ÅRSÖVERSIKT 2017

MUST

Grafisk formgivning och tryck: FMV-FSV Grafisk produktion, mars 2018
Foto sid 5, 9, 12, 16, 18, 23, 25, 30, 32, 44: Jimmy Croona/Försvarsmakten
Foto sid 19, 40, 42, 43, 46: Försvarsmakten
Foto sid 6: Kim Svensson/Försvarsmakten
Foto sid 15: Hampus Hagstedt/Försvarsmakten
Foto sid 27, 29: Bezav Mahmod/Försvarsmakten
Foto sid: 35: Niklas Englund/Försvarsmakten
Foto sid 39: Melker Dahlstrand/Sveriges Riksdag

Prodid: 180205-016

ÅRSÖVERSIKT 2017

MILITÄRA UNDERRÄTTELSE- OCH SÄKERHETSTJÄNSTEN

FÖRSVARSMAKTEN

Innehållsförteckning

Vision och verksamhetsidé

Musts vision

Ett säkrare Sverige i en osäker värld.

Musts verksamhetsidé

Must ger regeringen och Försvarsmakten unika beslutsunderlag om omvärldsutvecklingen och hot mot Sveriges säkerhet.

Must bidrar till att Försvarsmaktens förmågor utvecklas och att förbanden har en bra hot- och lägesuppfattning. Vi bidrar också till att Försvarsmakten och andra myndigheter har rätt nivå på sin säkerhet.

Must löser sina uppgifter med hög integritet och i samverkan med andra. Vi utvecklar oss kontinuerligt för att kunna möta förändrade krav.

Chefen Musts förord

Händelserna under 2017 visar att vi lever i en osäker värld. Flera terrordåd genomfördes i Europa och den 7 april drabbades även Sverige. Våldet fortsatte i Irak och Syrien och på många andra platser rådde alltjämt spänning och kris. Den militära aktiviteten i Sveriges närområde har ökat under senare år och Östersjöregionen är alltjämt en friktionsyta mellan öst och väst. Frågor om cybersäkerhet och samhällsfunktioners sårbarheter har fått stor uppmärksamhet i den offentliga debatten. Allt detta påverkar Sverige.

Underrättelsetjänsten behövs för att ge våra beslutsfattare unika underlag och bedömningar. Säkerhetstjänsten behövs för att våra skyddsvärden ska kunna skyddas. Tack vare kompetenta medarbetares hårda arbete har vi kunnat lösa vårt uppdrag. På Must känner vi att vår verksamhet är efterfrågad och bidrar till ett säkrare Sverige.

Försvarsmaktsövning *Aurora 17* var en viktig händelse under 2017. Genom *Aurora 17* och andra övningar har vi kunnat stärka Försvarsmaktens förmåga inom underrättelse- och säkerhetstjänst och vi har dragit många lärdomar.

Även om vi har fullt upp i vardagen måste vi också utveckla oss för framtiden. Hela Försvarsmakten arbetar med detta under rubriken Försvarsmakt 2025. På Must har vi under 2017 tagit fram en strategi som bidrag till den gemensamma utvecklingen och som vägledning för vårt interna förändringsarbete. De strategiska målen redovisas i denna årsöversikt.

Under hösten 2017 ruskades vi alla om av skildringar av kränkningar i kölvattnet av *#metoo*, och inom Försvarsmakten under *#givaktochbitihop*. Dessa visade tydligt att det inte duger att vara nöjd med läget. Vi måste fortsätta få bort trakasserier, förebygga kränkande särbehandling, och fortsätta arbeta för ökad jämställdhet och mångfald.

Must kan bara lösa sina uppgifter i samarbete med andra. Inom Försvarsmakten är samarbetsytorna otaliga. Must samarbetar med många myndigheter, och relationen med FRA och Säkerhetspolisen är särskilt bred, djup och god. Must finns representerat utanför Sverige genom försvarsattachéerna och genom vårt stöd till Försvarsmaktens internationella insatser. Därutöver arbetar vi tillsammans med internationella partner.

En kort årsöversikt kan bara visa en liten del av det som Must gör. Vi levererar underrättelser till regeringen och Försvarsmakten, vi leder säkerhetstjänsten i Försvarsmakten, samordnar signalskyddet för totalförsvaret och håller samman Försvarsmaktens utveckling av underrättelse- och säkerhetstjänsten. En stor del av det vi gör måste hållas hemligt, men inte allt. Årsöversikten för 2017 ger en möjlighet för alla att få en uppfattning om vad Must är och att få några ögonblicksbilder ur vår verksamhet.

Gunnar Karlson
Chef för Militära underrättelse- och säkerhetstjänsten

”Must kan bara lösa sina uppgifter i samarbete med andra”


OM MUST

Om Must

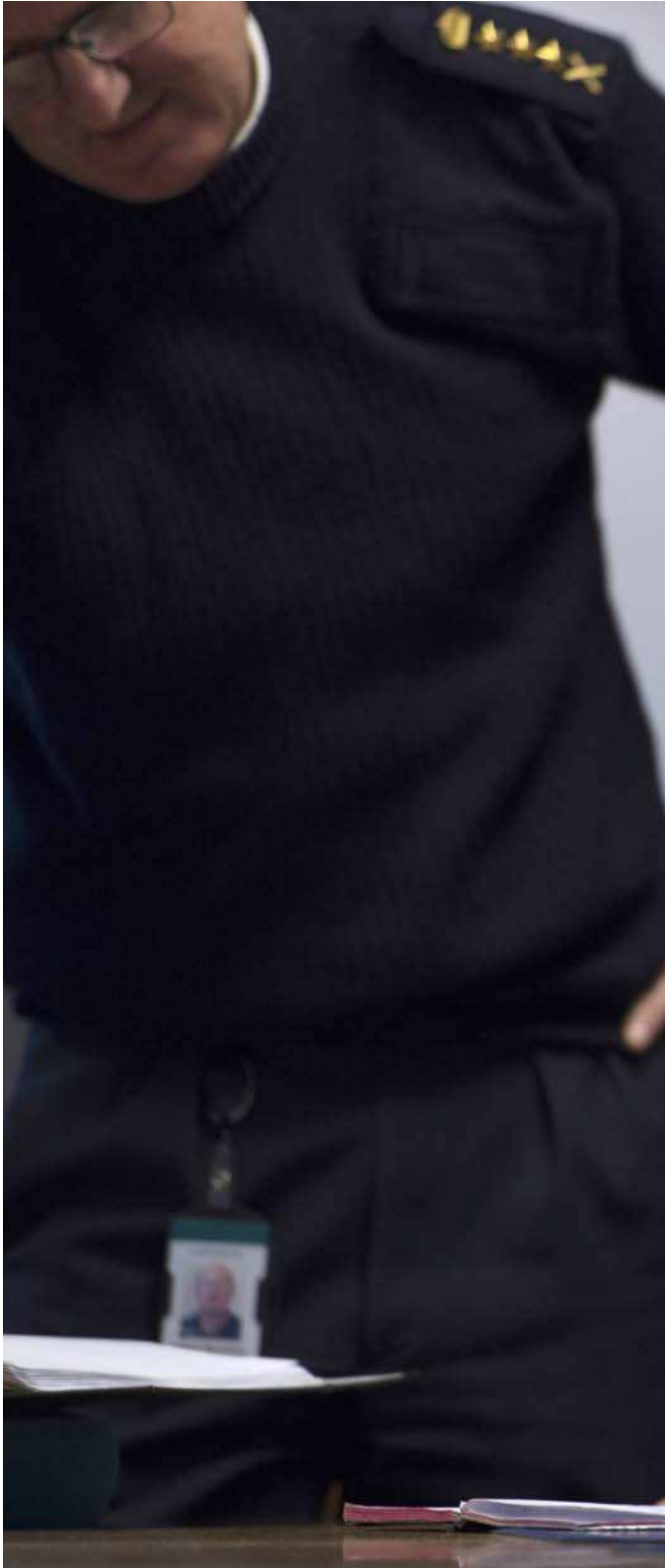
Musts historia

Det svenska försvaret har i århundranden samlat in och sammanställt information om hot mot Sverige och svenska intressen och om förhållanden i utlandet. År 1905, under pågående unionskris med Norge, beslutades att en stående underrättelsetjänst skulle inrättas vid Generalstaben, som var dåtidens motsvarighet till dagens militärhögkvarter. Det är detta årtal som ofta ses som startpunkten för den svenska militära underrättelsetjänsten. Den svenska säkerhetstjänsten grundades först ett årtionde senare och organiserades då även den vid Generalstaben. Dagens militära underrättelse- och säkerhetstjänst (Must) bildades 1994.

Musts uppdrag

Must bedriver försvarsunderrättelseverksamhet och militär underrättelse- och säkerhetstjänst samt leder och utvecklar underrättelse- och säkerhetstjänsten inom Försvarsmakten. Musts verksamhet syftar till att identifiera, bevaka och bedöma yttre hot mot Sverige och svenska intressen i utlandet, till stöd för regeringen och överbefälhavaren. Verksamheten syftar även till att upptäcka, identifiera och möta säkerhetshot som riktas mot Försvarsmakten och Försvarsmaktens intressen i Sverige och utomlands.
I Musts uppdrag ingår även att leda och samordna Sveriges försvarsattachéer.

Vad Must ska och får arbeta med regleras av lagar och förordningar samt av årliga inriktningar från regeringen och överbefälhavaren. Musts huvuduppdragsgivare är därmed regeringen (Regeringskansliet) och överbefälhavaren (Försvarsmakten) men delar av Musts produktion delges även andra mottagare.



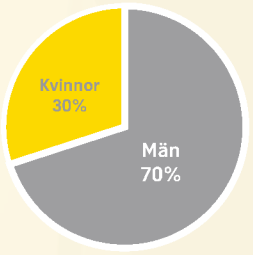
MUSTS ORGANISATION OCH PERSONAL

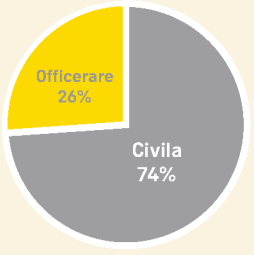
Must är en del av Försvarsmaktens Högkvarter. Musts två verksamhetsområden underrättelsetjänst respektive säkerhetstjänst bedrivs organisatoriskt i Underrättelsekontoret respektive Säkerhetskontoret. Musts verksamhet kräver egna stöd- och ledningsfunktioner, och dessa är samlade under Ledningskontoret. Som stöd för informationshantering finns sedan 2017 Informationshanteringskontoret.

En av Musts främsta tillgångar är våra kompetenta medarbetare. På Must arbetar experter inom olika kompetensområden som t.ex. statskunskap, militärstrategi, språk, ekonomi, teknik, IT, matematik, kryptologi, juridik och HR. Ungefär 30 % av våra medarbetare är kvinnor och 70 % män och en stor andel av vår personal har akademisk examen. Ungefär 74 % av dem som arbetar på Must är civila och 26 % är officerare.

Vi arbetar aktivt för att attrahera och behålla de bästa talangerna oavsett ålder, kön och bakgrund. Vi verkar även för att uppmuntra en kultur av förändring och fortsatt lärande. För att vi även framöver ska kunna lösa våra uppgifter med hög kvalitet och effektivitet ser vi positivt på kompetensutveckling. Must söker regelbundet ny personal och lediga tjänster utannonseras på Försvarsmaktens hemsida.

Must har en egen anslagspost i Försvarsmaktens budget. Utfallet för denna anslagspost 2017 var ca 832 miljoner kr.





UNDERRÄTTELSETJÄNST

”Ge underlag som stöd till svensk utrikes,- säkerhets- och försvarspolitik samt kartlägga yttre hot mot landet”

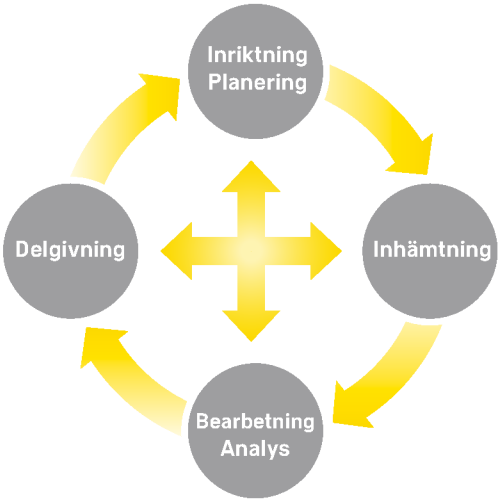
Underrättelsetjänst

Vad är försvarsunderrättelsetjänst?

Musts verksamhet syftar till att ge underlag som stöd till svensk utrikes-, säkerhets- och försvarspolitik samt till kartläggning av yttre hot mot landet enligt lagen om försvarsunderrättelsetjänst och regeringens årliga inriktning. På samma sätt lämnar Must underlag till övriga delar av Försvarsmakten avseende analyser och bedömningar om läget i omvärlden. Underlagen rör bl.a. närområdet, stöd till internationella insatser, stöd till långsiktig förmågeutveckling, underlag till försvarsplanläggning och operativ planering.

Försvarsmaktens behov av underrättelser anges i årlig inriktning som fastställs av överbefälhavaren. En viktig uppgift är att ge förvarning om eventuella hot mot Sverige. De årliga behoven kompletteras efter hand, med hänsyn till utvecklingen i omvärlden.

Verksamheten bedrivs i en underrättelseprocess som omfattar planering/inriktning, inhämtning, analys/bearbetning och delgivning till uppdragsgivarna. *Inhämtningen* genomförs genom flera olika källor så som öppna källor, tekniska och personbaserade källor. Även information från andra länder och organisationer används. *Bearbetning och analys* av information görs av Musts analytiker som också gör underrättelsebedömningar. Sådan bearbetning genomförs för olika geografiska områden till exempel Mellanöstern, eller tematiskt till exempel avseende massförstörelsevapen. *Delgivningen* sker dels genom skriftliga rapporter och underlag, dels genom muntliga föredragningar.



Must strävar både efter att bygga kunskap hos uppdragsgivarna och uppmärksamma dem på nya behov, möjligheter och hot. Must bidrar även med underlag om utvecklingen av stridskrafter i närområdet så att Försvarsmakten och dess förband har en god bild av läget och om eventuella hot.

Must stödjer också de internationella militära insatser som Sverige deltar i. Stödet sker både inför och under insatserna. Musts förbandsdel Nationella Underrättelseenheten (NUE), har personal i insatsområdena. Vid NUE finns även s.k. deskar som analyserar det som inhämtas i insatsområdena. Underrättelser och bedömningar delges både till regeringen och till Försvarsmakten. Stöd kan även ges till chefer i multinationella insatser i insatsområdena. Aktuella områden för NUE under 2017 har bl.a. varit Afghanistan, Irak, Somalia och Mali.

Must deltar också i Högkvarterets arbete med att utveckla Försvarsmaktens förmåga, materielförsörjning och försvarsplanering. Personal ur Must kan stödja genom att beskriva och bedöma utländska aktörers nuvarande och framtida förmåga och materiel.

Underrättelsetjänsten under 2017

Must har under 2017 lämnat omfattande information och bedömningar till uppdragsgivarna, dvs. regeringen (Regeringskansliet) och överbefälhavaren (Försvarsmakten). Efterfrågan har varit stor och rapporteringen har till exempel handlat om hur förhållandena i närområdet har utvecklats och hur de bedöms kommer att utvecklas såväl militärt som försvars- och säkerhetspolitiskt. Rapporteringen om möjliga sätt att bedriva påverkansoperationer och andra former av operationer som inte är av militär art, i fred och i ett så kallat ”gråzonsläge”, har rönt särskilt intresse. Vidare har Must rapporterat om terrorism i kris- och konfliktområden i olika delar av världen och som kan komma att påverka Sverige eller svenska intressen utomlands. Must har även analyserat och delgivit bedömningar om den säkerhetspolitiska och militärstrategiska utvecklingen i flera regioner, exempelvis Mellanöstern och Nordafrika.

Våra försvarsattachéer har rapporterat om den försvarspolitiska utvecklingen i de länder och regioner där de verkar. Vidare har de stöttat besöksutbyten på hög politisk och militär nivå samt hanterat samarbeten mellan Sverige och de berörda länderna.

Aktivitet i vårt närområde

Sveriges närområde har en central plats i Musts uppdrag att följa omvärldsutvecklingen. Både den aktuella situationen i området och de övergripande trenderna är av intresse. Must rapporterar sina observationer och bedömningar till regeringen och överbefälhavaren.

Under 2017 präglades relationerna mellan huvudaktörerna Ryssland och Nato av misstro. Detta gällde inte minst i fråga om utvecklingen i Östersjöregionen, som under en längre tid varit en friktionsyta mellan öst och väst. Huvudaktörerna definierar och verkar för sina säkerhetsintressen på sådana sätt att motsättningar förstärks och samarbetslösningar blir svåra att hitta. Politiska utspel och militära markeringar, till exempel övningar och beredskapskontroller, är vanligt förekommande. Dessa är integrerade delar av aktörernas strategiska kommunikation, vilket tenderar att framkalla ömsesidigt negativa reaktioner.

Den militära aktiviteten i närområdet har ökat under senare år. En uppmärksammad händelse 2017 var utplaceringen av Natos truppförstärkningar i de baltiska staterna och Polen. Detta är en av flera åtgärder från alliansens och USA:s sida för att påvisa enighet och beslutsamhet att stå upp för Natos kollektiva försvarsåtaganden. Kapacitetsuppbyggnaden hos de ryska styrkorna i västra militärområdet, inklusive Kaliningrad, fortsatte också under året. Ombeväpningen av styrkorna i den ryska exklaven uppfattas som en särskild utmaning för Natos handlingsfrihet i stora delar av Östersjöområdet och möjligen också som ett hot mot alliansens planerade robotförsvar i Europa.

Övningsverksamhet var ett centralt inslag i Östersjöregionen 2017. I september genomfördes den ryska strategiska stabs- och ledningsövningen *Zapad-2017*. Inför övningen hade några av Rysslands grannländer varnat för att övningen skulle kunna användas för att genomföra en permanent ombasering av ryska förband, vilket dock inte skedde. Denna diskussion föranledde ryska företrädare att kritisera det som uppfattades som en utbredd russofobi i väst och en felaktig syn på Ryssland som hot. Även Nato har övat i Östersjöområdet under 2017, t.ex. under övningen *BALTOPS*.

Parallellt med *Zapad-2017* i september ägde den svenska övningen *Aurora 17* rum, med deltagande från flera andra länder.

NÄROMRÅDETS HUVUDAKTÖRER

De militära och säkerhetspolitiska huvudaktörerna i Sveriges närområde är Ryssland, USA och ett antal europeiska stater som är Natomedlemmar. EU är också en säkerhetspolitisk aktör i närområdet, inte minst genom sin ekonomiska politik och sina utrikespolitiska ställningstaganden.

Ryssland eftersträvar ökat internationellt inflytande, främst i länderna i forna Sovjetunionen liksom runt Östersjön. De ryska politiska ambitionerna har på senare år åtföljts av en ökad militär förmåga. Rysslands agerande i bl.a. Ukraina och Syrien och förmodligen även mot USA i samband med presidentvalet 2016 visar både på hög ambition och på risktagande.

Ryssland upplever Natos närvaro och aktiviteter i östra Europa som ett hot mot sin nationella säkerhet och motiverar ofta militärreformen med behovet att stärka sitt försvar. Att förhindra att fler länder blir medlemmar av Nato är ett strategiskt ryskt intresse.

Det europeiska och transatlantiska säkerhetssamarbetet har fått förnyad prioritet och i USA har hotet från Ryssland debatterats frekvent. Det pågår ett antal initiativ inom Nato, EU och bilateralt med USA i syfte att höja den militära förmågan i Europa. Det är framför allt de baltiska staterna som upplever att deras säkerhet är utmanad. Dessutom sker försvarssatsningar i flera europeiska länder.

Terrorism

Under 2017 genomfördes flera terrorattentat i Europa, däribland i Sverige den 7 april. En rad attentatsförsök avvärjdes också i planerings- och förberedelsestadiet. Trots att antalet skadade i terrorattentaten under 2017 var lägre i jämförelse med åren 2015 och 2016 när större attentat utfördes i Paris och Bryssel, visade terroristgrupper såsom Daesh på bibehållen avsikt och förmåga att inspirera och understödja attentat i Europa.

År 2017 blev också det år när Daeshs självutnämnda statsbildning i Syrien och Irak, det så kallade kalifatet, föll samman. Likaså lossnade terroristgruppens grepp om vissa städer och områden i länder som Libyen och Filippinerna. Dessa positiva förändringar innebär dock inte att terrorhotet med nödvändighet kommer att minska i närtid, men sannolikt ändra karaktär. Medlemmar i Daesh som lämnat områden som gruppen tidigare behärskat kommer under 2018 att försöka hitta nya platser att verka i och uppehålla sig på. Vissa kommer att försöka återvända till sina hemländer. Daeshs tillbakagång ger troligen al-Qaida och andra våldsbejakande islamistiska grupper möjligheter att växa och förnyas. De väpnade konflikterna i Syrien, Afghanistan, Somalia, Jemen och Libyen pågår alltjämt och dessa konflikter kommer även framöver vara en grogrund för befintliga terroristgrupper att kunna växa och för nya att bildas.

I takt med att terroristgrupper ändrar karaktär och uppträdande, växer kraven på Must som underrättelse- och säkerhetstjänst att följa med i utvecklingen beträffande både teknik och andra förmågor på informationsbearbetningsområdet. I en värld där informationsmängden ständigt ökar och med hotaktörer som agerar gränsöverskridande, är teknisk utveckling, nationell samordning och internationellt samarbete grunden för att kunna behålla vaksamhet och en god beredskap inför hotet från internationella terroristgrupper och nätverk.

Must fortsätter sitt arbete med att delge sina uppdragsgivare underrättelser om utländska förhållanden som påverkar terrorhotet mot Sverige och mot andra länder. Rapporteringen syftar dels till att ge regeringen underlag som stöd för svenska ställningstaganden inom ramen för olika internationella fora, främst inom EU och FN:s säkerhetsråd, dels stödja Säkerhetspolisens uppdrag att förhindra terroristattentat i Sverige. I egenskap av Försvarsmaktens säkerhetstjänst har Must till uppgift att identifiera och avvärja terrorhot mot Försvarsmaktens skyddsvärden såväl hemma som utomlands.

Musts rapportering om förhållanden som påverkar terrorhotet kompletteras även av Musts säkerhetspolitiska och militärstrategiska analys och delgivning till uppdragsgivarna.

Det strategiska samarbetet med Säkerhetspolisen och FRA inom Nationellt centrum för terrorhotbedömning (NCT) är en av plattformarna för Must i det nationella kontraterrorsamarbetet.

NATIONELLT CENTRUM FÖR TERRORHOTBEDÖMNING (NCT)

Nationellt centrum för terrorhotbedömning (NCT) är en permanent arbetsgrupp med personal från Säkerhetspolisen, Försvarets radioanstalt (FRA) och Militära underrättelse och säkerhetstjänsten (Must).

NCT:s uppgift är att göra strategiska bedömningar av terrorhotet mot Sverige och svenska intressen utomlands på kort och lång sikt. NCT gör även analyser av händelser, trender och omvärldsutveckling med koppling till terrorism som berör eller kan komma att beröra Sverige och svenska intressen. Bedömningarna delges delar av Regeringskansliet samt myndigheter som ingår i Samverkansrådet mot terrorism och syftar till att ge tidig förvarning om förändringar som kan påverka hotbilden mot Sverige och svenska intressen och som kan kräva åtgärder. Samarbetet ger större möjligheter att ta tillvara den samlade kompetensen som finns vid Säkerhetspolisen, FRA och Must.

Hybridkrigföring och påverkansoperationer

Påverkansoperationer genomförs av statsaktörer som ett sätt att försöka få inflytande över andra länders säkerhetspolitik. Målsättningen med operationerna är exempelvis att påverka beslut, uppfattningar eller beteenden hos statsledningen, befolkningen eller särskilt utvalda målgrupper som ett sätt för en stat att främja sina egna säkerhetspolitiska mål.

Påverkan sker exempelvis genom att sprida vilseledande eller oriktig information för att skapa förvirring, misstro eller missnöje. Ämnet är inte nytt men fick förnyad aktualitet i samband med utredningarna om eventuell otillbörlig påverkan på presidentvalet i USA 2016.

Aktiviteterna pågår såväl i freds- som i krigstid och är en del i vad som brukar benämnas ”hybridkrigföring”, där dolt uppträdande med olika militära och civila förmågor, vilseledning och subversion ska skapa misstro och osäkerheter hos de som blir utsatta och undergräva försvarsviljan.

Även cyberspionage och cyberattacker används i hybridkrigföringen. Cyberspionage kan användas för att understödja påverkansoperationer eller för att förbereda cyberattacker. Cyberattacker mot civila mål i fred kan användas tillsammans med ekonomiska, diplomatiska och militära medel för att påverka en stats agerande och stabilitet och dess ekonomiska och politiska utveckling. Cyberattacker mot kritisk infrastruktur kan leda till stora kostnader och materiella skador. Den tekniska utvecklingen och vårt ökande beroende av internet ökar samhällets och individens sårbarhet och väntas öka möjligheterna att utnyttja cyberarenan i hybridkrigföring framöver.

Försvarsattachéerna: Försvarsmaktens representanter utomlands

Must ansvarar för Sveriges försvarsattachéer. Dessa är en resurs som stödjer såväl Must och övriga Försvarsmakten som andra myndigheter. Under 2017 har vi haft 26 fasta försvarsavdelningar, med s.k. sidoackrediteringar i ytterligare 34 länder, och fyra resande försvarsattachéer.

Generalmajor Bengt Svensson är sedan drygt tre år chef för den svenska försvarsavdelningen i Washington. Detta är hans andra stationering som attaché i Washington eftersom han mellan 2006-2009 hade rollen som arméattaché. Denna intervju gjordes i januari 2018 när Bengt Svensson var på besök i Sverige.

Försvarsavdelningen i Washington är Sveriges största med fyra utsända attachéer (Bengt Svensson, Per Danielson, Stefan Larsson och Stefan Jönsson), en assistent, en praktikant och en samlokaliserad representant från Försvarets materielverk. Två av attachéerna är även sidoackrediterade till Kanada respektive till Mexiko.

Försvarsavdelningen är en del av den svenska ambassaden som är belägen i House of Sweden vid Potomacfloden. Arbetet sker nära de andra avdelningarna på ambassaden, främst den politiska avdelningen och handelsavdelningen.

Hur ser det dagliga arbetet ut för en attaché i Washington?

Det är alltid ett högt tryck med frekventa möten och informella träffar med andra inom attachékåren och med amerikanska befattningshavare. Vi arbetar med att följa utvecklingen i USA och att stödja i de allt flera bilaterala frågorna som Sverige och USA har. Vi inbjuds ofta att delta i besök vid amerikanska förband. Vi är också mycket engagerade i att planera och ta emot besök från Försvarsmakten, svenska myndigheter och politiska företrädare. Vi och övriga delar av ambassaden har ofta flera svenska besök i veckan. Vi har även märkt av ett ökande intresse från svensk media och från allmänheten för försvarsrelaterade frågor och för utvecklingen i USA.

Hur fungerar samarbetet med attachékåren och med amerikanska befattningshavare?

I Washington arbetar flera hundra internationella försvarsattachéer och andra utsända representanter och det är en intensiv samverkan. Samtidigt är det också konkurrens om att få tillgång till amerikanska befattningshavare och alla länder vill få tillfälle att föra upp sina respektive nationella frågor och regionala intresseområden på dagordningen.

Sverige är en högt respekterad partner och vi upplever att man från amerikanskt håll lägger kraft vid våra gemensamma samarbets- och utvecklingsprojekt och övningar. Sverige och svenska Försvarsmakten har genom ett långsiktigt och hårt arbete fått ett gott renommé som utmärks av bred och djup kompetens och seriositet. Svenskt deltagande i internationella insatser och svensk försvarsindustri imponerar också.

Försvarsavdelningen får ett mycket gott stöd från Must och vi upplever att vi är bra förberedda för att svar upp mot de krav som ställs på oss.

Hur är det att arbeta i Washington?

Washington är en oerhört spännande och dynamisk stad att arbeta i. Hela världens länder, försvarsmakter och intresseorganisationer finns på plats. För mig känns det viktigt att få vara med och göra skillnad för Sverige och Försvarsmakten. Det märks att samarbetet mellan Sverige och USA har fördjupats på senare år och att vi verkligen bidrar till Försvarsmaktens operativa effekt.

Vilken betydelse har den medföljande?

Den medföljande partnern har en oerhört viktig roll. Det är ett lagarbete där jag och min fru stöttar varandra. Utöver de arbetsrelationer som attachéerna bygger under formella möten skapas det även värdefulla relationer och kontakter i informella sammanhang som vid mottagningar och middagar där de medföljande är aktiva. Sådana informella och goda relationer kan hjälpa till att öppna dörrar som annars ibland är stängda.

Vilka utmaningar ser du för försvarsavdelningen de kommande åren?

Den försvarspolitiska debatten i USA har varit ovanligt intensiv under den nya amerikanska administrationen. Politiska motsättningar har tidvis medfört att den federala regeringen har stängt ned sin verksamhet. Den utdragna processen med att få en ny amerikansk försvarsbudget har också skapat problem. Det är en utmaning för oss att analysera vad detta innebär för våra bilaterala samarbetsprojekt och gemensamma åtaganden.

En annan utmaning är att hela tiden, och i alla sammanhang vara målmedveten och att inte ta goda bilaterala relationer för givna. Vi måste ständigt arbeta hårt för att upprätthålla och utveckla vår roll och vårt samarbete.

SÄKERHETSTJÄNST

”Förebygga, upptäcka och motverka säkerhetshot som riktas mot Försvarsmakten och Försvarsmaktens intressen”

Säkerhetstjänst

Vad är säkerhetstjänst?

Den militära säkerhetstjänstens uppgift är att förebygga, upptäcka, och motverka säkerhetshot som riktas mot Försvarsmakten och Försvarsmaktens intressen i Sverige och utomlands.

Begreppet ”den militära säkerhetstjänsten” avser såväl verksamheten som dess organisation och består av säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalskyddstjänst. Med säkerhetshot menas aktörsdrivna hot, dvs. hot bakom vilket det står en eller flera aktörer i form av individer, grupper, nätverk, organisationer eller stater.

Säkerhetshoten indelas i fem övergripande kategorier:

- främmande underrättelseverksamhet
- kriminalitet
- sabotage
- subversion
- terrorism.

De säkerhetsintressen som säkerhetstjänsten skyddar är personal, materiel, information, anläggningar och verksamhet.

Den militära säkerhetstjänsten 2017

2017 var ett händelserikt år för säkerhetstjänsten med såväl förväntade som oväntade händelser. Totalförsvarsplaneringen intensifierades under året och säkerhetstjänsten har varit en del av detta omfattande arbete.

Säkerhetstjänsten behöver hitta lösningar för att möjliggöra totalförsvarsplanering utan att riskera säkerheten. Detta är viktigt eftersom förutsättningarna att kunna hantera sekretess ser olika ut vid olika myndigheter. Säkerhetstjänsten har en roll i att bygga upp kunskap och stödja myndigheterna i att etablera rutiner för att hantera sekretess.

Övningarna *Aurora 17* och *Zapad-2017* gav säkerhetstjänsten flera viktiga erfarenheter. Terrordådet i Stockholm 7 april var en av de händelser som var särskilt påtagliga för oss under 2017. Bland andra uppkomna händelser bör nämnas de som var relaterade till IT-tjänster och outsourcing. Cyberangrepp som *Cloud Hopper* vilka riktas mot IT-tjänsteleverantörer som tillhandahåller molntjänster för myndigheter och företag, samt myndigheters outsourcing av IT-drift är exempel på detta. Förutom hantering av fenomenen i sig, har dessa inneburit ett påtagligt ökat intresse för denna typ av frågor i samhället. Det har också blivit ett ökat fokus i statliga utredningar direkt eller indirekt kopplat till kommande säkerhetsskyddslag.

Hotet från främmande underrättelseverksamhet

Främmande underrättelseverksamhet mot Sverige och Försvarsmakten är en del av normalbilden och bedrivs dagligen året runt. Syftet med inhämtningen är exempelvis att kartlägga Försvarsmaktens personal, bedöma Sveriges operativa förmåga eller den tekniska utvecklingen. Den främmande underrättelseverksamheten sker både i Sverige och från utlandet.

Utländska underrättelseofficerare finns verksamma i Sverige och dessa försöker närma sig personer med tillgång till olika typer av information. En underrättelseofficer har normalt sett en täckbefattning som gör det möjligt för denne att träffa och knyta kontakter med personer i verksamheter denne vill få information om. Exempelvis kan en underrättelseofficer med en befattning vid en handelsrepresentation enklare närma sig representanter från försvarsindustrin.

Utöver personer med en täckbefattning som permanent verkar i Sverige finns det underrättelseofficerare som reser in i landet för att genomföra möten, rekognosera eller stödja annan verksamhet. Det förekommer även att underrättelseofficerare ingår i officiella delegationer som besöker Sverige, exempelvis i syfte att hitta personal som har tillgång till eftertraktad information, ställa specifika frågor eller genomföra olika typer av dold inhämtning.

Exportrestriktioner och sanktioner begränsar tillgången till allmänt tillgänglig information om vissa civila och militära produkter, vilket kan leda till att främmande underrättelsetjänster istället aktivt försöker inhämta information om sådana produkter. För att dölja sin underrättelseverksamhet använder främmande underrättelsetjänster sig av organisationer och företag som bedriver till synes legitim verksamhet. Syftet är exempelvis att möjliggöra uppköp av känslig teknik och dölja den faktiska slutkunden, det vill säga underrättelsetjänsten eller utländsk försvarsindustri.

Inhämtning mot Sverige och svensk personal bedrivs även i andra länder. Exempelvis kan en försvarsmaktsanställds visumansökan inför en utlandsresa vara ett intressant dokument i främmande makts kartläggning. I en visumansökan måste man ofta, utöver personuppgifter, även uppge syfte med resan, arbetsgivare, vistelseort, hur många gånger man har varit i landet i fråga, vem som står värd för besöket samt om man har släktingar i landet, etc. Det kan vara ett lagbrott i landet man reser till att ljuga eller lämna oriktiga uppgifter i sin visumansökan.

Vid internationellt samarbete och vid resor utomlands kartlägger utländska säkerhetstjänster riskbeteenden hos svenska försvarsmaktsanställda. Dessa säkerhetstjänster kan använda denna information i sitt underrättelsearbete, för kompromettering, närmande och trakasserier. Många länder har lagstiftning som tvingar landets egna medborgare eller organisationer i landet att samarbeta med landets underrättelse- och säkerhetstjänst till stöd för denna verksamhet.

Främmande underrättelsetjänster bedriver även omfattande signalspaning och data- och nätverksoperationer. Informationsförluster till främmande makt kan ytterst påverka våra möjligheter att verka i kris och krig.

”Spionen lägger pussel, behåll din bit”

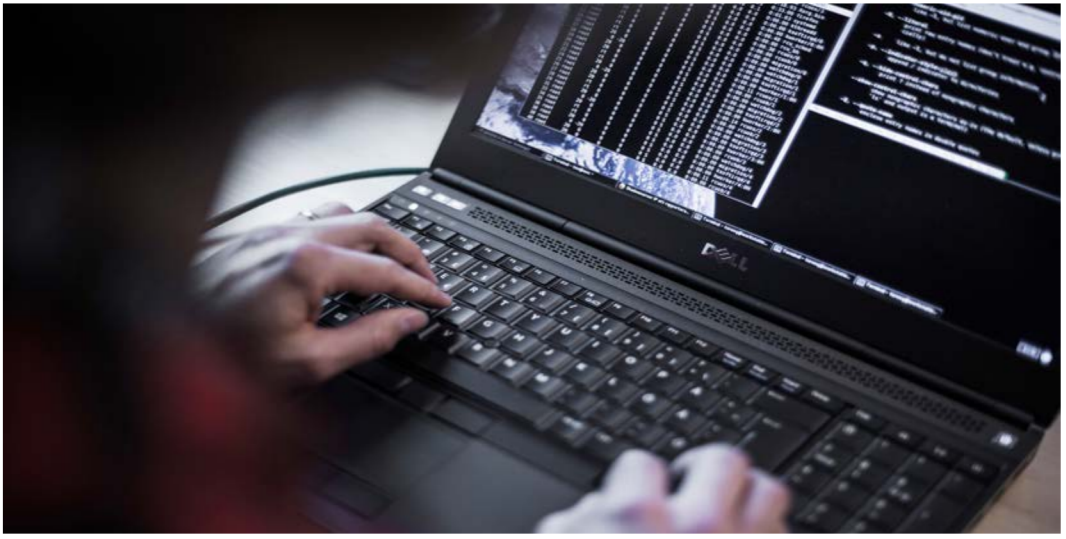
Analys och ansvar vid outsourcing

Inom Försvarsmakten, andra myndigheter och i delar av den privata sektorn finns erfarenheter och goda kunskaper om informationshantering, IT-säkerhet och risker med utkontraktering av verksamhet till leverantörer s.k. outsourcing.

De senaste årens informationsförluster och uppmärksamhet gällande outsourcing har även medfört ett ökat intresse från media och allmänheten samt från flera delar av den privata sektorn. Flera myndigheter och politisk ledning har även gett dessa frågor ökad uppmärksamhet. I debatten är det ofta fokus på frågan om sekretess, det vill säga hur hemlig informationen är. Utöver sekretess behöver man dock även ta hänsyn till annat som också är skyddsvärt: att informationen är tillgänglig när den behövs, att informationen inte förändras på ett otillåtet sätt samt att det går att härleda inträffade händelser.

”Konfidentialitet – Tillgänglighet – Riktighet – Spårbarhet”

I media kan det ibland framställas som att det är outsourcing i sig som är problemet, men det är att förenkla en komplex fråga. Det finns omständigheter där outsourcing, även ur ett säkerhetsskyddsperspektiv, kan vara det bästa alternativet, men det krävs eftertanke och planering. För att lyckas outsourca en verksamhet med bibehållet säkerhetsskydd ska man börja med en säkerhetsanalys som tar hänsyn till alla aspekter; verksamhetens krav, vad som är skyddsvärt, hotbild, sårbarheter, risker och riskhantering. I en säkerhetsanalys bör man även tänka på möjligheter att hantera eventuella förändringar i förutsättningarna så som förändrad hotbild, ändrade ägarförhållanden hos leverantörer och underleverantörer, förändrat omvärldsläge eller för den delen ändrade krav från verksamheten.



Med verksamhetsansvar följer också ett ansvar för säkerhetsskyddet och det gäller oavsett var verksamheten genomförs eller av vem. Enligt säkerhetsskyddsförordningen är det tydligt att säkerhetsskyddet ska kontrolleras. Det är därför viktigt att kontrollaspekter så som rätten att kontrollera skrivs in i avtal vid en outsourcing. För att kunna outsourca ska även den egna organisationens förmåga och kompetens att kontrollera tas med i avvägningen.

”Man kan aldrig kontraktera bort ansvaret. Outsourcing kräver säkerhetskunskap på flera platser i organisationen”

SAMVERKANSGRUPPEN FÖR INFORMATIONSSÄKERHET – SAMFI

Inom ramen för Samverkansgruppen för informationssäkerhet, där Must är Försvarsmaktens medlem, samarbetar myndigheter med särskilt utpekat ansvar för informationssäkerhetsfrågor i samhället.

De myndigheter som ingår är Myndigheten för samhällsskydd och beredskap (MSB), Post- och telestyrelsen (PTS), Försvarets radioanstalt (FRA), Säkerhetspolisen (Säpo), Polismyndigheten, Försvarets materielverk (FMV) och Försvarsmakten. SAMFI genomför årligen konferensen Informationssäkerhet för offentlig sektor.

NATIONELL SAMVERKAN TILL SKYDD MOT ALLVARLIGA IT-HOT – NSIT

Nationell samverkan till skydd mot allvarliga IT-hot (NSIT) är en samverkansform mellan Säkerhetspolisen (Säpo), Militära underrättelse- och säkerhetstjänsten (Must) och Försvarets radioanstalt (FRA). NSIT analyserar och bedömer hot och sårbarheter när det gäller allvarliga eller kvalificerade IT-angrepp mot det mest skyddsvärda nationella intressena. NSIT utvecklar samverkan och genomför aktiviteter syftande till att försvåra för en kvalificerad angripare att komma åt eller skada skyddsvärda civila eller militära resurser.

Under året har delprojekt inom områdena hotanalys, förvarning och upptäckt samt hantering av incidenter genomförts. Arbetet har utförts av projektgrupper med deltagare från de tre organisationerna. Resultaten från de olika projekten används såväl i det tekniska som strategiska arbetet med att försvåra för en kvalificerad angripare att komma åt eller skada svenska skyddsvärda civila eller militära resurser.

Förmågan att hantera allvarliga IT-hot är beroende av personal med rätt kompetens, förmåga att samverka och förmåga att samordna resurser. Kunskap och förståelse hos andra myndigheter och aktörer i samhället inklusive politisk ledning är också avgörande för förmågan. NSIT har lett till ökad förmåga att tillsammans möta komplexa och allvarliga IT-hot.

Säkerhetstjänstens roll vid övningar

För att svensk övningsverksamhet ska kunna genomföras på ett säkert sätt behövs ett gott säkerhetstänkande på alla nivåer både före, under och efter övningar. Must värnar om att säkerhetsaspekterna finns med under hela processen.

Övningar är nödvändiga för att stärka Försvarsmaktens förmåga men de väcker också intresse hos långt fler än de som övar. Vid övningar visar Försvarsmaktens sina förmågor och vilka förbättringsområden som finns. Främmande underrättelsetjänster vill skaffa sig information inom många områden: från politisk beslutsfattning, operativ förmåga, militär ledning, samarbets- och samverkansförmåga, hantering av störningar, hantering av missnöjesyttringar till kunskap om tekniska system.

Därför bedrivs säkerhetstjänst på alla nivåer under övningar. Inom de övande förbanden och i övningsledning finns en säkerhetsorganisation för att övningen ska kunna genomföras på det sätt som är tänkt. För säkerhetstjänsten på central nivå är uppgiften att motverka säkerhetshotande verksamhet och verka för att inte skyddsvärden ska exponeras. För att lyckas med den uppgiften arbetar Must för att klarlägga säkerhetshotande verksamhet, dvs. att hålla uppsikt både över främmande underrättelseverksamhet och vilka metoder som används, samt att analysera vad målsättningen är.

Det är också viktigt att ha ett gott säkerhetstänkande tiden efter en övning då slutsatser om förbandens uppnådda resultat och eventuella brister annars riskerar att exponeras.

Under 2017 var övningsverksamheten ovanligt intensiv, men tack vare bra förberedelser, en väl fungerande säkerhetsorganisation, avdelade säkerhetsförband, genomförda operationer och ett mycket bra samarbete inom säkerhetstjänsten och med Säkerhetspolisen blev resultatet klart godkänt.

”De analyser vi gör och de erfarenheter vi drar av övningar stödjer oss i vår utveckling. Detta ska vi värna om och skydda från obehöriga intressenter”

UTLÄNDSKT INTRESSE FÖR AURORA 17

Främmande makt följer kontinuerligt Försvarsmaktens övningsverksamhet för att bedöma vår operativa förmåga. Inhämtning mot Försvarsmaktens övningar bedrivs över tiden med en rad olika metoder och sensorer. Främmande makt utnyttjar exempelvis både signalspaning och personbaserad inhämtning.

Aurora 17 **var den största övning som Försvarsmakten genomfört på decennier och hade ett stort deltagande av utländska förband från exempelvis Finland, Frankrike och USA. Underrättelseinhämtningen från främmande makt i samband med *Aurora 17* riktades exempelvis mot de internationella enheternas materiel, svensk förmåga att ta emot stöd från utländska förband samt hur lednings- och kommunikationssystem användes.**

Under året, och inte minst under *Aurora 17*, har vi sett en positiv trend vad gäller rapportering från allmänheten av verksamhet som man uppfattar som misstänkt eller onormal.

Systematiskt säkerhetsskyddsarbete

För att värna om de egna skyddsvärdena, eller de som man förvaltar åt någon annan, behövs ett systematiskt säkerhetsskyddsarbete. Genom att arbeta strukturerat med säkerhetsskyddsfrågor minskar risken för att skyddsvärden utsätts för hot eller fara.

En erfarenhet från kontrollerna av Försvarsmaktens systematiska säkerhetsskyddsarbete är att den regelstyrda dokumentationen för säkerhetsplanering, dvs. säkerhetsanalys och säkerhetsplan, inte alltid är tillräcklig. Säkerhetsskyddet måste vara förankrat i verksamheten. Det är viktigt att det görs en god analys av verksamheten och dess olika delar. Skyddsvärden måste identifieras, och utifrån dessa görs ett fortsatt säkerhetsanalys- och planarbete där hotbild, sårbarheter och åtgärder ingår. Säkerhetsanalysen ska alltid uppdateras när verksamheten eller hoten ändras.

Åtgärder för att skydda verksamheten och de identifierade skyddsvärdena kan delas in i två kategorier: de som redan är reglerade i olika regelverk, respektive de som kan beslutas om på lokal nivå. De senare kan innebära t.ex. skärpta restriktioner i tillträde till anläggningar eller områden eller ökad bevakning av vaktstyrka. Vilka åtgärder som behövs kan skilja sig åt beroende på de lokala förutsättningarna.

”Det viktiga är att göra en uppdaterad analys efter de förändrade förutsättningar och att vara medveten om riskerna”

Det bästa säkerhetsskyddet uppnås genom ett systematiskt säkerhetsskyddsarbete där uppdaterade analyser och säkerhetsplaner med planerade och genomförda säkerhetsskyddsåtgärder är en integrerad process med verksamheten och verksamhetsplaneringen.

Vad är ett av Försvarsmakten godkänt krypto?

Enligt säkerhetsskyddsförordningen ska hemliga uppgifter som sänds i ett datanät utanför myndighetens kontroll krypteras med ett kryptosystem som har godkänts av Försvarsmakten. Varför finns det ett sådant krav och vad innebär detta?

Forcering av kryptosystem har haft stor betydelse för händelseförlopp i världshistorien i hundratals år och har det än idag. Kryptoområdet har i de flesta länder en särställning och omgärdas av speciella regelverk. Det finns flera anledningar till detta:

- Ett dåligt konstruerat kryptosystem kan ge stor skada utan att det märks, vilket skiljer krypto från andra IT-säkerhetsmekanismer.
- Om man hittar en brist i ett system kan skadan redan vara skedd. Även om bristen åtgärdas kan all trafik som tidigare har krypterats med det bristande systemet finnas lagrad. Om en obehörig forcerar kryptot kan hemlig information från många år tillbaka komma i orätta händer.
- Länder vill skydda sig själva men även signalspana på andra. Detta innebär att det inte ligger i ländernas intresse att exportera bra system eftersom det skulle kunna försvåra den egna signalspaningen. Detta måste man vara medveten om då man förhåller sig till andra nationers krypton.
- Hela utvecklingsarbetet behöver vara under kontroll. Systemen innehåller så mycket kod att en skicklig, illvillig leverantör skulle kunna lägga in en s.k. ”bakdörr” i systemet utan att granskaren märker det. Detta innebär att det måste finnas ett förtroende både för systemet i sig, leverantören av kryptosystemet och för hela försörjningskedjan.

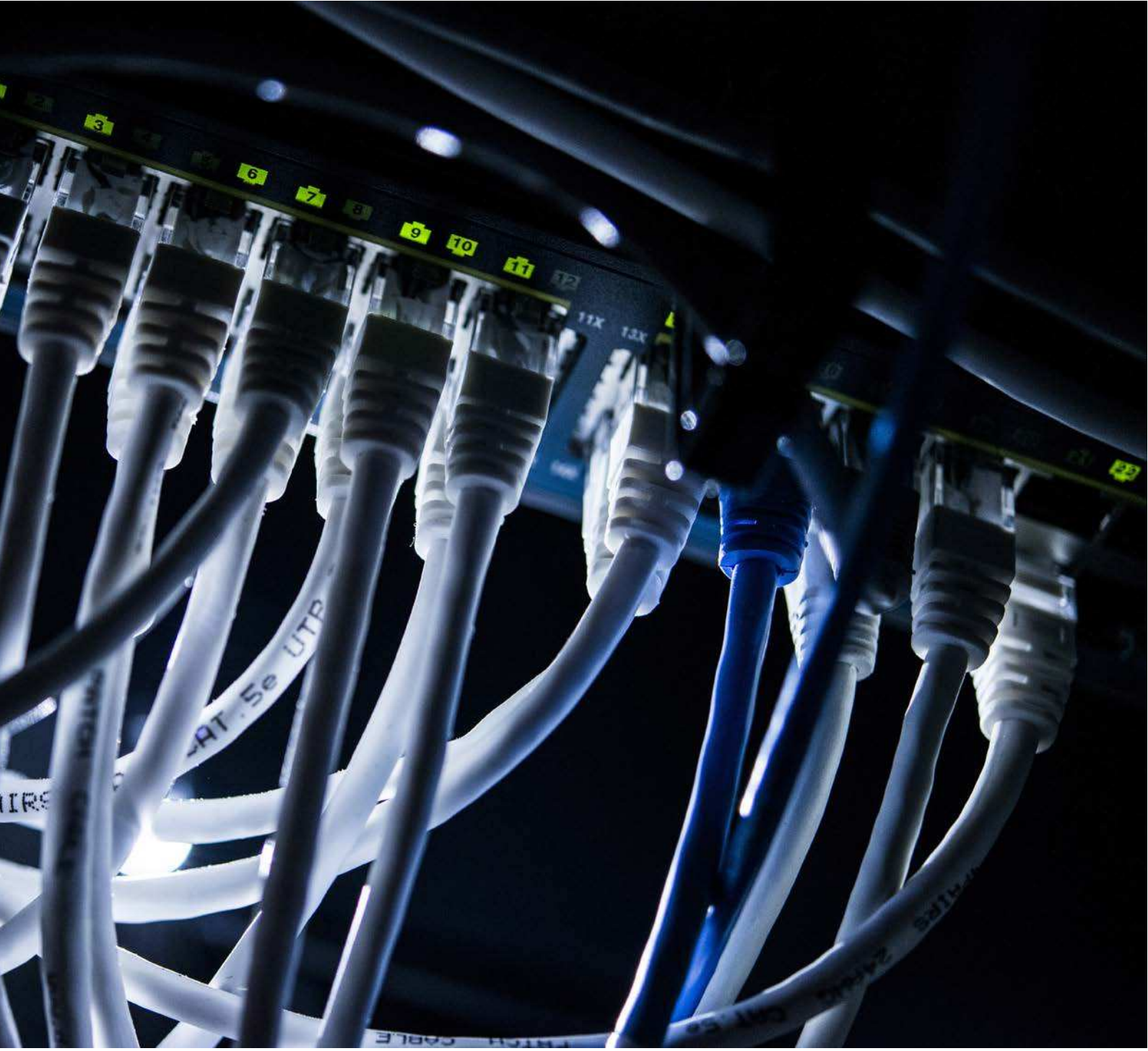
Det är svårt och kostsamt att kravställa, bygga och granska kryptosystem som ska skydda hemlig information. Därför har ansvar och resurser lagts på en myndighet, Försvarsmakten, som har fått uppgiften för hela totalförsvaret. Regeringen har i budgetpropositionen för 2018 fastslagit att krypto är ett nationellt säkerhetsintresse.

Den senaste produkten som har godkänts av Must är ett så kallat höghastighetskrypto, kallat MGDI, som kan skydda information klassad Hemlig/Top Secret mellan två platser.

Utveckling av system för totalförsvarskommunikation

För säker telefonkommunikation på nivån Hemlig/Secret används idag system som inte är anpassade för nya telenät. Dessa system behöver successivt fasas ut och ersättas. En utmaning med övergången till nya system är att det till del krävs en egen infrastruktur som ska kunna användas av hela totalförsvaret.

Som en del i den nya utvecklingen tas ett system fram med en mobil kryptotelefon för Hemlig/Secret, kallat 7411. Den första versionen av denna kommer att ha en traditionell kryptonyckelhantering där användaren i förväg behöver veta i vilken grupp man ska kommunicera. Nästa steg är att tillföra en kryptonyckelserver som gör det möjligt för två parter att kommunicera med unika nycklar mellan varandra.



INFORMATIONSHANTERINGSKONTORET

”Stärka Musts flexibilitet och förmåga att svara upp mot verksamhetskrav på informationshantering och informationssystem”

Informationshanteringskontoret

Vad är Informationshanteringskontoret?

De funktioner som ansvarar för Must-gemensam informationshantering samt planering, utveckling och vidmakthållande av gemensamma IT-system är sedan den 1 januari 2017 sammanslagna till ett nybildat kontor: Must Informationshanteringskontor (IHK). Kontoret arbetar för att stärka Musts flexibilitet och förmåga att kunna svara upp mot olika verksamhetskrav på informationshantering och informationssystem.

För att lösa sina uppgifter inhämtar Must information från en rad olika källor. Stora informationsmängder behöver hanteras och kraven på automatiserade och smarta informationssystem växer hela tiden. I arbetet med att upptäcka, identifiera och möta yttre hot mot Försvarsmakten och Sverige krävs flera olika informationssystem och Must är beroende av ett eget systemstöd. Systemen är oftast dimensionerade för att hantera hemliga uppgifter som är försvarssekretess och som därmed ställer särskilda krav på informations- och IT-säkerhet.

Informationshantering vid Must ställer särskilda krav eftersom vissa aspekter av verksamheten är unika. Hanteringen av systemen behöver kunna fungera såväl i fred som i kris och krig.

Chefen för Informationshanteringskontoret är tillika Must Chief Information Officer (Must CIO), och ansvarar för att inrikta och samordna informationshantering och informationsinfrastruktur vid Must. Kontorets arbetsområde spänner över ett brett fält: allt ifrån att leda och utveckla administrativa processer för informationshantering till att bedriva teknisk utveckling och vidmakthållande av IT-system. Vid kontoret arbetar både fast anställd personal och ett stort antal konsulter. Målsättningen är att successivt växla konsulter mot fast anställd personal.

Under 2017 har ett särskilt fokus varit att etablera Informationshanteringskontorets verksamhet och interna processer för att skapa förutsättningar för fortsatt utveckling av informationshantering och informationssystem.

Planering och samverkan

I Informationshanteringskontorets ansvar ingår att balansera verksamhetens krav på funktionalitet gentemot ekonomisk rationalitet och IT-säkerhet. Kontoret ansvarar även för att företräda Musts samlade intressen på informationshanteringsområdet såväl inom som utanför Försvarsmakten.

Målet är att arbeta nära verksamheten och utveckla funktionalitet som är anpassad till Musts mångskiftande verksamhet. Huvuddelen av planeringsarbetet genomförs av s.k. förvaltningsledare, som arbetar nära övriga kontor på Must. Förvaltningsledarna omsätter de olika systemkraven till en sammanvägd plan som sedan utgör grunden för utveckling och vidmakthållande av systemen.

Utveckling och vidmakthållande av system

Informationshanteringskontoret arbetar med att vidareutveckla applikationer för informationshantering, till stöd för både operativ verksamhet, analys/bearbetning och för administrativ verksamhet.

Musts målsättning är att i så stor utsträckning som möjligt anpassa försvarsmaktsgemensamma generella tekniska lösningar till de behov som Must har. Vid behov kan dock Informationshanteringskontoret bedriva egen utveckling av IT-system och kommunikationslösningar. Detta kan ske t.ex. om det saknas befintliga generella lösningar eller om Must har särskilda verksamhetsbehov. Inom kontoret finns arbetslag med olika typer av teknisk kompetens, exempelvis om tekniska plattformar, nätverk och infrastruktur, operativsystem och program.

Systemförvaltning handlar om att kontinuerligt vidmakthålla den funktionalitet som har utvecklats och att se till att säkerheten i systemet upprätthålls över tid. Detta görs genom att löpande uppdatera systemen och omsätta både hårdvara och mjukvara.

Fortsatt arbete

Must fortsätter att utvecklas i takt med de snabba förändringar som sker inom informationshanteringsområdet. Detta för att kunna dra nytta av möjligheter, men även för att kunna hantera sårbarheter. Must ska bygga vidare på etablerade samarbeten och utveckla nya för att skapa bästa möjliga förutsättningar för att kunna möta framtida utmaningar.

Förvaltningsledaren tolkar behoven och hjälper till att hitta lösningar.

Björn-Erik arbetar som förvaltningsledare och har varit på Must i 9 år. Han har tidigare arbetat med IT-frågor i näringslivet och har en bakgrund som officer.

Vad gör man som förvaltningsledare?

Jag stödjer chefer på Musts säkerhetskontor med informationshanteringsfrågor på ett verksamhetsnära plan. Jag arbetar med hur IT ska stödja informationshanteringen och kontorets kärnverksamhet. Jag jobbar nära de medarbetare som axlar ett tyngre ansvar och har ett större engagemang för informations- och IT-frågorna, de s.k. superanvändarna. De tillför kunskap, ned till minsta beståndsdel, om informationshanteringen inom sina respektive områden. Jag får sedan stöd från de mer tekniknära befattningshavarna på Informationshanteringskontoret med att ta fram tekniska lösningar.

Vilka utmaningar ser du med informationshanteringen på Must?

IT kan vara svåröverskådligt och komplicerat i sig och i kombination med sekretess blir det ofta utmaningar som man måste ta sig an. Det pågår flera strategiska projekt i Försvarsmaktens regi som kommer att ha stor påverkan på Musts informationshantering och det känns viktigt att slutresultatet blir bra för Musts hela verksamhet. I detta har förvaltningsledarna en viktig roll, tillsammans med linjechefer och superanvändarna ute på kontoren.

I alla stödjande organisationer är kundnöjdhet viktig. Försvarsmaktens medarbetarundersökning ger oss värdefull feedback och ger oss mål att sträva mot.

Vad är det bästa med arbetet?

Det är väldigt roligt att arbeta verksamhetsnära med experterna ute på de andra kontoren och att vara med och bidra till Musts utveckling.

VILKA GRANSKAR MUST?

Vilka granskar Must?

Att följa och respektera lagar och förordningar är en självklarhet för Must, som måste ha uppdragsgivarnas och allmänhetens förtroende. På grund av behovet av att hemlighålla vår förmåga och vår information för utländska underrättelseaktörer får obehöriga ingen detaljerad insyn i Musts verksamhet. Musts rapporter och säkerhetsskyddsåtgärder är av samma skäl normalt belagda med sekretess.

För att säkerställa att Must följer givna lagar, förordningar och direktiv finns externa inspektionsorgan som granskar verksamheten. Deras granskningar utgör samtidigt ett stöd för Must eftersom de tillför viktiga juridiska perspektiv på verksamheten. Granskningarna föregås alltid av ett omfattande förberedelsearbete i syfte att ge granskande myndigheter så bra underlag som möjligt.

Statens inspektion för försvarsunderrättelseverksamheten

Under 2017 har Must vid flera tillfällen granskats av Statens inspektion för försvarsunderrättelseverksamheten (SIUN), som bl.a. kontrollerat att verksamheten bedrivits i enlighet med lagen om försvarsunderrättelseverksamhet. SIUN har även granskat att Försvarsmaktens personuppgiftsbehandling utförs enligt Lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. (www.siun.se)

Datainspektionen

Även Datainspektionen (DI) kontrollerar att Must följer Lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt även den allmänna Personuppgiftslagen. Must har under 2017 fortsatt arbetet med att åtgärda förelägganden och påpekanden från tidigare år. (www.datainspektionen.se)

Riksrevisionen

Musts ekonomiska redovisning och efterlevnad av uppställda förvaltningskrav granskas av Riksrevisionen och genom försvarsmaktsinterna processer. (www.riksrevisionen.se)

Dialog med uppdragsgivarna

En kontinuerlig dialog med Regeringskansliet, främst med Enheten för samordning av försvarsunderrättelsefrågor (SUND) på Försvarsdepartementet, säkerställer att underrättelseprodukterna motsvarar regeringens förväntningar. Motsvarande dialoger sker med övriga staber och ledningar i Högkvarteret för att säkerställa överbefälhavarens beställningar.

Lagarna som specifikt styr Musts verksamhet är Lagen (2000:130) om försvarsunderrättelseverksamhet, Säkerhetsskyddslagen (1996:627) samt Lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Bland annat regleras frågor om sekretess och säkerhetsskydd i lagstiftningen.

NATIONELLT SAMARBETE OCH STÖD TILL TOTALFÖRSVARET

”Ökad samverkan har förbättrat vår beredskap och förmåga”


FÖRSVARSMAKTEN

Nationellt samarbete och stöd till totalförsvaret

Utöver den dagliga samverkan med övriga Försvarsmakten har Must även ett nära samarbete med myndigheter och andra delar av totalförsvaret.

Som tidigare nämnts ingår Must och Musts medarbetare i flera formella arbetsgrupper som exempelvis SAMFI, NSIT och NCT. Musts ledning har även regelbundna möten med flera myndighetschefer bl.a. inom ramen för Samverkansrådet mot terrorism. Samarbetet med Försvarets radioanstalt (FRA) samt med Säkerhetspolisen är särskilt väl utvecklat.

Must deltar även i flera offentliga sammanhang, exempelvis Folk och Försvars årliga rikskonferens i Sälen, och Almedalsveckan. Must utbildar även berörda inom totalförsvarets olika delar i signalskyddsfrågor och stödjer på så sätt myndigheters och andra samhällsfunktioners långsiktiga säkerhetsarbete.

Denna nationella samverkan har ökat de senaste åren och har förbättrat vår beredskap och förmåga att tillsammans med andra bygga det nya totalförsvaret.

Anders Thornberg, fd. Generaldirektör Säkerhetspolisen. Gunnar Karlson, Chef Must. Dag Hartelius, Generaldirektör FRA. Foto: Björn Tesch.

MUST STRATEGI

”Möjliggöra en strukturerad och medveten påverkan på framtiden”

Must strategi

Must strategi 2025 fastställdes av Chefen för Must i januari 2018 och arbetet med att införa denna strategi har påbörjats inom organisationens olika delar.

Strategin är ett uttryck för hur Must bidrar till Försvarsmaktens förändringsarbete, FM 2025, och syftar till att möjliggöra en strukturerad och medveten påverkan på framtiden.

Strategin ska utgöra grunden för Musts prioriteringar under perioden fram mot 2025. Den ska även vägleda Must i beslut på alla nivåer och ge en ram för hur vi planerar och genomför vår verksamhet.

Fem strategiska mål

1

Utveckla Musts roll

Delta aktivt och genomföra bred delgivning inom totalförsvaret.
Ta ett vidgat ansvar för samhällets säkerhetsskydd.
Utveckla samarbetet inom det svenska underrättelse- och säkerhetssamhället.

2

Påverka våra externa förutsättningar

Verka för högt förtroende och respekt för Must.
Driva särskilt utvalda nationella och internationella samarbeten.
Påverka och använda Musts juridiska förutsättningar.

3

Utveckla professionen

Utveckla en generell grundförståelse för underrättelse- och säkerhetstjänst samt för teknikens betydelse hos alla anställda.
Attrahera och behåll de bästa talangerna.

4

Stärka anpassningsförmågan

Uppmuntra en kultur av förändring och lärande.
Stärka förmågan att verka i kris och krig.

5

Utnyttja teknikens fördelar

Genomföra verksamhetsnära utveckling.
Genomföra en genomgripande modernisering av Musts verksamhetsstöd.

Ett säkrare Sverige i en osäker värld

FÖRSVARSMAKTEN

107 85 Stockholm, tel 08-788 75 00
www.forsvarsmakten.se