information man publicerar om sig själv och sitt arbete i olika sociala nätverk på internet. Aningslösheten kan ge en underrättelseaktör möjligheten att skapa underlag för ett närmande. Ju mer kvalificerat närmandet är desto svårare är det att upptäcka för den som blir utsatt.

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 eftersöks. 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 andra gåvor.

Under år 2009 har Försvarsmakten deltagit i ett stort antal övningar med den typ av skyddsvärd materiel och förband som tilldrar sig ett intresse från främmande makt. Ett flertal ryska övningar och NATO-övningar har genomförts i vårt närområde varav Loyal Arrow hade en direkt påverkan på Försvarsmakten. I samband med den här typen av övningar finns normalt sett ett stort antal signalspaningsplattformar i luften, på havsytan och på marken som inhämtar underrättelser. Antalet aktörer som regelbundet signalspanar från luften i Sveriges närområde har under året ökat och ett offensivare uppträdande har kunnat konstateras. Huruvida detta beror

på relationen mellan Ryssland och NATO eller ländernas relation till Sverige är inte klarlagt men oavsett skäl så har det en direkt påverkan för försvarsindustrins prov- och försöksverksamhet. Under 2009 har förvarningssystemet fungerat väl och inga större informationsförluster har identifierats.

Även kriminella- och politiska grupperingar ägnar sig åt spaning och inhämtning av information rörande Försvarsmakten, både fysiskt och via internet. Under övningen Loyal Arrow upptäcktes flera fall av både rörlig och fast spaning. Syftet var sannolikt att kartlägga bevakningsrutiner. Också i samband med säkerhetsskyddade transporter har det förekommit att någon har övervakat verksamheten i anslutning till en anläggning.

Säkerhetshoten mot den svenska Afghanistanstyrkan

Under 2009 har säkerhetssituationen i Afghanistan försämrats. Den negativa utvecklingen har inte bara inneburit konsekvenser för civilbefolkningen utan också märkbart påverkat den svenska insatsen. Antalet attacker i det svenska ansvarsområdet har ökat och ändrats till sin karaktär. Vid ett flertal tillfällen har svenska och finska enheter hamnat i strid med väpnade afghanska grupper. Trupperna har utsatts för direktverkande eld i kombination med egenhändigt tillverkade laddningar av gamla granater, raketer och minor. Under slutet av året har även hemtillverkade sprängämnen börjat användas. Attackerna har genomförts i områden som ansetts vara osäkra och där det av olika skäl finns ett stort motstånd gentemot den internationella närvaron.

Underrättelseinhämtningen riktad mot det svenska truppbidraget i Mazar-e-Sharif har inte minskat under 2009. Snarare pekar trenden mot ett ökat underrättelsehot. Att antalet identifierade fall av underrättelseinhämtning blivit fler behöver dock inte till fullo ha sin grund i ett ökat hot utan kan också vara ett utslag av en förbättrad förmåga hos Försvarsmakten att identifiera och klarlägga säkerhetshotande verksamhet.

Under 2007 och 2008 kunde den militära säkerhetstjänsten fastställa att det bedrevs en aktiv underrättelseinhämtning inom och i anslutning till den svenska campen Northern Lights. Sedan dess har säkerhetsskyddsåtgärder vidtagits vilket förbättrat den interna säkerheten och reducerat möjligheterna för olika aktörer att bedriva underrättelseinhämtning inne på den svenska campen.

Redan tidigt fanns misstankar om att underrättelseinhämtningen inte bara hade kopplingar till lokala och regionala makthavare utan också till statsaktörer med intressen i Afghanistan. Under 2009 har denna bedömning kunnat beläggas. Flera statsaktörer bedriver traditionell underrättelseverksamhet via ambassader och konsulat men även genom företag och icke statliga organisationer. Bredden av underrättelseaktörer, dess skiftande agendor och lojaliteter är ett ständigt närvarande och påtagligt hot mot den svenska insatsen. Särskilt problematiskt är de fall där de afghanska säkerhetsstrukturerna har infiltrerats av det väpnade motståndet, kriminella aktörer eller statsaktörer.

Under året har svensk personals agerande vid flera tillfällen medfört risk för informationsförluster. Obetänksamhet, slarv och bristande förståelse för behovet av säkerhetsskyddsåtgärder medför att enskilda medarbetare agerar på ett felaktigt och sårbart sätt. Bland annat har handlingar förvarats och information delgivits på ett sådant sätt att det funnits en uppenbar risk att obehöriga, främst lokalanställda, har kunnat ta del av sekretessbelagd information.

Användandet av mobiltelefoni har fortsatt att öka, en utveckling som till viss del är problematisk. Då samtalen går via en lokal telefonoperatör finns inga möjligheter för Försvarsmakten att kontrollera vem eller vilka som kan tänkas ha tillgång till information om kommunikationen och dess innehåll Avlyssningsmöjligheterna är många så länge inte kommunikationen krypteras eller trafikskyddas. Även möjligheten att positionera mobiltelefoner gör det möjligt för en angripare att veta var de svenska förbanden befinner sig i förhållande till de basstationer som operatören har placerat ut. Det sistnämnda är särskilt allvarligt då det inte kan uteslutas att det väpnade motståndet eller andra aktörer därigenom kan få kännedom om rörelsemönstret för enskilda patruller.

Under slutet av året har anställda i utlandsstyrkan, och till dem närstående, utsatts för hot. Det är klarlagt att det finns en koppling mellan hoten och det svenska truppbidraget i Afghanistan, ett så kallat överfört hot. Även från andra länder finns exempel där soldater och anhöriga utsatts för hot till följd utav insatsen i Afghanistan. Sårbarheten är framförallt kopplad till den enskildes användande av privata kommunikationsmedel främst mobiltelefoner och sociala nätverk på internet. Under 2010 kommer detta särskilt att följas upp inom ramen för operationssäkerhet och guidelines i syfte att minska riskerna vid användning av social medier kommer att tas fram.

Signalspanings- och cyberhotet

Signalspaning har traditionellt sett främst genomförts av statsaktörer då verksamheten krävt stora ekonomiska resurser och ett omfattande teknisk kunnande. Den tekniska utvecklingen har dock inneburit förändringar. Idag finns ett större utbud av produkter för avlyssning med ett format och pris som gör det möjligt för fler aktörer att bedriva signalspaning. Exempel på detta är utrustning för avlyssning av mobil kommunikation.

Risken för avlyssning är ett ständigt närvarande hot vid Försvarsmaktens internationella insatser men även här hemma. I Sveriges närområde har alla stater någon form av kvalificerade signalspaningssystem för kommunikationsspaning och teknisk spaning. Den kan bestå i egen utrustning eller gemensam utrustning inom ramen för en internationell organisation som till exempel NATO. Stationära signalspaningsplattformar på marken såväl som rörliga plattformar i luften och på havsytan används för att inhämta signalunderrättelser.

Signalspaning är ofta mycket svårt att upptäcka eftersom den i så stor utsträckning sker passivt. Det är framförallt frekvenser för alla typer av radiokommunikation som avlyssnas. För att kunna avslyssna telefoni som går över tråd måste en angripare ha fysisk access till aktuell

nätstruktur. Mobiltelefoni är mer sårbart för avlyssning då mängden gränssnitt där avlyssning kan ske, mellan den som ringer och den som är mottagare, är stor. Ofta vet användaren inte hur samtalet kopplas eller vem som kan läsa trafiken. Detsamma gäller för internetuppkopplingar.

De IT-relaterade hoten har under 2009 fortsatt att växa. Antalet aktörer bedöms också ha ökat. I huvudsak kan aktörerna delas in i fyra grupper. Statsaktörer som avdelar stora resurser för datornätverksoperationer (CNO), icke statliga aktörer som utvecklat förmågan inom ramen för terrorism samt så kallade ”hackers” som genom sitt agerande på nätet utgör ett hot mot samhället och därmed även mot Försvarsmakten. Kriminella grupperingar har insett att det går att tjäna pengar genom att stjäla personinformation, konton, lösenord med mera som sedan kan användas i utpressningssyfte eller för bedrägerier.

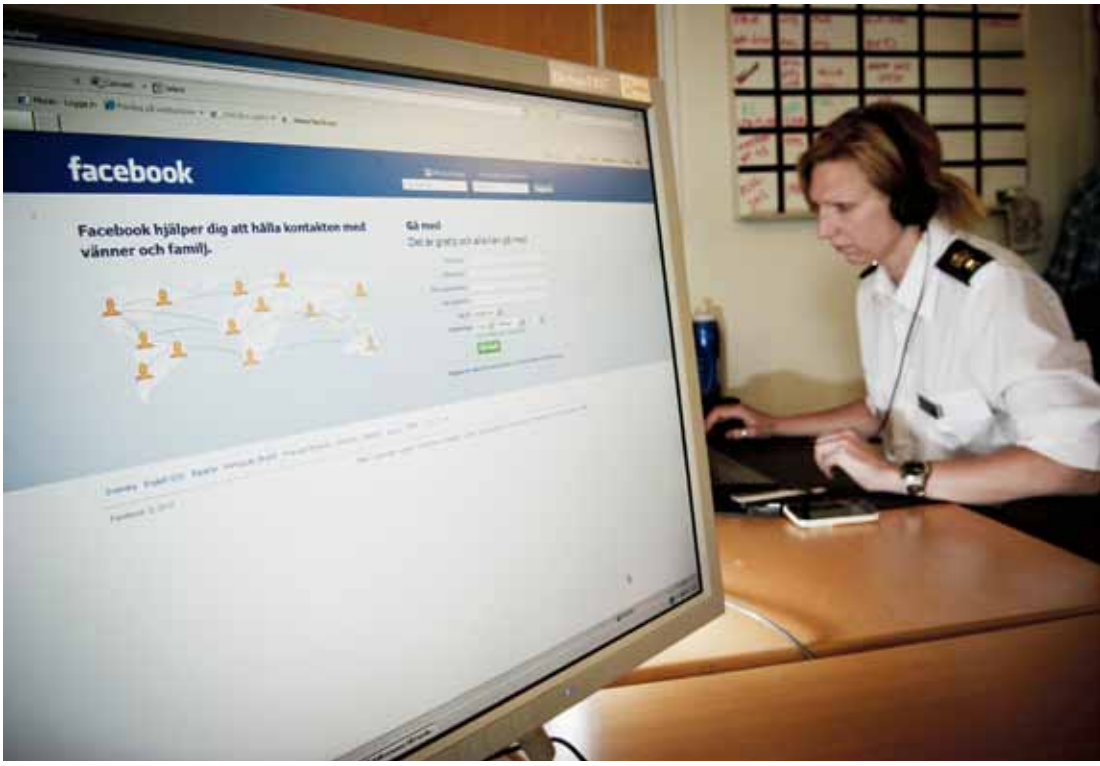
Det enskilt största hotet inom cyberområdet riktat mot Försvarsmakten är främmande makts underrättelseinhämtning via dator- och nätverksintrång. Indikationer under året visar att flera främmande underrättelsetjänster lägger ner stora resurser och bedriver en omfattande verksamhet inom detta område. Resurserna består bland annat av tekniska, språkliga och analytiska kompetenser.

Under senare år har flera IT-angrepp riktats mot myndigheter i Sverige men även mot hela nationer. Estland utsattes i samband med den uppmärksammade flytten av en bronsstaty och Georgien vid tiden för kriget med Ryssland. I båda

fallen användes datornätverksoperationer i form av överbelastningsattacker (DDoS) för att bland annat stänga ner alla offentliga hemsidor. I Estlands fall innebar attacken också att all internettrafik in och ut ur landet helt stängdes ner under ett par dygn.

Under 2009 har Försvarsmakten varit utsatt för ett stort antal angrepp via skadlig kod, både nationellt och internationellt. Incidenterna har analyserats för att kunna klarlägga hur den skadliga koden har tagit sig in i systemet, vad den har gjort och hur den fungerar. Syftet med analysen har varit att kunna vidta ytterligare åtgärder för att förbättra säkerhetskyddet. Försvarsmakten har i grunden ett bra skydd eftersom IT-arkitekturen är frikopplad från internet. I de internationella insatserna finns dock epost- och kommunikationslösningar som är känsligare för störningar. Vanligast är att skadlig kod kommer in i Försvarsmaktens system via e-post eller bärbara lagringsmedia som till exempel USB-minnen, CD-skivor etcetera. Den skadliga koden utgörs främst av trojaner som försöker skapa en förbindelse mellan aktuella dator och en internetansluten dator utanför Försvarsmakten. Syftet är att därigenom kunna fjärrstyra just den klient som har smittas och därefter sprida sig vidare inom det nätverk som datorn är ansluten till. Försvarsmakter i andra länder som inte haft en lika tydlig separering av system har visat sig mer sårbara och drabbats hårdare av attacker via skadlig kod.

Underrättelseinhämtning och informationsförluster i sociala nätverk



De sociala nätverken på internet har under de senaste åren vuxit kraftigt. De kan beskrivas som användardrivna tjänster som kopplar ihop information om personer på ett spontant och interaktivt sätt. De är oftast webbaserade och innehåller funktioner som låter personer publicera information som kan ses av andra och som andra kan knyta an till, till exempel genom att kommentera publicerad information. Men samtidigt som de sociala nätverken har skapat nya möjligheter för mänsklig kommunikation har de också blivit en arena för underrättelseinhämtning och kriminalitet.

Sociala nätverk ger underrättelseaktörer nya möjligheter att direkt kontakta de personer som är intressanta ur underrättelsesynpunkt. Exempel på detta är de närmanden och försök till underrättelseinhämtning som riktats mot enskilda medarbetare vid det svenska truppbidraget i Afghanistan. Dessa har via Facebook kontaktats av för dem okända personer. Inledningsvis har de fått frågor av alldaglig karaktär varefter frågorna övergått till att specifikt kretsa kring uppdraget i Afghanistan. Den här typen av kontakttagning kan syfta till att inhämta aktuell information men kan också vara ett led i en underrättelseaktörs långsiktiga arbete

riktat mot personer som bedöms vara intressanta.

Medarbetares behov av att kommunicera med anhöriga och vänner samt beskriva sitt arbete riskerar att sekretessbelagda uppgifter oavsiktligt röjs. Information om planerade insatser och förbandets förmåga (eller brister i förmågan) att genomföra dessa är normalt sekretessbelagt om motståndaren får fördelar av informationen. I andra fall kan det dock vara svårare för den enskilde att urskilja vad som kan vara sekretessbelagt och därmed inte får publiceras. Det finns också exempel på att ovana att hantera oväntade händelser leder till att sekretessbelagda uppgifter röjs. Massmedias behov av snabb information kan leda till att Försvarsmakten publicerar information utan att först göra en tillräcklig sekretessbedömning. Till exempel kan bilder efter attentat mot fordon ge upplysningar om fordonens skydd vilket sedan ligger till grund för motståndarens taktikanpassning.

Information publicerad på ett socialt nätverk, i massmedia eller genom Försvarsmaktens informationstjänst behöver dock inte vara sekretessbelagd för att en underrättelseaktör skall kunna dra nytta av den. Texter och bilder som beskriver vår förmåga och utrustning kan verka harmlös men kan vara den enda källa som motståndaren inledningsvis har. Genom informationen underlättas också fortsatt underrättelseinhämtning och ger möjligheter att bedöma vår förmåga.

En underrättelseaktör kan från sociala nätverk inhämta information om en persons preferenser i form av intressen med

mera. Informationen ger underlag för och kan underlätta ett fortsatt närmande via sociala nätverk eller genom direktkontakt med aktuell person. Det är enkelt för en underrättelseaktör att skapa en digital personakt genom att löpande automatiskt ladda ner och spara den personliga information som den enskilde delar med sig av på sociala nätverk. Att i efterhand radera eller ändra utlagd information är därför inte tillräckligt eftersom materialet redan kan ha sparats för senare bearbetning, bedömning och användning.

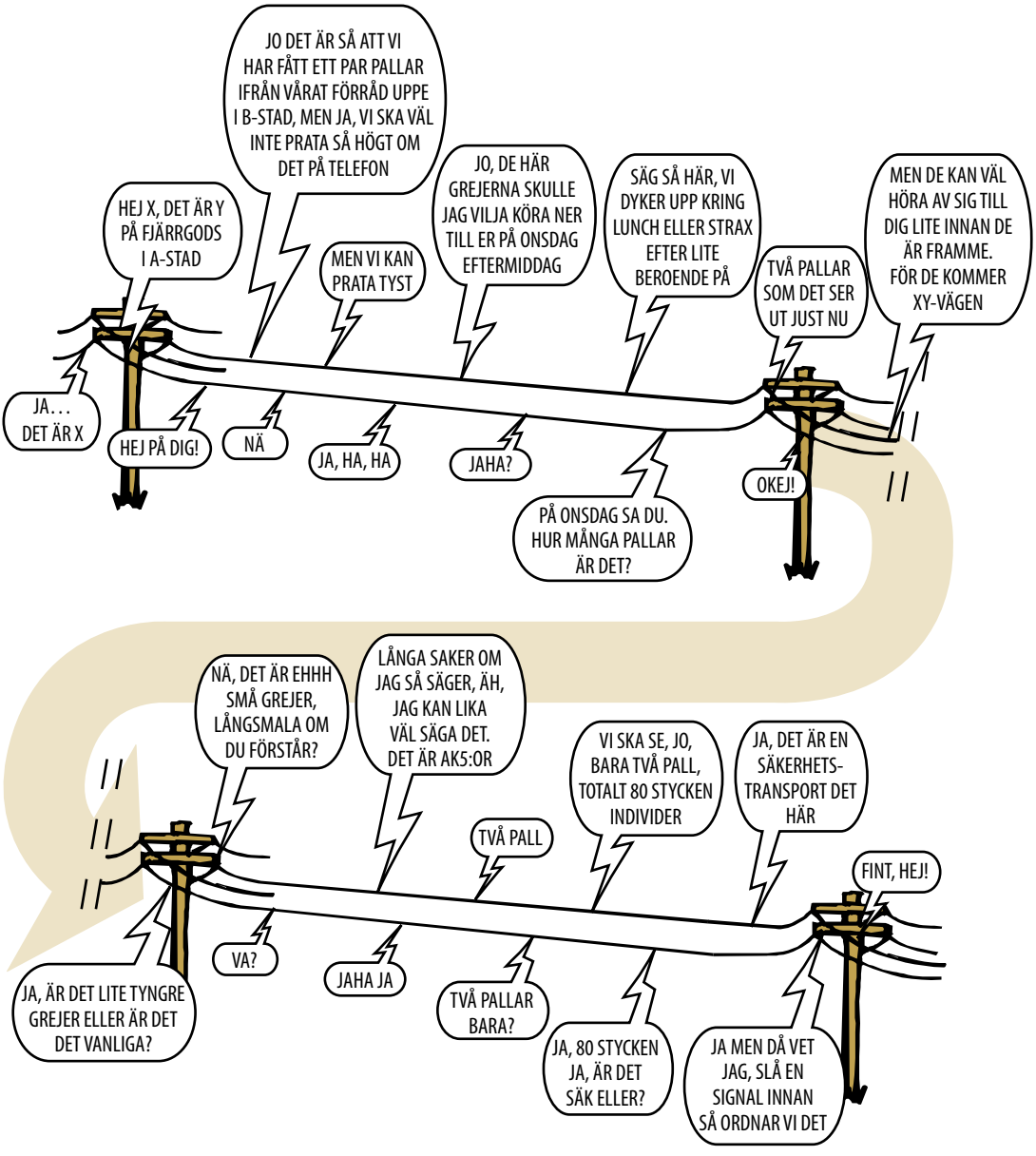
De medarbetare som i sin tjänst hanterar sekretessbelagda uppgifter kan för en underrättelseaktör vara extra intressanta att kartlägga. Förutom information om individen och dennes arbetsuppgifter kan hans eller hennes kopplingar till andra medarbetare i Försvarsmakten vara värdefull information. Genom den sistnämnda kan en underrättelseaktör utröna vilka som är informationsbärare av specifik sekretessbelagd information som aktören eftersöker.

Personlig information publicerad på sociala nätverk kan i vissa fall även uppfattas som pinsam eller skadlig för en individ om informationen når utanför den krets av personer som informationen var avsedd för. Personlig information, som av andra kan uppfattas stötande, skulle i värsta fall kunna användas av en underrättelseaktör i utpressningssyfte eller för att misskreditera en person.

Många är delaktiga i flera olika sociala nätverk men väljer att inte framträda med sin fullständiga identitet i alla dessa. Personlig information om en individ på anonyma sociala nätverk kan ibland sammankopplas med personlig information på sociala nätverk där personen är identifierbar. Genom att jämföra texter och bilder på olika sociala nätverk skulle en underrättelseaktör kunna sluta sig till vilken person som ligger bakom ett alias på ett anonymt socialt nätverk.

Vissa digitalkameror förser bilder med serienumret på digitalkameran vilket innebär att jämförande studier av olika sociala nätverk kan automatiseras. Det finns också forskning som visar att varje digitalkamera ger digitala bilder unika fingeravtryck och att detta kan användas för att visa vilka bilder som har tagits med en viss digitalkamera.

Den ökade användningen av sociala nätverk medför sålunda nya sårbarheter, både för den enskilde medarbetaren som för Försvarsmakten. Under året har därför en omfattande utbildnings- och informationsinsats genomförts i syfte att öka medvetenheten om riskerna med att publicera personlig information samt uppgifter om sitt arbete på internet. Ett arbete har också inletts för att ta fram övergripande guidelines för den enskilde medarbetarens användning av sociala nätverk.


JO DET ÄR SÅ ATT VI HAR FÅTT ETT PAR PALLAR IFRÅN VÅRAT FÖRRÅD UPPE I B-STAD, MEN JA, VI SKA VÄL INTE PRATA SÅ HÖGT OM DET PÅ TELEFON
HEJ X, DET ÄR Y PÅ FJÄRRGODS I A-STAD
MEN VI KAN PRATA TYST
JO, DE HÄR GREJERNA SKULLE JAG VILJA KÖRA NER TILL ER PÅ ONSDAG EFTERMIDDAG
SÄG SÅ HÄR, VI DYKER UPP KRING LUNCH ELLER STRAX EFTER LITE BEROENDE PÅ
TVÅ PALLAR SOM DET SER UT JUST NU
MEN DE KAN VÄL HÖRA AV SIG TILL DIG LITE INNAN DE ÄR FRAMME. FÖR DE KOMMER XY-VÄGEN
JA… DET ÄR X
HEJ PÅ DIG!
NÄ
JA, HA, HA
JAHA?
PÅ ONSDAG SA DU. HUR MÅNGA PALLAR ÄR DET?
OKEJ!
NÄ, DET ÄR EHHH SMÅ GREJER, LÅNGSMALA OM DU FÖRSTÅR?
LÅNGA SAKER OM JAG SÅ SÄGER, ÄH, JAG KAN LIKA VÄL SÄGA DET. DET ÄR AK5:OR
VI SKA SE, JO, BARA TVÅ PALL, TOTALT 80 STYCKEN INDIVIDER
JA, DET ÄR EN SÄKERHETS-TRANSPORT DET HÄR
TVÅ PALL
FINT, HEJ!
VA?
JAHA JA
TVÅ PALLAR BARA?
JA, 80 STYCKEN JA, ÄR DET SÄK ELLER?
JA MEN DÅ VET JAG, SLÅ EN SIGNAL INNAN SÅ ORDNAR VI DET
JA, ÄR DET LITE TYNGRE GREJER ELLER ÄR DET DET VANLIGA?

Kampanj Ekeby 2.0

Samtalet på föregående sida baseras på en verklig händelse. På en öppen (vanlig) telefonlinje planeras och diskuteras en skyddad transport. Trots att samtalet inte är krypterat avslöjas i detalj vilken typ av vapen som skall fraktas, färdvägen och ungefärlig tidpunkt för transporten. Ett agerande som är förenat med stora risker.

Försvarsmaktens vapen är eftertraktade i kriminella kretsar och bristande säkerhetsmedvetande skapar sårbarheter. Öppna sambandsmedel kan med enkla medel avlyssnas i syfte att kartlägga transporter av skyddsvärd materiel. Om vapen, ammunition och sprängmedel hamnar i orätta händer kan det få långtgående konsekvenser.

Under 2000-talet har antalet förlustanmälda vapen inom Försvarsmakten stadigt fortsatt att minska. Att helt undvika förluster är dock inte möjligt och ett högt säkerhetsmedvetande hos personalen är en förutsättning för att minimera risken för att vapen förkommer. I det aktuella fallet brast medarbetarna i sitt säkerhetsmedvetande. En kriminell grupp kunde ha avlyssnat samtalet och därefter försökt tillskansa sig vapnen vid ett rån. Ett rån som om det hade lyckats kunde inneburit direkt livsfara för chauffören vid råntillfället men även för tredje person den dag

de stulna vapnen hade använts i kriminell verksamhet.

Det aktuella telefonsamtalet är dessvärre inte unikt. Den kontrollverksamhet som den militära säkerhetstjänsten bedriver visar att säkerhetsmedvetandet och signaldisciplinen gradvis har försämrats bland Försvarsmaktens anställda.

Den tekniska utrustning som Försvarsmakten förfogar över för att kryptera samtal och därigenom göra dem avlyssningssäkra används i för liten utsträckning samtidigt som mobiltelefoni blir ett allt mer vanligt förekommande kommunikationsmedel, både vid övningar såväl som vid skarp verksamhet. Även om det är svårare att avlyssna en mobiltelefon än en fast telefonförbindelse är mobiltelefoni inte på något sätt en säker kommunikationsform. Att kommunicera hemliga eller känsliga uppgifter via sin mobiltelefon innebär en uppenbar risk för informationsförluster.

Under det kalla krigets dagar fanns en gedigen kunskap om hotet från främmande underrättelsetjänst samt de övriga säkerhetshot som riktades mot Försvarsmakten. I takt med att världen har förändrats har tyvärr också säkerhetsmedvetandet kommit att minska.

Det blir allt vanligare att personal i utlandsstyrkan beskriver sin vardag och sitt arbete genom att publicera texter och bilder på olika internetforum som till exempel Facebook, Bilddagboken och bloggar. Även om varje foto eller text i sig själv inte röjer några sekretessbelagda uppgifter kan helheten bidra till kart-

läggning. De bilder som läggs ut kan sammantaget ge en motståndare en god överblick av hur våra camper är uppbyggda, vilka rutiner vi har och hur vi verkar. Därigenom kan en angripare skapa sig en uppfattning av våra eventuella sårbarheter och hur dessa kan utnyttjas om man vill skada det svenska truppbidraget.

Den moderna informationsteknologin ger fantastiska möjligheter att förenkla och effektivisera arbetet men innebär också nya sårbarheter. Att ha god ordning på sina hemliga handlingar är en självklarhet för Försvarsmaktens anställda samtidigt som en del medarbetare lagrar stora mängder information på digitala lagringsmedia och då framför allt USB-minnen. I föregående årsrapport beskrevs bland annat konsekvenserna av att en Försvarsmaktsanställd glömde kvar ett USB-minne på biblioteket vid Stockholms Universitet. USB-minnet innehöll sekretessbelagda uppgifter som personen i fråga använt inom ramen för sin tjänstgöring i Afghanistan och sedan tagit med sig hem på sitt USB-minne. Då en av de sekretessbelagda handlingarna som fanns på USB-minnet var upprättad av en annan nation kom ärendet också att påverka Försvarsmaktens anseende i ett internationell perspektiv.

Den enskildes beteende och agerande kan mot bakgrund av de exempel som beskrivit ha en stor betydelse även för Försvarsmakten och i sin förlängning relationen till annan stat eller mellanfolklig organisation. Det fanns därför ett stort behov av att förändra attityden till säkerhetstjänst, öka säkerhetsmedvetandet för att därigenom kunna förändra medarbetarnas beteenden.

Under hösten 2008 drogs därför riktlinjerna upp för en kampanj riktad till Försvarsmaktens anställda. Inledningsvis var huvudsyftet att genom informations- och utbildningsinsatser förbättra signaldisciplinen i Försvarsmakten. Under planeringsarbetet stod det allt mer klart att det fanns ett behov av ett bredare anslag. Kampanjen kom därför också att få till syfte att informera om säkerhetshoten och vilka konsekvenser de har för den enskilde medarbetarens vardag såväl som för Försvarsmaktens verksamheter.

Kampanjen gavs namnet Ekeby 2.0 efter en välkänd instruktionsfilm från kalla krigets dagar. Även om mycket hänt sedan dess är filmen relevant även i våra dagar då hotet från signalspaning och övrig underrättelseverksamhet alltjämt består.

Ett särskilt utbildningsmaterial producerades och föreläsningar planerades in vid Försvarsmaktens olika verksamhetsställen. Under tolv intensiva veckor turnerade säkerhetskontorets operative ledare runt i landet för att möta Försvarsmaktens personal. Allt ifrån mekaniker vid verkstäder till regementschefer. Sammantaget genomfördes inte mindre än 70 aktiviteter med sammanlagt omkring 7.500 deltagare.

Att förändra attityder tar lång tid och rundresan kommer att följas upp med ytterligare informations- och utbildningsinsatser under 2010 och 2011. Redan hösten 2009 kunde dock effekter skönjas. Vid signalkontroller i samband med övningsverksamhet noterades en förbättrad signaldisciplin vilket därmed inneburit att riskerna för informationsförluster kunnat minskas.

Säkerhetsskyddsavtal mellan Sverige och andra länder

Till den militära säkerhetstjänstens uppgifter hör att förhandla fram internationella säkerhetsskyddsavtal. Förhandlingarna sker på uppdrag av regeringen och syftet med avtalen är att möjliggöra utbyte av hemliga uppgifter mellan Sverige och andra länder. Behovet av att utbyta hemliga uppgifter kan till exempel ha sin grund i ett gemensamt försvarsmaterielprojekt, svenska exportsatsningar med mera. Även i samband med militärt samarbete såsom Nordic Battle Group finns behov av säkerhetsskyddsavtal.

Under 2009 undertecknade Sverige säkerhetsskyddsavtal med Sydkorea och Singapore. Avtalet med Sydkorea tecknades i Stockholm i samband det sydkoreanska statsbesöket i juli medan avtalet med Singapore signerades under hösten. Genom avtalen skapas möjligheter för ett utökat samarbete mellan länderna inom försvarsindustri och säkerhetsforskning.

Under året har även avtal förhandlats med ett flertal andra länder och under 2010 beräknas några säkerhetsskyddsavtal att undertecknas. Avtal har under början av 2010 ingåtts med de nordiska länderna.

Avtalen utgör en rättsligt bindande brygga mellan Sveriges och andra länders säkerhetslagstiftning och innehåller vanligtvis bestämmelser om informationssäkerhetsklassning, ömsesidigt skydd av hemliga uppgifter, rutiner för överföring av hemliga uppgifter, besöksrutiner samt bestämmelser om gemensam samverkan vid händelse av röjda uppgifter. Med avtalen som grund kan säkerhetsrutiner utvecklas som säkerställer att uppgifter som utbyts eller gemensamt tas fram inom samarbeten och projekt ges ett ändamålsenligt och likartat säkerhetsskydd.

I utbytet av hemliga uppgifter med andra länder och internationella organisationer förekommer det att hemliga uppgifter röjs eller förloras. Informationsförluster av denna typ kan påverka Sveriges utlandsförbindelser och Sveriges trovärdighet i internationella sammanhang. För att minska risken för detta skall upprättaren av information som kan ha förlorats eller blivit röjd omgående informeras så snart misstanke finns om informationsförlust. Informationen skall skyndsamt lämnas även om inte ärendet har utretts klart för att undvika att störa relationen med upprättaren ytterligare. I Försvarsmakten ansvarar den militära säkerhetstjänsten för vidare kontakter med det berörda landets nationella säkerhetsmyndighet. Genom samverkan vidtas åtgärder för att utreda det inträffade och för att minska skadan av ett röjande.

Egna noteringar