Ert tjänsteställe, handläggare | Ert datum | Er beteckning

Vårt tjänsteställe, handläggare | Vårt föregående datum | Vår föregående beteckning

Fredrik Plantin, fredrik.plantin@mil.se

Södra militärregionens säkerhetshotsbeskrivning 2018

Svar före

Härmed utsänds den öppna säkerhetshotbeskrivningen för Södra Militärregion (MR S) 2018. Den är ett stöd vid säkerhetsplanering och som utbildningsmaterial för respektive förband/organisationsenhet. Eventuella förändringar i säkerhetshotbilden utsänds genom särskild skrivelse.

Säkerhetshotbeskrivning är en öppen sammanställning av egna och externas öppna underlag och rapporter. Säkerhetshotbeskrivningen har förband/organisationsenheter inom MR S område som huvudmottagare och delges övriga som orientering. Säkerhetshotbeskrivning ska delges samtlig personal inom respektive organisation.

Stycken i skrivelsen som väsentligt förändrats markeras med ett lodrätt streck i högermarginalelen, se högermarginal.

Skrivelsen fastställs att gälla fr.o.m. 2018-09-27, MR S tidigare utgåvor upphävs härmed.

Referenser.

- MUST Årsöversikt 2018
- Säkerhetspolisens årsbok 2017
- NCT Helårsbedömning 2018
- MSB Informationssäkerhet Trender 2015
- Försvarsmaktens Folder Terrorhot 2013
- EUROPOL Changes in modus operandi of IS 2016
- EUROPOL Terror and trend report 2016
- National security threat assessment LITHUANIA 2016
- The Crimea Operation. FOI, Totalförsvarets forskningsinstitut,
- Kampen om sannheten. Forsvarets forskningsinstitutt, 2014. Norge

Innehåll

1. Sammanfattning

Flertalet nationer[1] bedriver underrättelseverksamhet i och mot Sverige, främmande underrättelseverksamhet som bedrivs i Sverige är omfattande och kartlägger företrädare för Sverige och Försvarsmaktens verksamhet. Utländska underrättelseofficerare som är stationerade i Sverige under diplomatiska täckbefattningar kartlägger såväl Försvarsmaktens som civila samhällsviktiga funktioner inom ramen för totalförsvaret. Det förekommer regelbundet att personer följer och på olika sätt dokumenterar Försvarsmaktens verksamhet.

Dessa nationer har ett intresse för vår militära verksamhet såsom operativ förmåga, vilken kapacitet vi har att möta kränkningar av olika slag, våra teknologiska lösningar samt utveckling och materielförsök. Sverige är ett framstående land inom innovationer och hög-teknologi. Detta gäller bland annat utvecklingen av vapen och stödsystem vilket medför att företag, skolor och andra myndigheter inte är undantagna från inhämtningsförsök av främmande underrättelsetjänster[2]. Personal inom Försvarsmakten och viktiga samhällsfunktioner på så kallade nyckelbefattningar (informationsbärare), inklusive sådana som kan förutspås en framtida karriär, kan tilldra sig intresse för rekrytering eller tjänstgöra som aningslösa uppgiftslämnare. Därav är information och utbildning av personal vid förband/enheter en nödvändighet, speciellt vid samverkan, samövning och besöksverksamhet med andra nationer.

Underrättelseinhämtning är i de flesta fall även en förutsättning för att kunna bedriva kriminalitet. Före angrepp mot ett objekt bedöms kartläggning ske för att ge information om larm, låstyper, säkerhetsskyddsanordningar, våra bevaknings-, insats- och patrulleringsrutiner, förekomst av hundar, provkörning av flyktvägar m.m. Utifrån tillgänglig statistik över inträffade säkerhetsrelaterade händelser 2017, är bedömningen att ett fortsatt intresse från kriminella och kriminella organisationer kvarstår under året 2018. Omfattningen av den kriminella verksamheten tar sig uttryck inom ett flertal olika områden såsom stölder av kapitalvaror som lätt kan omsättas i pengar, drivmedel, angrepp på ammunitions- och mobiliseringsförråd, ekonomiska brott både externa och interna, försök till och stöld av vapen och ammunition i bruk.

För Försvarsmaktens personal förståelse och efterlevnad av aktuella säkerhetsskyddsbestämmelser tillsammans med uppmärksamhet och misstänksamhet är av största vikt för att försvåra kriminella organisationers eventuella angrepp mot våra objekt och vår verksamhet. Identifiering av skyddsvärden inom egen verksamhet är en avgörande faktor för att kunna bedöma relevant säkerhetshotbild.

[1] Säkerhetspolisens årsbok 2017
[2] MUST Årsöversikt 2017

Vidmakthållande och utveckling av övningar under 2018, prov och försök samt annan skyddsvärd verksamhet bedöms vara av speciellt intresse för främmande och kriminell underrättelseinhämtning. Risk för infiltration är påtaglig i de fall där Försvarsmakten i anspråktar personer i organisationen som har kopplingar till kriminella nätverk. Detta kan ske både genom att personer i dessa kretsar söker tjänster, kallas in för utbildning eller ansöker om att bli hemvärnsmän i Försvarsmakten. Innan ny personal anställs eller kontrakteras ska säkerhetsprövning genomföras och utbildning genomföras i säkerhetstjänst med syfte att kontinuerligt upprätthålla ett bra infiltrationsskydd.

Säkerhetsprövningen och i synnerhet säkerhetsprövningsintervjuen ska inte forceras utan utgör ett av FM viktigaste verktyg för en bra och säker rekrytering.

Sverige kommer sannolikt att betraktas som ett legitimt mål för våldsfrämjande religiösa extremistiska aktörer såväl i Sverige som utomlands. Det finns ett fåtal aktörer som troligen både kommer ha intention och kapacitet att genomföra våldshandlingar som kan rubriceras som terrorattentat i Sverige. Bland dessa finns dels de som rest och återvänt efter att ha stridit med våldsfrämjande religiösa grupperingar, dels individer som inte rest, men som inspirerats av våldfrämjande religiöst extremistisk propaganda.

Med terrorattentat avses exempelvis attentat mot utpekade personer eller grupper, begränsade sprängattentat mot allmänheten eller påverkan på delar av kritisk infrastruktur. Daesh[3] kommer sannolikt att vara den främsta inspiratören för våldsfrämjande religiösa extremister i Sverige under 2018. Flera andra europeiska länder är utpekade mål för Daesh och gruppen prioriterar troligen vissa stater före Sverige vid styrd attentatsplanering[4]. Hot i form av terrorism mot Sverige och Försvarsmakten följer Säkerhetspolisens nationella bedömning. Händelser som inträffat under 2016-2017 i Europa understryker allvaret och bekräftar att även Sverige kan utsättas för allvarliga händelser.

Hot mot Försvarsmaktens informations- och ledningssystem föreligger alltjämt. Den enskilt viktigaste säkerhetshöjande åtgärden är att informera och utbilda samtlig personal om rutiner, organisation/ansvar och hotbild rörande myndighetens informationssystem samt ge kunskap om metoder för att minimera riskerna vid olika typer av säkerhetshot.

En bedömning måste göras av vilka verksamheter som kräver redundans och reservfunktioner. Åtgärder som kan införas med kort varsel kan inkludera följande:

[3] Daesh ± al-Dawla al-Islamiyya fi al-Iraq wa al-Sham. Daesh benämns även Islamiska staten i Irak och Levanten/Syrien (Isil/ Isis).

[4] NCT Helårsbedömning 2017

- Revidering av den egna säkerhetsorganisationen.
- Sektionering av enheter/avdelningar.
- Höjning av säkerhetsnivån i passersystem genom införande av både kort- och kodsystem, till exempel vid entréer.
- Byte av lösenord för IT-system. Kräv svårare lösenord och kortare giltighetstid.
- Granskning och uppföljning av loggning till IT och passersystem.
- Behov av och revidering av befintliga bevakningsplaner och larmfunktioner.

Organisationsenheter bör planera och i valda delar förbereda för möjligheten till en hastigt förändrad hotnivå.

2. Hotområden

2.1. Analyser, planer och kontroller

Som grund för säkerhetsarbetet ligger verksamhets- och säkerhetsanalyser. Analyserna skall visa vilka skyddsvärden som finns inom verksamheten samt bedömning av vilka hot som finns mot det skyddsvärda. Analysarbetet berör inte enbart säkerhetspersonal utan bör involvera personal från respektive verksamhet. Analyserna skall utmynna i säkerhetsplaner och bestämmelser. Regelbundna kontroller syftar till att klarlägga säkerhetsläget samt att initiera åtgärder för att avhjälpa brister.

Upprättade SUA-avtal bör regelbundet följas upp avseende efterlevnaden av ingånget avtal och det är verksamhetsägarens ansvar det vill säga förbandschefens ansvar.

Förbandschefers ansvarar att kontrollera att SUA finns och att det följs på den outsourcade verksamheten som bedrivs på, i och invid eller på annat sätt har samröre med den egna verksamheten.

2.2. Säkerhetshotande verksamhet inom Militärregion Syd

Säkerhetshotande verksamhet mot Försvarsmaktens skyddsvärden indelas i:

- Främmande underrättelseverksamhet.
- Terrorism.
- Sabotage.
- Subversion.
- Kriminalitet.

Den säkerhetshotande verksamhet som bedöms vara aktuell inom MR S ansvarsområde utgörs i första hand av följande områden:

- Främmande underrättelseverksamhet.
- Kriminalitet.
- Subversion (infiltration och propaganda).

Hot mot våra informations- och ledningssystem kan utföras av såväl inre som yttre aktörer.

Hot mot informationssystem skall bedömas inom följande områden:

- Fysiska hot som påverkar hårdvara (skadegörelse, tillgrepp, miljö).
- Logiska hot (virus, obehörig access).
- Administrativa hot (bristande utbildningstillstånd, behörighetsadministration).

Härutöver utgör framförallt terrorhot ett område som måste beaktas, eftersom hotnivån snabbt kan förändras samt kan komma att kräva viss uthållighet.

OrgE bör identifiera och klarlägga de säkerhetsskyddsbrister som kan förväntas uppstå vid en förändrad hotbild inom terrorismen mest troliga/möjliga normerande modus operandi i syfte att minska insatstiden för säkerhetsskyddsinsatser och att skapa uthållighet.

2.3. Säkerhetshotbeskrivning

2.3.1. Hotnivåer

5	MYCKET HÖGT HOT	Incidenter inträffar mer eller mindre dagligen. Aktören bedöms genomföra verksamheten till varje pris utan hänsyn till konsekvenser för den egna säkerheten . Ogynsamma miljö - och /eller sociala faktorer finns och har mycket stor uppdragshotande inverkan.
4	HÖGT HOT	Info som tyder på hög kapacitet, intention och tillfälle hos potentiell aktör Incidenter har inträffat vid ett flertal tillfällen i närtid Ogynsamma miljö - och / eller sociala faktorer finns och har stor och möjligen uppdragshotande inverkan
3	FÖRHÖJT HOT	Info som tyder på reell kapacitet, intention och tillfälle hos potentiell aktör Enstaka incidenter har inträffat. Ogynsamma miljö - och /eller sociala faktorer finns och har stor men inte uppdragshotande inverkan
2	LÅGT HOT	Info som tyder på begränsad kapacitet, intention och tillfälle hos potentiell aktör Inga incidenter har förekommit i närtid. Ogynsamma miljö - och /eller sociala faktorer finns men har låg inverkan.
1	ICKE IDENTIFIERAT HOT	Ingen info som tyder på kapacitet, intention och tillfälle hos potentiell aktör Inga incidenter har förekommit i närtid. Ogynsamma miljö - och /eller sociala faktorer saknas .

Bild 1; De hotnivåer (begrepp) som används inom Försvarsmakten. Den bedömda hotnivån innebär en samlad bedömning av en eller flera aktörers kapacitet, intention och tillfälle, att i tid och rum, direkt eller indirekt, angripa eller på annat sätt medvetet påverka en eller flera identifierade skyddsvärda tillgångar.

2.3.2. Främmande underrättelseorganisationer

I Säkerhetspolisens årsbok från 2017[5] framgår det att största underrättelsehotet mot Sverige utgörs av Ryssland. Rysslands spionage i och mot Sverige är mycket omfattande och har dessutom ökat i anslutning till krisen i Ukraina. På olaglig väg och i skydd av diplomatiska skenbefattningar samlar ryska underrättelseofficerare in information om det svenska försvaret, totalförsvaret, politik, ekonomi, teknik och forskning. Säkerhetspolisen bedömer till exempel att cirka en tredjedel av de ryska diplomaterna i Sverige arbetar under täckbefattning. Så såg det ut 2015 och så har det sett ut under flera år. Ryssland anmäler dessa personer som diplomater eller annan utsänd personal men i verkligheten är de underrättelseofficerare. Oftast arbetar de antingen för den militära underrättelsetjänsten GRU eller för dess civila motsvarighet SVR, som är sprunget ur det sovjetiska KGB. Under 2015 har rysk ambassadpersonal ombetts lämna landet på grund av verksamhet som inte är förenlig med Wienkonventionen om diplomatiska förbindelser[6]. Personalen inom den ryska underrättelsetjänsten anses av bedömare vara mycket välutbildade, yrkeskunniga och ambitiösa. Internationellt anses Sverige vara av stort intresse på grund av vår kompetens inom flertalet områden exempelvis forskning och utveckling samt vårt internationella samarbete. Inom MR S område bedrivs verksamhet över tiden som ingår i denna forskning och utveckling för att stärka FM förmåga på sikt. Vidare finns det dagligen enheter inom området som ingår i internationellt utbyte, beredskap eller under förberedelser för internationell tjänst.

Verksamhet som kan vara intressant för främmande makt är:

- Organisation, beredskap och förmåga vid våra förband och enheter.
- Utveckling, förändring och utbildning av förband.
- Nationella och multinationella övningar och insatser.
- Försvarsmaktens och försvarsindustrins prov- och försöksverksamhet.
- Utbildning, verksamhet och rotation av förband med internationella uppgifter.
- Specifik militär materiel (t.ex. kryptomateriel, målsökare, demonstratorer).
- Inom ramen för inspektioner, bi- och multilateral övningsverksamhet (t.ex. elever, lärare, örlogsbesök, kamratföreningsverksamhet växeltjänstgöring, utbyte mellan hemvärnsförband).
- Nyckelpersonal samt nuvarande och kommande chefer.
- Infrastruktur vid uppbyggnad eller avveckling av militära anläggningar.

Inom ramen för internationellt utbyte kan inhämtning ske t.ex. genom:

[5] Säkerhetspolisens årsbok 2017
[6] Säkerhetspolisens årsbok 2015

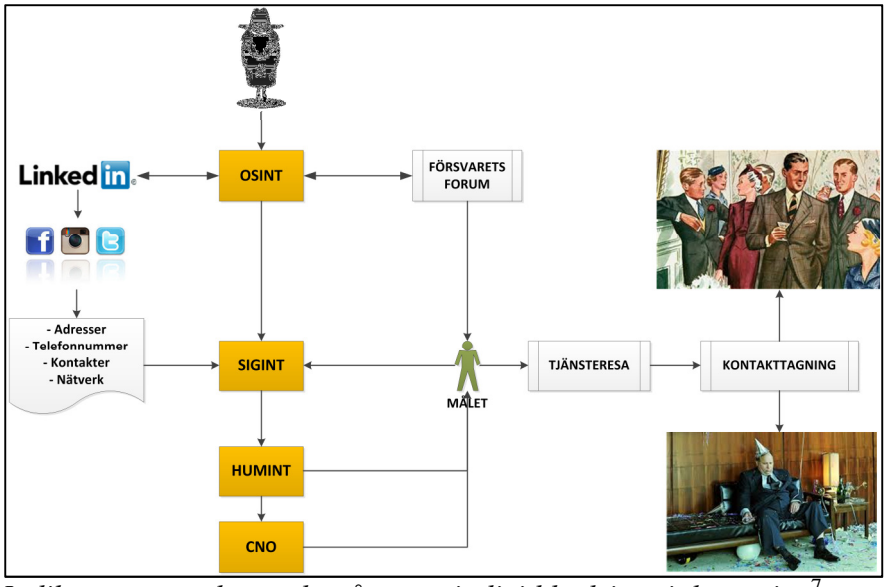
- Olika former av försök till kontaktverksamhet riktad mot personal inom Försvarsmakten,
- Studier och kopiering av handlingar/datafiler som lämnats kvar på expeditioner eller i andra lokaler,
- Kontroll av befintliga brevfack och papperskorgar,
- Avlyssning/överhörning av samtal - dölja språkkunskaper,
- Fotografering av materiel och objekt t ex med mobiltelefon med kamerafunktion,
- Högre chef ex i en FN missionen kan efterfråga information ex. personallistor och förmågebeskrivande dokument
- Oklara ackrediteringar och regelverk inom IT-baserade informationssystem.

Insiders/ SUA

Många utländska underrättelseorganisationer är intresserade och betjänta av att ha ”insiders”. Detta skapar man genom att inledningsvis kartlägga en blivande målpersons intressen och sårbarheter. Personal med uppgift att skapa kontakt har normalt en hög social och språklig kompetens och kan t.ex. tillhöra en utländsk beskickning. Den blivande insidern/målpersonen ska skapas en känsla av denne gör nytta på ett oskyldigt och positivt sätt. Syftet är att få svar på så många underrättelsefrågor som möjligt utan att hot behöver användas. Lyckas man med en sådan värvning har man skapat en ”insider” som kan vara svår för Försvarsmakten att upptäcka. Det är nödvändigt att all FM personal får insikt om hur ett närmande kan gå till så att ingen luras att bli en så kallad aningslös informationslämnare till främmande makt. Till exempel kan en företrädare för främmande makt återkomma lång tid efter ett besök via e-post, telefon, sociala medier eller annat för att knyta upp en kontakt.

Värvning av personal sker ofta enligt följande modus operandi:

- Analysfas – var finns önskvärd information?
- Målsökningsfas – vem eller vilka har access till önskvärd information?
- Studiefas – kartläggning av möjliga informationsbärare.
- Närmandefas – närmande sker naturligt och tillsynes slumpmässigt.
- Vänskapsfas – relationen fördjupas.
- Tillvänjningsfas – utdelning av gåvor och enklare testuppdrag.
- Värvningsfas – relation utvecklas till en vana och positiv känsloupplevelse, informationsbärare kan inte backa ur – underförtäckta hot om avslöjande.



Indikatorer som kan tyda på att en individ bedriver inhämtning[7]

- Försöker att skaffa access till information som individen inte är behörig till.
- Begära av andra att inhämta eller möjliggöra access till sekretessbelagd eller på annat sätt känslig information som individen inte är behörig till.
- Ovanlig nyfikenhet eller frågvishet, i synnerhet gentemot arbetskamrater, i ärenden som individen inte behöver för sin tjänst eller till vilka individen inte är behörig.
- Omfattande användning av kopiator, fax eller dator för att reproducera sekretessbelagd eller på annat sätt känsligt eller skyddat material, till en sådan grad att det inte kan förklaras med behov för tjänsten, särskilt om detta sker när andra inte är närvarande.
- Återkommande arbete utanför ordinarie arbetstider när detta inte krävs för tjänsten och när andra inte är på kontoret. För att undvika att synas vid de tillfällen då spionaget genomförs kan spionen komma tidigt till arbetet och/eller stanna sent, då risken att någon gör iakttagelser som kan rapporteras är väsentligen lägre.

Ickelinjär hotet

Det svenska samhället är i all väsentligt robust men samtidigt påverkningsbart. Det påverkningsbara i samhället är bland annat vårt beroende av el- och vattenförsörjning, men även vår mottaglighet för information genom att ständigt vara uppkopplad på internet eller genom traditionell media. Samhället kan påverkas och manipuleras eller utsättas för svåra påfrestningar av en utländsk

[7] OSINT = Open Source Intelligence. SIGINT = Signals Intelligence. HUMINT = Human Intelligence. CNO = Computer Network Operations.

aktör utan att Sverige befinner sig i krig, och ett krig som utspelas mellan arméer på ett slagfält tappar allt mer sin relevans. Utvecklingen av militära funktioner så som psykologiska operationer, informationsteknologi och IT-förband blir allt viktigare. En effekt av att nyttja icke -militära metoder medför att gränsdragningen mellan krig och fred blir otydlig. En annan är att strategiska mål kan uppnås av en angripare, genom förnekelse, desinformation och tvivel[8].

Den ryska olagliga annekteringen av Krim 2014 är ett tydligt exempel på detta. Det är tydligt att användningen av informationsoperationer i konflikter är här för att stanna. Ett antal aspekter på informationskrigföring skildras i en FOI-rapport om Rysslands annektering av Krim[9]. I februari 2014 publicerades påstått autentiska e-postmeddelanden som antydde att de nya ukrainska ledarna styrdes från väst, läckta av någon som kallade sig Anonymous Ukraine. Ryska myndigheter beordrade därpå blockering av pro-ukrainska grupper på sociala nätverk i Ryssland. Även framstående oppositionella ryssar fick vid ungefär samma tidpunkt se sina webbplatser officiellt blockeras av de ryska myndigheterna. Hemsidor för ukrainska myndigheter och både pro-ryska och pro-ukrainska nyhetsredaktioner utsattes därefter för överbelastningsattacker där det inte gick att fastställa vem som låg bakom.

Den ukrainska säkerhetstjänsten rapporterade om intrång med skadlig kod i parlamentsledamöters mobiltelefoner och teleoperatören *Ukrtelecom* meddelade i inledningen av Krim-operationen att fiberkablar hade kapats och att uniformerad personal hade tagit över deras knutpunkter[10]. Mest slående var kanske ändå samordning mellan olika sensorer och funktioners sätt att bedriva informationskrigföring. Samordnat levererades ett budskap från den ryska politiska ledningen, dess diplomatiska beskickningar och rysk statskontrollerad internationell media som RT (tidigare Russia Today). I budskapet användes information från de läckta telefonsamtalen med amerikanska och estniska diplomater. De avlyssnade diplomatsamtalen antyder att kvalificerad signalspaning användes för att få ett massmedialt genomslag som spred tvivel och osäkerhet i västvärlden. Information spreds med hjälp av sociala medier och plockades därefter upp av traditionella media.

Informationsoperationer kompletterade den traditionella militära verksamheten och var en viktig faktor för den ryska framgången i Krim-operationen, konstaterar FOI[11]. En likartad bedömning görs av norska Forsvarets forskningsinstitutt: ryska cyberangrepp på viktiga ukrainska kommunikationskanaler syftade till att styra kommunikationsmöjligheterna för

[8] MSB Informationssäkerhet: Trender 2015
[9] The Crimea Operation: Implications for Future Russian Military Interventions. *A Rude Awakening. Ramifications of Russian Aggression Towards Ukraine.* FOI, Totalförsvarets forskningsinstitut, Stockholm, 2014.
[10] MSB Informationssäkerhet: Trender 2015
[11] The Crimea Operation: Implications for Future Russian Military Interventions. *A Rude Awakening. Ramifications of Russian Aggression Towards Ukraine.* FOI, Totalförsvarets forskningsinstitut, Stockholm, 2014.

utvalda målgrupper, och samtidigt som Krim kommunikationsmässigt skars av från omvärlden genomfördes en massiv informationskampanj riktad mot västvärlden i syfte att få ut ett budskap om legitimiteten i det ryska agerandet[12]. Liknande exempel kan hämtas från andra moderna konflikter.

2.3.3. *Kriminell underrättelseinhämtning*

Försvarsmaktens personal har access till materiel som är stöldbegärlig och kan hamna i lojalitetskonflikter genom samröre med olika kriminella nätverk, eller i samband med hot, olämpligt umgänge eller andra påtryckningar. Kriminell underrättelseinhämtning har konstaterats i form av telefonsamtal till förläggningar, vaktlokaler och till personal i övrigt inom Försvarsmakten. Syftet med samtalen bedöms vara att inhämta information om var viss verksamhet bedrivs, omfattning och förekomst av vapen. Även underrättelseinhämtning i syfte att klarlägga huruvida objektet är larmat och omfattningen av våra motåtgärder har sannolikt skett.

Informationsspridning via Internet såsom hemsidor, bloggar och sociala nätverk ökar. I en del fall har förekomst av sekretessbelagd information påträffats. I de flesta fall rör det sig om okunskap i den enskildes iver att presentera sig själv och egen organisation. Chef för Förband, skolor och centra med underställda chefer skall säkerställa att kunskap sprids till anställda, kontrakterade, rekryter, hemvärns- och frivilligpersonal. Utbildning skall genomföras om riskerna vid publicering av uppgifter på Internet, i syfte att öka egen personals säkerhetsmedvetande.

Förekomst av s.k. ”tavelförsäljare” inrapporteras med jämna mellanrum. Företeelsen bedöms kvarstå. Verksamheten bedöms till stor del vara kommersiell och utövas av studenter vilka på detta sätt finansierar sina studier. Underrättelseinhämtning kan dock inte uteslutas och då främst som förberedelse till kriminell verksamhet. Så kallade ”tavelförsäljare” skall fortsättningsvis inrapporteras.

2.3.4. Övrig underrättelseverksamhet

På Internet förekommer ett antal intressegrupper där medlemmar visar stort intresse för militär verksamhet och Försvarsmaktens objekt. Målet för dessa grupper är att inhämta information om var och hur vi genomför vår verksamhet och vilka möjligheter det finns att erhålla tillträde till militära anläggningar. Okunskap och bristande säkerhetsmedvetenhet ligger ofta bakom publicering av sekretessbelagda uppgifter om vår verksamhet och våra anläggningar.
Under det senaste året har allt fler olika intressegrupper etablerats på Internet av personer med anknytning till Försvarsmakten. I vissa fall har attribut antagits som kan återfinnas inom den kriminella världen. Härmed kan personen ifråga komma

[12] Henning André Søgard och Janne Merete Hagen. *FFI-fokus: Kampen om sannheten*. Forsvarets forskningsinstitutt, 2014.

att bli föremål för kontakttagning och medför på sikt risk för att dras in i den kriminella världen. I förlängningen kan detta medföra att personen måste skiljas från sin anställning inom Försvarsmakten.
MR S J2 rekommenderar anställda inom organisationsenheter att ta kontakt med säkerhetstjänsten för rådgivning innan publicering och presentation av intressegrupp sker på Internet.

2.3.5. Kriminalitet

Kriminalitet är vid sidan av främmande underrättelseinhämtning den form av säkerhetshotande verksamhet inom MR S område som för närvarande bedöms vara den mest påtagliga. Omfattningen av den kriminella verksamheten inom MR S tar sig uttryck inom ett flertal olika områden, såsom angrepp på teleanläggningar, ammunitionsförråd och andra förråd samt ekonomiska brott både externa och interna.
Kriminella har ett fortsatt intresse för militär materiel av olika slag i Sverige och detta intresse bedöms kvarstå under 2018.
Inom MR S område har främst följande materialslag, utöver vapen, ammunition samt spräng- och tändmedel intresserat kriminella:

- Optisk materiel (kikare/bildförstärkare).
- Sambandsmateriel (kommunikationsutrustning).
- Uniformer.
- Drivmedel.
- Metaller (koppar, aluminium).
- Ballistiska skydd.
- Hjälm 90.
- Skyddsmask 90 MTB.

Materiel av intresse i kriminella kretsar avyttras på illegal väg och den bedöms troligen användas i annan kriminell verksamhet inom eller utom Sverige. Försvarsmaktens avveckling av materiel och dess slutdestination bedöms också vara av intresse inom kriminella kretsar.
Vad avser den ekonomiska brottsligheten består den av både externt och internt relaterade händelser. Internt tar det sig uttryck såsom stöld av IT-utrustning, drivmedel, pengar och militär utrustning m.m. I en del fall har befintliga säkerhetsskyddsanordningar t.ex. grindar och lås satts ur spel.
En inkörsport till kriminalitet som kan drabba Försvarsmakten är förekomst och missbruk av droger, anabola steroider eller andra typer av berusningsmedel. Drogmissbruk finansieras oftast genom olika former av kriminalitet, men skall också ses ur ett verksamhetssäkerhetsperspektiv. Det medför en ökad risk att personal som hanterar vapen, framför fordon m.m. kan vara påverkade av droger. Inom MR S område har enstaka fall av drogmissbruk inträffat, både inom grundutbildning och inom hemvärnet. Därför bör utbildning och information rörande droger planeras för personal inom förband och enheter.

2.3.6. Terrorism

Nedan är ett utdrag av terrordåd som drabbat Europeiska länder i närtid.

- 13 nov 2015 i Paris.
- 22 mars 2016 i Bryssel.
- 28 juni 2016 i Istanbuls.
- 14 juli 2016 i Nice.
- 22 juli 2016 i München.
- 26 juli 2016 i St Étienne-du-Rouvray.
- 19 dec 2017 i Berlin.
- 19 dec 2017 i Zürich.
- 1 jan 2017 i Istanbul.
- 22 mars 2017 I London.
- 3 april 2017 i S:t Petersburg.
- 7 april 2017 i Stockholm.
- 20 april 2017 i Paris.
- 22 maj 2017 i Manchester.
- 3 juni 2017 i London.
- 20 juni 2017 i Bryssel.
- 9 aug 2017 i Levallois-Perret.
- 17 aug 2017 i Katalonien.
- 18 aug 2017 i Åbo.
- 26 aug 2017 i Bryssel.

Religiöst motiverad terrorism

Hot i form av terrorism mot Sverige och Försvarsmakten följer Säkerhetspolisens nationella bedömning. Händelser som inträffat under 2016-2017 i Europa understryker allvaret och bekräftar att även Sverige kan utsättas för allvarliga händelser. En terrorist är oftast ideologiskt motiverad i de extrema ytterkanterna av politik eller religion. Den ideologiska motiveringen är ofta kopplad till en konflikt eller sakfråga som uppfattas som orättvis. Idag är det sunniislamistiska extremister som begår de allvarligaste terroristbrotten[13].

De pågående konflikterna i Mellanöstern under 2016-2017 den i särklass mest drivande faktorn bakom terrorismen. Ett exceptionellt högt antal svenskar har anslutit sig till sunniextremistiska terroristgrupper verksamma i Syrien och Irak. Att ansluta sig till en terroristgrupp är allvarligt då personens kapacitet och intuition att utföra terroristattentat kan öka. De flesta svenskar som ansluter sig till terroristgrupper är unga män mellan 18 och 30 år, födda i Sverige med minst en förälder född utomlands och saknar eller har låg inkomst. En tredjedel har kriminell bakgrund. Den stora majoriteten av individer har rest till Syrien för att ansluta sig till den så kallade Islamiska

[13] Säkerhetspolisens årsbok 2015

staten men under 2016 har de flesta nya resenärerna i första hand anslutit sig till Jabhat Fatah al-Sham eller närliggande grupper.

Jabhat Fatah al-Sham kallade sig tidigare för Jabhat al-Nusra eller Nusrafronten och har varit en del av al-Qaidas nätverk[14]. De som överlever och väljer att återvända har samlat på sig ny kunskap, nya kontakter, sänkt sin våldströskel och kan bli statusgestalt för andra extremister. De återvändare som fortfarande anser att ideologin är korrekt fortsätter troligtvis att verka i Sverige inom stödverksamhet eller radikalisering[15]. Daeshs verkar även som inspirationskälla för individer som inte har möjlighet att resa tillkonfliktområden för att ansluta sig till gruppen men som är villiga att agera på gruppens uppmaningar till attentat i västvärlden. Daesh har särskilt uppmanat sina anhängare i västländer att genomföra attentat i länder som kriminaliserat resor till konfliktområden i syfte att bistå eller träna hos terrornätverk[16]. Daesh är den grupp som under senare tid haft starkast förmåga att förmå och inspirera anhängare till attentat i västvärlden. al-Qaida verkar mer långsiktigt och har inte prioriterat attentatsplanering mot västvärlden på senare tid. Detta förhindrar inte att ensamagerande individer inspirerade av al-Qaida kan agera på eget bevåg utan uppdrag från organisationen

På senare tid har västvärlden utsatts för attentat genomförda av ensamagerande gärningsmän som agerar utifrån en våldsbejakande islamistisk ideologi. En ensam gärningsperson eller mindre grupper skapar vanligen mindre uppmärksamhet varvid dessa vanligen är svårare att detektera innan en kommande attack[17].

Attentaten under 2017 har genomförts, eller varit planerade att genomföras, med relativt enkla medel som stick- eller skjutvapen. Sprängmedel användes i samband med attentaten i Bryssel samt som tilltänkt tillvägagångssätt i planerade attentat på andra platser. Attentatet i Nice den 14 juli 2016 och i Berlin den 19 december 2016, då förövarna använde lastbilar som tillvägagångssätt för att döda folkmassor på allmän plats, visar emellertid att även attentat som genomförs med enklare medel kan leda till ett stort skadeutfall. Daesh har genom officiella kanaler tagit på sig ansvaret för flera av de terrorattentat som har genomförts under 2016[18]

Politiskt motiverad terrorism

Med politiskt motiverad terrorism avses här främst våldshandlingar utförda av aktörer motiverade av antingen våldsfrämjande högerideologi den s.k. vit makt-miljön eller våldsfrämjande vänsterideologi den s.k. autonoma miljön i Sverige. Vit makt-miljön består av individer och grupper som strävar efter ett etniskt homogent samhälle och ett styrelseskick som baseras på etnicitet. Aktörerna inom

[14] NCT Helårsbedömning 2017
[15] Säkerhetspolisens årsbok 2017
[16] EUROPOL Terror and trend report 2016
[17] Säkerhetspolisens årsbok 2017
[18] NCT Helårsbedömning 2017

den autonoma miljön består av individer och grupper som strävar efter ett klasslöst samhälle fritt från ett förtryck som aktörerna upplever komma från alla typer av auktoriteter och hierarkier. Inom båda dessa grupper finns aktörer som förespråkar väpnad kamp. Detta kan möjligen även inspirera enskilda individer ur båda grupperna att genomföra handlingar som skulle kunna klassificeras som terrorbrott.

Båda grupperna har det senaste året uppvisat en låg aktivitetsnivå avseende våldshandlingar som skulle kunna rubriceras som terrorattentat. Det finns dock sannolikt individer och grupper inom båda grupperna som har kapacitet att genomföra våldshandlingar som skulle kunna rubriceras som terrorattentat. Möjligen kommer även ett fåtal individer kopplade till eller inspirerade av dessa grupper också ha sådana intentioner under 2017[19].

Hotet mot Försvarsmakten skyddsvärde kan variera över tiden och styrs av vår verksamhet. Engagemang utomlands inom ramen för internationella övningar eller insatser kan medföra att hotbilden höjs. Delvis på grund av att deltagande länder och utländsk personal kan ha en annan hotbild vad avser terrorism och kan medföra att vi måste anpassa våra säkerhetsskyddsåtgärder. Säkerhetsanalys ska genomföras inför varje sådant tillfälle. De senaste årens utveckling av hotet från terrorism ställer nya krav på säkerhetsskyddsåtgärder, exempelvis vad gäller säkerhetsprövning, informationssäkerhet och tillträdesskydd. Det föreligger idag en hotbild där en aktör exempelvis vill skapa tillträde enbart för att utföra våldsamma terrorhandlingar. Detta ställer delvis nya krav på säkerhetsprövning av personal med tillträde till Försvarsmaktens anläggningar, att personuppgifter på Försvarsmaktens personal har ett ändamålsenligt skydd och att det fysiska tillträdesskyddet anpassas efter aktuell hotbild.

2.3.7. Subversion

Verksamhet som syftar till att genom vilseledande informationsspridning påverka en specifik målgrupps lägesuppfattning, lojalitet eller förtroende. Hotet från subversion hör informationsarenan till och kan utövas av både statsaktörer och icke-statliga aktörer liksom av olika intressegrupper eller enskilda individer. Samtliga aktörer använder i en ökad grad sociala medier för att sprida desinformation och vilseledning riktat mot Försvarsmaktens personal. Försvarsmaktens personal ska upplysas om vikten av källkritik samt att analysera risker med att publicera personlig information på sociala medier. Innan information från externa källor används inom egen verksamhet skall adekvat källkritik genomföras. För mer information se punkten det ickelinjära hotet.

2.3.8. Sabotage

Med sabotage avses verksamhet som syftar till att förstöra, hindra, försvåra eller störa ett visst objekt eller viss verksamhet. Sabotage kan exempelvis handla om sprängningar, angrepp på kritisk infrastruktur, bakteriologisk eller kemisk

[19] NCT Helårsbedömning 2017

påverkan av vital försörjning, stöld och skadegörelse. Hotet från sabotageaktioner är främst aktuellt i skymningsläge eller krigstid. I fredstid består hotet i de förberedelser som görs för att kunna genomföra aktioner i ett senare läge.

Försvarsmaktens personal bör redan i fredstid vara uppmärksamma på misstänkt verksamhet som skulle kunna indikera att en angripare genomför rekognosceringar eller vidtar andra förberedelser. Det skall dock framhållas att det ofta är svårt att bedöma om angrepp mot våra objekt skall klassificeras som sabotage eller grov skadegörelse.

2.3.9. Infiltration

Risken för infiltration är påtaglig i de fall Försvarsmakten får in personal i organisationen som har kopplingar till främmande underrättelsetjänster, den organiserade kriminaliteten, autonoma miljön eller religiöst inriktade grupperingar. Det är sannolikt att dessa grupperingar aktivt försöker få tillgång till tjänster i Försvarsmakten. Detta kan ske både direkt, genom att personer söker tjänster i Försvarsmakten eller indirekt genom att de får tillgång till information genom aktiv målsökning mot anställd personal.

Risk för infiltration i samband med övningsverksamhet föreligger från personer som uppträder i Försvarsmaktens uniformer och fordon. Det är viktigt att understryka och utbilda egen personal att uniform inte är en legitimation för tillträde och/eller behörighet. Identitet kontrolleras med ID-handling och vid behov genom kontakt med utfärdare.

Den anställda personalen innehar kompetenser och förmågor som är eftertraktade i många olika typer av verksamheter, inte minst av mindre nogräknade säkerhetsföretag och olika kriminella organisationer. Våra vidtagna säkerhetshöjande åtgärder ökar behovet av insiders för den kriminella verksamheten riktad mot Försvarsmakten. Personal tillhörande hemvärnet kan vara en personalgrupp som är av intresse för kriminella organisationer både i syfte att värva medlemmar med specifika kunskaper eller för att komma över vapen.

2.4. Informations- och ledningssystem

2.4.1. Hot mot våra informations- och ledningssystem

Hot mot våra informations- och ledningssystem utgörs av angrepp eller andra störningar som kan ge upphov till driftavbrott, informationsförlust, förvanskning eller sekretessförlust. Hoten mot Försvarsmaktens informationssystem kan generellt beskrivas som:
Obehörig och oönskad användning och påverkan av Försvarsmakten.
Information av aktörer utanför Försvarsmakten.
Obehörig och oönskad användning och påverkan av Försvarsmaktens information av egen personal (okunskap, insider(BESKT[20]).

[20] FM förkortning av en påverkbar person som uppfyller en eller fler kategorier av Besviken, Ekonomiskt, Socialt, Kontakter, Tillfället

Olycka, hårdvaruhaveri, programvaruhaveri och påverkan av olika miljöfaktorer.
Angriparens syfte är oftast att komma över information. Tillvägagångssättet är relativt likartat oavsett angripare. Intresset bedöms vara underlag rörande säkerhetspolitik, förbandsutveckling och teknikutveckling. Främmande makt kan även använda IT som ett vapen genom att störa och förvanska information. Bakomliggande syfte kan vara att avskräcka, vilseleda, utpressa alternativt för kunna utöva psykologisk krigsföring.
Kriminella individer och nätverk är inriktade i huvudsak mot mål som kan utnyttjas för ekonomisk vinning. En stor del av den ekonomiska marknaden sker idag via Internet, vilket har skapat möjligheter för kriminell verksamhet med låga risker. Främmande makt kan även använda sig av tredjehands parter, som till exempel kriminella, politiska eller religiösa grupper, för att vilseleda och/eller dölja sina motiv, intentioner eller identitet.
Riktade attacker mot informationssystem och informationstillgångar kan genomföras utan begränsningar och från hela världen. Ett exempel på en sådan riktad attack är den skadliga koden "Stuxnet" som konstruerades för att slå ut specifika mål som använder industriella styrsystem. En efterföljare till ”Stuxnet” är "Flame" som är en avancerad skadlig kod för angrepp på specifika mål. Utvecklingen i övrigt går från masspridande skadlig kod till specialanpassade verktyg för specifika målgrupper och ändamål, så kallat ”spjutfiske” eller ”Spear Phishing”. Mål för attacker är ofta nyckelpersoner och/eller verksamhetskritisk infrastruktur. Avancerade angrepp kan vara mycket svåra att upptäcka. En skadlig kod kan finnas kvar länge i ett system. Koden har också förmåga att ändra sig för att försvåra upptäckt och den kan radera sig själv eller raderas av angriparen, allt i syfte att undgå upptäckt. Sociala nätverk används även för kontakttagning i syfte att värva uppgiftslämnare samt ge underlag för hot och utpressning mot person samt dennes kollegor och familj. Tendensen tyder även på en ökad exponering av skyddsvärd information i form av text och bild som kan ge ett underrättelsevärde för främmande makt eller kriminella.
Det finns flera metoder som kan användas enskilt eller i kombination för att angripa ett mål med hjälp av IT. Användandet av sociala medier möjliggör ökad interaktion mellan användare och tjänster på internet vilket hela tiden skapar nya möjligheter att kunna lura användaren till att göra tillsynes oskyldiga saker som direkt kan påverka säkerheten. Det är även vanligt att katastrofer och andra stora händelser används för att locka användaren till att vidta åtgärder som omedvetet möjliggör spridande av datavirus eller bedrägerier. Användandet av icke signerad eller krypterad E-post fortsätter att öka som ett alternativ till fysisk post, vilket gör att E-post fortfarande är populärt använda för att sprida skadlig kod eller genomföra bedrägerier med. Angriparen kan även vara skicklig i att inge förtroende, så kallad ”social engineering” och behöver inte enbart agera i den digitala världen utan kan även agera fysiskt.
Kombinationen av att blanda privata enheter och nätverk med arbetsgivarens enheter och nätverk (BYOD/BYON) öppnar upp nya in- och utgångar till IT-systemen, vilket är att betrakta som allvarliga säkerhetshål som kan åsidosätta IT-systemet befintliga säkerhetsmekanismer (USB minne tillhörande Försvarsmakten används på privat dator).

Stora mängder öppen information kan även om rätt behandlad avslöja detaljer som tillsammans är skyddsvärda. Automatisk insamling och analys av stora mängder information är idag ett verktyg för underrättelseinhämtning.
Lokalt driftsatta system som inte auktoriserats och ackrediterats enligt Försvarsmaktens livscykelmodell innebär ökad risk, då de ofta har bristande säkerhet och är sårbara för attacker från såväl extern som intern aktör.

2.4.2. Mobiltelefoner

Skadlig kod i mobiltelefoner förekommer och kommer att bli allt vanligare. Bärare av skadlig kod kan bland annat vara s.k. ”Appar” som användaren laddar ner. Bluetooth kan i aktivt läge innebära att en obehörig obemärkt kan utnyttja sårbarheter i en mobiltelefon för att skaffa sig åtkomst till telefonen. WiFi används allt mer då telefonerna blir mer beroende av snabb datatrafik. Wifi är lätt att manipulera vilket kan användas för avlysning samt för injektion av skadlig kod. Som en säkerhetshöjande åtgärd bör man alltid använda avancerad kryptering som WPA-2 med komplexa lösenord som regelbundet byts ut. Det är även viktigt att det faktiska WiFi nätverket man är ansluter till kontrolleras och administreras på ett säkert sätt.
Mobiltelefoner kan användas för positionering i syfte att kartlägga förband och skyddsvärda anläggningar. Moderna mobiltelefoner har GPS som bl.a. kan användas för att positionera bilder tagna med mobilens kamera s.k. ”geotaggning”. Mobiltelefoner är lätta att avlyssna. De kan fungera som avlyssningsutrustning i en lokal där .t ex. skyddsvärd verksamhet pågår. En extern aktör kan förse mobiltelefonen med skadlig kod som medger att den kopplas upp för att lyssna eller aktivera kameran. Inköp av s.k. ”bruslådor”[21] bör föregås av kontroll av giltigt säkerhetsgodkännande inom Försvarsmakten.

2.4.3. Signalspaning

Signalspaning mot våra sambandssystem pågår ständigt såväl mot verksamheten i det civila samhället som mot Försvarsmakten. Tekniken för signalspaning är under ständig utveckling och det som tidigare inte lät sig göras kan ske i dag. Det är därför av stor vikt att kunskap om aktuellt telekrigshot är föremål för utbildning inom respektive organisationsenhet. Avlyssningsrisken skall alltid beaktas vid all militär verksamhet.

2.4.4. Kopiatorer

Många moderna kopiatorer lagrar kopierade dokument i minnet vilket innebär risk för informationsförlust. Stora mängder kopierade dokument kan finnas på kopiatorns hårddisk åtkomliga för obehöriga t.ex. vid service eller skrotning/omsättning. Dokument som innehåller sekretess får endast kopieras på för detta ändamål godkänd kopiator.

[21] ”Bruslåda” ljudisolerad låda för förvaring av mobiltelefon för att förhindra informationsförlust

2.5. Informationssäkerhet

Pågående förändringar i Försvarsmaktens organisation kan innebära en ökad risksituation att personalen kan komma att känna besvikelse mot Försvarsmakten som arbetsgivare då en för den enskilde osäker ekonomisk och social framtidssituation kan förväntas. Till följd av detta kan lojaliteten mot Försvarsmakten riskera att avta och inbjuda till att säkerhetsmedvetandet eftersätts. Resultat och konsekvenser av detta kan få allvarliga följder för Försvarsmakten. Förtroendet för Försvarsmakten kan undergrävas och samarbetsklimat till annan stat eller organisation kan skadas.

I samband med Försvarsmakten omstrukturering/förändring finns risk att sekretessbelagd information som avser tidigare förhållanden kan komma att betraktas som mindre skyddsvärd eller röjas på grund av oaktsamhet. Personal under avveckling utgör en risk då dessa har kunskap om förhållanden som omges av sekretess. Enskilda kan visa bitterhet eller besvikelse genom att vända sig mot Försvarsmakten. Detta kan ta sig uttryck i form av tillgrepp, men också i enstaka och extrema fall leda till missnöjesyttringar i form av hot och våld m.m.

3. Säkerhetsskyddsåtgärder

Det är av stor vikt att anställda vid FM förstår att säkerhetstjänst är allas och envars ansvar genom ex rapportera brister, sårbarheter och oklarheter.

Lokala säkerhetsfunktioner uppmuntras utveckla/vidmakthåll lokala nätverket med ex företag/organisation vars verksamhet bedrivs nära OrgE skyddsvärden, likt grannsamverkan för säkerhet kan dessa rapportera avvikelser från normalbilden, en normalbild som de vanligen har god uppfattning om.

Det är vid flertalet tillfällen mer lämpat att som försvarsmaktsanställd, i synnerhet skyddsvakt/MP, agera ex genom att fråga och därefter vid behov rapportera än att observera och rapportera. Inte sällan så blir den sistnämnda alternativet en informationsfattig rapport som lämnar fler frågetecken än utropstecken.

3.1. Skydd mot främmande underrättelseverksamhet

Kontinuerlig inrapportering av skyddsvärd och säkerhetshotande verksamhet inom Försvarsmakten är en förutsättning för att kunna samordna och prioritera säkerhetstjänsten.

All personal vid förbanden inom MR S ansvarsområde, ska till MR S J2 via egen säkerhetsorganisation inlämna rapport om kontakt eller samverkan har skett med representant från främmande makt eller annan främmande statlig myndighet i och utom tjänsten.

Kontroll av outsourcing inom garnisonen. Företag och entreprenörer som finns i och i anslutning till materiel, personal, information och anläggningar där FM har verksamhetsansvaret.

3.2. Skydd mot kriminalitet

Chef som har ansvar för att förvara skyddsvärd materiel ska göra en analys och besluta skyddsnivå för förvaring av tilldelad materiel. I analysen ska hänsyn tas till mängd av skyddsvärd materiel, materielslag och bedömd hotbild. Vid övningsverksamhet ska man särskilt analysera förvaring av stöldbegärlig och verksamhetskritisk materiel över tiden, samt under transport till och från aktuellt övnings/ grupperingsområde. Verksamhetskritisk materiel bör där så är möjligt inte förvaras i obevakade förråd. Ett alternativ kan vara att låsa in materielen i en på platsen tillförd kassun.

Försvarsmakten har under de senaste åren genomfört stora investeringar för säker förvaring av vapen och ammunition. Genom dessa åtgärder bedöms hotbilden, vad avser tillgrepp av vapen, ha förskjutits mot vapen i bruk. Särskild uppmärksamhet av vapenhantering bör genomföras inför och under större övningar. Tillgrepp genom insiders ska vara föremål för särskild säkerhetsanalys vid planering av verksamhet där större mängder vapen förekommer, t.ex. större övningar och transporter av vapen. Genomgång av gällande bestämmelser i förvaring och hantering av vapen är av största vikt och skall vara en naturlig del i planering och genomförande av övningar. Om förlust av vapen sker ska ansvarigt befäl/arbetsledare veta vilka omedelbara åtgärder som ska vidtas. Dessa åtgärder ska inskrivas i övningsbestämmelser och vara föremål för utbildning.

Vid större övningar och allmänt under utbildning bör behovet av användning av privat mobiltelefon analyseras och regleras. Rutiner för hantering av mobiltelefon i tjänsten skall regleras i förbands styrdokument. Säkerhetsskyddsåtgärder skall anpassas med hänsyn till resultat av genomförd säkerhetsanalys.

Det är av största vikt att ronderings- och insatsstyrkor samt personal ur FMLOG, FMV, FSV och FMTIS är uppmärksamma på ”onormala” tecken runt och vid objekt. Även den minsta skada som t.ex. små ”millimeterstora” hål på en ammunitionsdörr/vägg eller ett lås kan vara en del av förberedelse till inbrott. Förekomst av misstänkta fordon i närheten av Försvarsmaktens objekt är intressant och särskilt fabrikat, registreringsnummer och färg.

Den småskaliga kriminaliteten är många gånger lokalt knuten verksamhet och bl.a. den anledningen uppmuntras OrgE säkerhetsfunktion utveckla/bibehålla en god samverkan med lokala polisen.

Stölder(konsekvenser) kan minimeras genom:

- Internkontroll.
- Kontroll och inventering av nycklar till befintliga utrymmen.

- Kontroll(inventering) av utrymmen med IT-media.
- Regelbunden kontroll att befintliga säkerhetsskyddsutrustningar.
- Återkommande och oanmälda inventeringar av stöldbegärlig utrustning.
- Analys om omfattning och förvaring av verksamhetskritisk materiel.

3.3. Skydd mot terrorism

Hotbilden avseende terrorism kan variera över tiden inom ramen för inspektioner bi- och multilateral övningsverksamhet. Andra deltagande länder och utländsk personal kan ha en annan hotbild vad avser terrorism och kan komma att ställa krav på säkerhetsskyddsåtgärder i samband med deltagande i internationella övningar inom svenskt territorium. Säkerhetsanalys med säkerhetsplan skall alltid genomföras inför varje sådant övningstillfälle.

Att angripa militär personal i Sverige kan ge den effekt som är avsedd med ett terrorangrepp. Därför ska uppträdande i uniform vid resor och vid uppträdande på allmänna platser övervägas och bör undvikas då det ej är nödvändigt. Terrorismens spridning under senare år och händelser pekar på vikten av att man i förbandens/enheternas årliga översyn av säkerhetsanalyser och säkerhetsplaner även beaktar olika scenarier i planeringssammanhang. På detta sätt utvecklas en planering för en förändrad hotbild i förhållande till dagens hotsituation mot Försvarsmaktens olika förband.

Hotbilden kan snabbt höjas och kan även bestå under en tidsperiod med en möjlig större inverkan på verksamheten men även bidra till kostnader för hastigt och tillfälligt vidtagna säkerhetsskyddsåtgärder. Kostnader som möjligen kan minskas om vissa förberedelser är gjorda sedan tidigare.

3.4. Skydd mot sabotage

Sabotage som säkerhetshot bör skiljas från sabotage som vald metod. Framförallt är detta viktigt för att kunna utforma relevanta skyddsåtgärder.

3.5. Skydd mot infiltration

Uppmärksamhet på tendenser, tecken eller olika former av extrema yttringar måste följas upp och dessa individers förhållande klarläggas. I praktiken kan detta ske genom säkerhetssamtal med personal. Detta skall göras i syfte att säkerställa förtroendet för Försvarsmakten samt att försvåra tillgrepp av vapen och viktig materiel. Chefer för förband och organisationsenheter måste vara uppmärksam på egen personals sociala situation så att enskilda inte riskerar att utsättas för kriminella och extrema organisationers intresse. I detta sammanhang skall särskilt poängteras vikten av en grundlig säkerhetsprövning och referenstagning inför rekrytering. Underlag för bedömning av sökande kan i särskilda fall inhämtas via respektive förbands säkerhetsorganisation.

Det finns indikatorer att personal i en behovsställning, ex rekryterande chef, kan vara mer benägen att genomföra en något mindre djupgående säkerhetsprövningsintervju. Det kan misstänkas att detta gäller i synnerhet när personalkategorin ifråga tillhör vad som anses vara sk svårrekryterad nyckelpersonal.

Den kombinationen ökar risken att anställningsprocessen forceras varvid det viktiga och vanligen tidskrävande förarbetet inför säkerhetsintervjun kan bli bristande. Vid intervjuer kan även vissa frågor/frågetecken inte penetreras på ett önskvärt sätt. I dessa fall, då en sådan situation föreligger, bör säkerhetsprövning lämpligen ledas av någon annan.

Uttrycket - Hellre en bra vakans än en dålig rekrytering – är fortfarande gällande.

3.6. Informationsskydd och skydd av IT-system

Den enskilt viktigaste säkerhetshöjande åtgärden är att informera och utbilda samtlig personal om rutiner, organisation/ansvar och hotbild rörande myndighetens informationssystem samt ge kunskap om metoder för att minimera riskerna vid olika typer av säkerhetshot. Det är även viktigt att utbilda användaren i hur denne säkert kan förhålla sitt privata användande av teknik med arbetsgivarens verksamhet och regler. Informationssystem inklusive tillfälliga IT-lösningar som är verksamhetskritiska och/eller innehåller skyddsvärd information, skall ha ett säkerhetsskydd som är anpassat mot aktuella hot och risker. Detta uppnås genom att genomföra verksamhets- och säkerhetsanalyser samt att följa de regelverk som finns och som reglerar IT-säkerhet och IT-verksamhet.

Säkerhetsskyddet av ett informationssystem skall beaktas under hela dess livslängd, från idé till avveckling. Auktorisations- och ackrediteringsprocessen är en förutsättning för detta. Vid exempelvis utvecklingsprojekt, omstruktureringar eller större övningar är det nödvändigt att redan från början ha med säkerhetstjänsten så att inte brister och luckor byggs in från början.

Informationssystem får enbart användas för de informationssäkerhetsklasser de är avsedda för. Att lagra hemlig information på öppna lagringsmedia eller i öppna nätverk får inte förekomma. Särskilda kontroller kommer att genomföras och åtgärder vidtas.

4. Övrigt

Förbands, skolors och centras säkerhetsrapportering ska ske till MR S J2 och HKV INSS J2 i IS UNDSÄK, senast inom 24 timmar.

Förbands, skolors och centras skyddsvärda verksamhet ska inrapporteras till MR S J2 med så lång framförhållning som möjligt enligt utgivna anvisningar.

Förband, skolors och centras säkerhetsorganisationer kan efter förfrågan erhålla särskilt hotbildsunderlag från MR S J2.

5. Ytterligare information

Ytterligare sammanställd information avseende hot och aktuell hotbild redovisas i MUST Säkerhetsårsbedömmande 2018 (SÅB)[22]. Som bilaga till MUST SÅB finns ett, ej sekretessklassificerad, bildspel som lämpar sig mycket väl till presentationer av hoten.

MR S J2 producerar flera produkter avseende Regional hotbilden och aktuella händelser i MR S bl.a. Veckoorientering med informationssäkerhetsklass Hemlig/Secret (H/S). De instanser med intresse, behov och som kan hantera informationssäkerhetsklassen H/S kan kontakta MR S J2.

6. Beslut

Beslut om föreliggande öppna säkerhetshotbeskrivning har fattats av C MR S Överste Jan Pålsson. I den slutliga handläggningen har örlogskapten Jonas Jönsson samt kapten Fredrik Plantin, den senare tillika föredragande.

Pålsson, Jan

Överste Jan Pålsson

Handlingen är fastställd i Försvarsmaktens elektroniska dokument- och ärendehanteringssystem.

[22] SÄKUR SÅB 2018

Sändlista

P 4	(avsett för enheterna i Kvarn)
Ing 2	(även avsett för Hemvärnsbat)
1. ubflj	
3. sjöstriflj	
4. sjöstriflj	
MarinB	(även avsett för Hemvärnsbat)
F 7	(avsett för enheterna i Linköpings garnison)
F 17	
Hkpflj	(avsett bl.a. för 3.hkpskv samt Hemvärnsbat)
FMLOG	(avsett för J2)
FMTIS	
MSS	(avsett för enheterna i Kvarn)
SSS	
LSS	(avsett för Hästveda)
FMTS	
SWEDEC	

Som orientering

HKV MUST SÄKK	
HKV INSS J2	
HKV INSS J3	
HKV ATS	
HKV MTS	
HKV FTS	
I 19	(avsett för MR N)
LG	(avsett för MR M)
P 4	(avsett för MR V)

Inom P 7

MR S	
G 2	(även avsett för Hemvärnsbat)

Utanför Försvarsmakten

FMV
Box 13400
580 13 Linköping

FMV
Amiralitetsgatan 25
371 82 Karlskrona

FOI
Box 1165
581 11 Linköping

Ekobrottsmyndigheten Malmö
Box 27
211 20 Malmö

Säkerhetspolisen
Region Syd
Box 12312
102 28 Stockholm

Säkerhetspolisen
Region Öst
Box 12312
102 28 Stockholm

Fortifikationsverket
Beredskaps- och säkerhetsenheten
631 89 Eskilstuna

Polisregion Syd (avsett för UND samt Gränspolis i samtliga Polisomr.)
205 90 Malmö

Polisregion Öst (avsett för UND samt Gränspolis i samtliga Polisomr.)
Box 345
581 03 Linköping

Tullverket (avsett Analyssektionen Nationella enheten MALMÖ)
Box 112854
112 98 Stockholm

Kustbevakningens Und (avsett för Nationella UND)