FÖRSVARSHÖGSKOLAN

C-UPPSATS

Författare Major Niclas Holmquist	**Förband** S 1	**Program** ChP T 03–05
FHS handledare Tekn.dr. Per Hyberg och kn/aing Magnus Astell		
Uppdragsgivare FHS, Krigsvetenskapliga institutionen	**Beteckning** 19 100:2068	**Kontaktman** Militärtekniska institutionen

Elektronisk krigföring i lågintensitetskonflikter – sensorsamverkan för effektivare insatsförband

Försvarsmaktens tekniska system idag är starkt präglade av kalla krigets optimering mot ett anfall från en reguljär stormakt, varför förmågan avseende elektronisk krigföring i dagens moderna lågintensitetskonflikter är starkt begränsad.

Uppsatsens syfte är att klarlägga om tillförsel av moderna högteknologiska hjälpmedel för elektronisk krigföring ger några avgörande taktiska fördelar för våra internationella insatsförband när de ska verka mot icke-reguljära aktörer i dagens moderna lågintensitetskonflikter.

Uppsatsen visar på betydande brister hos våra insatsförband och att det är utomordentligt viktigt att tillföra dom signalspanings- och störförmåga mot olika sambandssystem. Vidare är det inom den grundläggande förmågan underrättelser/information vi har mest att vinna på att tillföra nya tekniska förmågor avseende elektronisk krigföring. Ledstjärnan i allt detta är att kombinera flera olika typer av underrättelseförmågor såsom SIGINT, IMINT, HUMINT, OSINT inklusive direktriktat stöd från olika underrättelseorganisationer hemma i Sverige. Den elektroniska krigföringen med sina olika tekniska sensorer är tveklöst en mycket viktig delkomponent i detta sammanhang. Det finns därför alla anledning att se på tillförseln av nya tekniska förmågor till våra insatsförband som en helhet hellre än som enskilda autonoma system.

Bilaga 1: Förkortningar
Bilaga 2: Abstract in English

Nyckelord: Asymmetri, elektronisk krigföring, gerillakrigföring, lågintensitetskonflikter, sensorfusion, telekrigföring, terrorism, underrättelsetjänst.

Innehåll

Kapitel 1
INLEDNING

Sverige stod under hela kalla kriget neutralt mellan de två stormaktsblocken. Det har dock sedan Sovjetunionens sönderfall framkommit att det inte var någon tvekan om vem som egentligen var fienden. All planering som Försvarsmakten genomförde gick ut på att möta en sovjetisk invasion österifrån. De svenska officerarna har i generationer vetat exakt vilken uppgift de skulle lösa om ryssen kom. De visste exakt på vilken strand, i vilket skogsparti, på och över vilket hav de skulle möta sin fiende. De visste också exakt hur han var organiserad, vilken taktik han skulle använda mot dom och vilka stridsvagnar, jagare och stridsflygplan de skulle mäta sina krafter med. Verkligheten idag är en helt annan. Vi vet knappt var i världen nästa konflikt uppstår, om motståndaren är en armé eller paramilitära kriminella ligor, vilken utrustning han har, hur han är organiserad eller vilken taktik han praktiserar.

Den nya inriktningen med ett ökande svenskt deltagande i internationella insatser innebär att risken för att komma i kontakt med icke-reguljära extremister av olika slag ökar.[1] Det är sannolikt att våra insatsförband ställs i en situation där vi tvingas att verka i en för oss ogynnsam terräng som innebär att vi måste välja mellan omfattande egna och civila förluster eller låta motståndaren löpa. Vi får alltså svårt att använda våra militära vapensystem på ett effektivt sätt, vilket leder till att vår överlägsna militära kapacitet blir mindre relevant.[2]

1.1 Problemställning

Problemformulering

De hot vid lågintensitetskonflikter som idag är en realitet är mycket diversifierade och väldigt specifika för varje enskild konflikt. Ny teknik blir allt mer tillgänglig till en överkomlig kostnad, särskilt informationsteknologi. Det blir allt vanligare att icke-reguljära aktörer exempelvis använder högteknologiska civila kommunikationssystem, mot vilka våra insatser är omgärdade av juridiska spörsmål som berör både personlig integritet och kommersiella intressen. Försvarsmaktens tekniska system idag är starkt präglade av kalla krigets optimering mot ett anfall från en reguljär stormakt, varför förmågan avseende elektronisk krigföring i dagens lågintensitetskonflikter är starkt begränsad.

Syfte

Syftet med den här uppsatsen är att klarlägga om tillförsel av moderna högteknologiska hjälpmedel för elektronisk krigföring ger några avgörande taktiska fördelar för våra internationella insatsförband i lågintensitetskonflikter.

---

[1] Jakobsson, Johan (2004), *Terrorism och extremism som hotbild* (Stockholm: Totalförsvarets forskningsinstitut), s. 41.

[2] Rekkedal, Nils Marius (2002), ”Nye trender innen krigføringen: Men kriger er i dag som i tidligere tider, vanskelige å forutse”, Baudin, Arne; Hagman, Thomas och Ångström, Jan (eds.), *En ny medeltid? En introduktion till militärteori i lågintensiva konflikter* (Stockholm: Försvarshögskolan), s.36.

Frågeställningar

Följande centrala frågeställning är styrande för undersökningen:

1. Vilka taktiska fördelar kan identifieras om nya tekniska förmågor för elektronisk krigföring tillförs våra insatsförband i moderna lågintensitetskonflikter?

Följande delfrågeställningar ska bidra till att svara på den centrala frågeställningen:

2. Vilka medel och metoder som nyttjar det elektromagnetiska spektret eller datornätverk har använts operativt av icke-reguljära aktörer i lågintensitetskonflikter under perioden 1991–2004? Med operativt menas de medel som varit nödvändiga för att kunna planera och genomföra väpnade insatser. Med medel menas materielsystem och tekniska utrustningar.

3. Vilka förmågor för elektronisk krigföring har Försvarsmaktens förband i internationella insatser idag och vilka brister kan, jämfört med lågintensitetshoten, identifieras?

4. Vilka tekniska förmågor för elektronisk krigföring mot kartlagda lågintensitetshot och som är operativt realiserbara senast 2010 kan identifieras och därmed komplettera identifierade brister? Med operativt realiserbara senast 2010 menas vilken teknisk utrustning som utan vidare forskning kan upphandlas och integreras i operativa militära tekniska system inom en femårsperiod.

1.2 Avgränsningar

1991 är en naturlig startpunkt. Det är i och med Sovjetunionens fall och kalla krigets slut som lågintensitetskonflikterna ökar i antal.[3] När den ena av de två supermakterna förlorar sin maktposition försvinner den bipolära världsordningen. Locket som dämpat inomstatliga konflikter i skuggan av det kalla kriget försvinner och nya hot ges en ökad genomslagskraft.[4] Bedömningar av hur teknikutvecklingen påverkar hoten vid **framtida** lågintensitetskonflikter blir lätt spekulativa i den här typen av uppsatser eftersom sådana bedömningar av hög kvalitet är omgärdade av sträng sekretess. Sekretess skapar problem för hela examinationsprocessen och undviks därför. Dessutom förefaller även bedömningar av hur teknikutvecklingen påverkar förmågorna i våra insatsförband i framtiden också bli spekulativa. Anledningen till detta är att förändringarna i Försvarsmakten påverkas av många olika osäkerhetsfaktorer såsom politiska prioriteringar, minskande ekonomi och kraftig omställning från plattformsbaserat till nätverksbaserat försvar. Uppsatsen stannar alltså i nutid och svarar på frågan om all den moderna högteknologi som är tillgänglig idag, och som är möjlig att göra militärt operativ före 2010, skulle ge några taktiska fördelar.

---

[3] Rekkedal, ”Nye trender innen krigføringen: Men kriger er i dag som i tidligere tider, vanskelige å forutse”, s. 23.
[4] Jakobsson, *Terrorism och extremism som hotbild*, s. 12 och 57.

För att undvika att spekulera i möjlig framtida hotbild behandlas endast de hot och medel som de facto har använts av icke-reguljära styrkor i de senaste lågintensitetskonflikterna.

När det gäller rumsavgränsningen fokuserar uppsatsen på de svenska insatsförbandens förmågor vid internationella fredfrämjande insatser i lågintensitetskonflikter, varför försvar mot ett väpnat angrepp mot Sverige inte avhandlas. De lågintensitetshot som kan vara möjliga mot Sverige skiljer sig dock inte från dem som är aktuella i övriga världen. Däremot kommer denna typ av hot att analyseras utifrån de moderna lågintensitetskonflikterna som förekommit i världen sedan Sovjetunionens sönderfall.

Krigföringsförmåga kan indelas i fysiska, konceptuella och moraliska faktorer. De fysiska består av stridskrafterna, dess materiel, personal och övriga resurser. De konceptuella faktorerna består av doktriner, policy och dylikt. De moraliska faktorerna består av chefernas ledarskap, stridskrafternas vilja och värdegrund.[5] Denna uppsats behandlar i huvudsak endast de materiella delarna av de fysiska faktorerna vilket ger ett djup i analysen istället för bredd. Det bredare angripssättet riskerar göra slutsatserna för generella och intetsägande. Med de materiella delarna avses tekniska lösningar och utrustningar med specifika förmågor till elektronisk krigföring. Uppsatsen avser alltså inte ge svar på organisatoriska frågor eller ta ställning i val av plattformar. Dock kommer de att omnämnas i de sammanhang där de förekommit i verkligheten.

Elektronisk protektion omfattar skydd av egna system mot en motståndares telekrigföring och dennes exploatering av **våra** system, exempelvis vår kryptering av data och bandspridning av kommunikationssignaler. Dator- och nätverks-försvar (CND[6]) omfattar försvar och skydd av **våra** informationssystem, datorer och nätverk av dessa från en motståndares offensiva åtgärder. I denna uppsats ligger fokus på motsatsen: Att exploatera **motståndaren** och dennes system exempelvis med underrättelsesensorer, elektronisk stödverksamhet, elektronisk attack, dator- och nätverksexploatering (CNE), eller dator- och nätverksattacker (CNA). Därför avhandlas inte elektronisk protektion och CND i denna uppsats.

Mörkerutrustningar på gruppnivå är idag redan så implementerade och spridda att de inte avhandlas i denna uppsats.

HPM-vapen anses inte kunna vara operativa inom tidsavgränsningen och avhandlas därför inte i denna uppsats.

1.3 Antaganden

Interoperabilitet är en funktion av gemensamma stabsprocedurer, språk och tekniska lösningar vilka mer eller mindre bidrar till förmågan att lösa uppgiften i samverkan med andra nationers staber och förband.[7] Detta krävs för att våra insatsförband ska kunna verka i multinationella operationer, främst med nationer i EU och Nato. Förband och staber ska alltså fungera tillsammans tillfredställande avseende materiel, personal och metoder. Våra insatsförbands förmåga till interoperabilitet antas vara god.

Politiska överväganden och konsekvenser antas gå i riktning mot att anskaffning av nya tekniska förmågor för elektronisk krigföring till våra

[5] Försvarsmakten (2002), *Militärstrategisk doktrin 2002* (Stockholm: Försvarsmakten), s. 75.
[6] Förklaring av samtliga förkortningar återfinns i bilaga 1.
[7] Försvarsmakten, *Militärstrategisk doktrin 2002*, s. 116.

insatsförband kan genomföras. Härmed antas att de ekonomiska förutsättningarna för anskaffning föreligger.

Juridiska överväganden och konsekvenser i form av regler för insats (Rules of Engagement, ROE) antas inte sätta några hinder för användande av tillförda tekniska förmågor.

1.4 Centrala begrepp

Elektronisk krigföring

Verksamheten omfattar;

- Bekämpning, förvanskning eller exploatering av motparters inhämtning, bearbetning eller delgivning av information.
- Förhindrande av motståndarens bekämpning, förvanskning eller exploatering av vår inhämtning, bearbetning eller delgivning av information.

Syftet är att skydda och försvara egna insatser, samtidigt som motståndarnas försvåras eller förhindras.

Elektronisk krigföring omfattar telekrigföring, CNO (Computer Network Operations) och övrig signalkrigföring.

Telekrigföring är verksamhet som utnyttjar det elektromagnetiska spektret för att bekämpa, förvanska eller exploatera motparters inhämtning, bearbetning eller delgivning av information och skyddar för oss ogynnsamt utnyttjande av det elektromagnetiska spektret. Telekrigföring består av elektronisk attack, elektronisk stödverksamhet och elektronisk protektion.

CNO (dator- och nätverksoperationer) är verksamhet som utnyttjar datorer och nätverk av datorer samt dess delsystem för offensiva och defensiva aktiviteter. Syftet är att skydda och försvara egen verksamhet på informationsarenan samtidigt som en motståndares verksamhet försvåras eller förhindras. CNO består av dator- och nätverksförsvar (Computer Network Defence, CND), dator- och nätverksexploatering (Computer Network Exploitation, CNE), och dator- och nätverksattack (Computer Network Attack, CNA).

Övrig signalkrigföring omfattas av verksamhet som **inte** är telekrigföring eller CNO, men som till sin natur är likartade och därför kan inordnas under elektronisk krigföring. Exempel på områden är hydroakustik, akustik, magnetism och seismologi. Syftet med övrig signalkrigföring är att likt telekrig och CNO exploatera området för att medge eget utnyttjande samtidigt som man strävar efter att hindra motparten att utnyttja detsamma.[8]

De sex grundläggande förmågorna

Det som tidigare klassiskt benämndes *stridens grunder* inarbetades först i de militära basfunktionerna i Försvarsmaktens militärstrategiska doktrin från 2002. Basfunktionerna användes för att beskriva krigföringsförmåga och bestod av ledning, verkan, rörlighet, skydd, underrättelser och uthållighet.[9] I den nya doktrinen för markoperationer från 2004 har dessa sammanförts och utvecklats till *sex grundläggande förmågor* där basfunktionen underrättelser har utökats till den

[8] Försvarsmakten (2003), *Försvarsmaktens grundsyn informationsoperationer, IO* (Stockholm: Försvarsmakten, utkast, fastställt för tillämpning 2003-12-11), s. 17–18.
[9] Försvarsmakten *Militärstrategisk doktrin 2002*, s. 76–77.

grundläggande förmågan underrättelser **och** information. Dessa sex förmågor samverkar och stödjer varandra i ett system under genomförandet av strid. De ska hanteras som en tankemässig modell för att åstadkomma de samordningsvinster som uppstår när de samverkar för att uppnå ett mål. Förmågorna hjälper oss också att tänka i termer av vilken effekt vi eftersträvar under en insats. Detta resulterar i underlag för hur förband med sina materielsystem bör kombineras, samordnas och användas vid insats.[10]

Taktisk fördel

Taktisk fördel representerar den teoretiska definition som ska operationaliseras i uppsatsen. Fördel är liktydigt med gynnsam faktor i betydelsen gynnsam följd, synonymt med gagn i betydelsen gynnsam inverkan på viss verksamhet.[11] Med begreppet *taktisk fördel* menas i denna uppsats gynnsam inverkan på de svenska insatsförbandens taktiska verksamhet vid deltagande i internationella insatser. Inverkan kan även vara indirekt av operativ eller strategisk karaktär. Den gynnsamma inverkan kan vara av tre huvudtyper.

1. Ökning av en eller flera av de sex grundläggande förmågorna.
2. Ökning av egna alternativa taktiska handlingsmöjligheter och därmed ökad flexibilitet och robusthet. Detta kan omvänt tolkas som motverkad degradering av taktisk förmåga.
3. Möjlighet till nya kombinationer av olika sensor- och/eller verkanssystem som sätter en motståndare i en mycket svår valsituation, ett dilemma, även kallat kombinerade vapen (Combined Arms).

Insatsförband

Insatsförband är förband och resurser avsedda för att genomföra uppgifter inom ramen för någon eller några av Försvarsmaktens uppgifter. För dessa förband gäller:

- De är kompletta, färdigutbildade förband med personal och materiel.
- Förbanden har 0–90 dagars beredskap.
- Förbanden är underställda en operativ/taktisk chef.
- Personalen är anställd eller har kontrakt och är krigsplacerad i förbandet, alternativt är i slutskedet av sin utbildning.
- Personalen kan vara i tjänst vid förbandet, hemförlovad med beredskap och krav på regelbunden tjänst eller hemförlovad med kontrakt för eventuell mission.
- Insatsförbanden kan också undantagsvis vara resurser ur grundorganisationen, som under viss tid och särskilda omständigheter avdelas för att lösa specifika uppgifter.[12]

---

[10] Försvarsmakten (2004), *Doktrin för markoperationer – 2004* (Stockholm: Försvarsmakten), s. 15–16.
[11] Språkdata Göteborgs universitet (1995), *Nationalencyklopedins ordbok* (Höganäs: Bra böcker AB), första bandet, s. 477 och 518.
[12] Försvarsmakten (2003), *Årsrapport från perspektivplaneringen 2002–2003; Målbildsinriktningar inför Försvarsbeslut 2004 – rapport 7* (Stockholm: Försvarsmakten), s. 52–53.

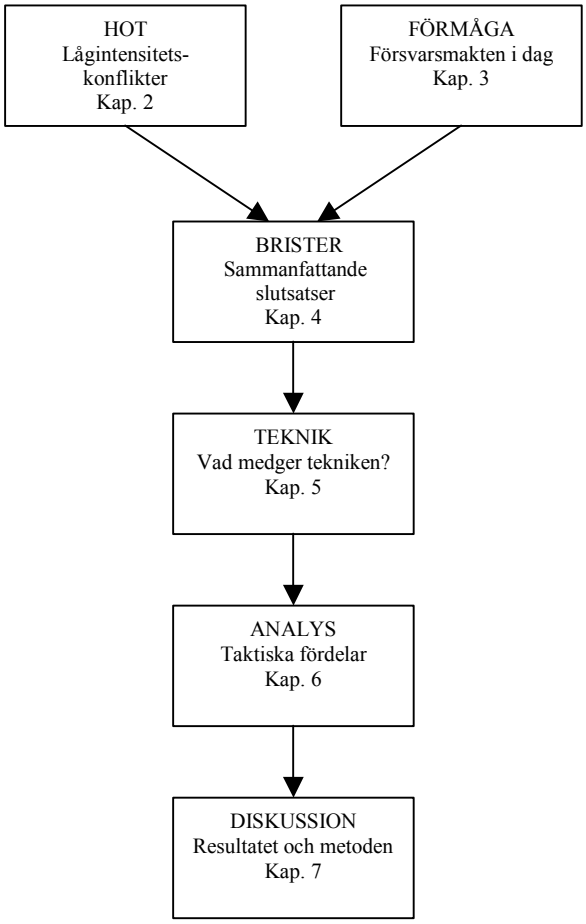
Lågintensitetskonflikter

Begreppet beskrivs och definieras i kapitel 2 nedan.

1.5 Tillvägagångssätt

Uppsatsen betraktar problemställningen från två olika perspektiv, det krigsvetenskapliga och det militärtekniska. De krigsvetenskapliga glasögonen sätter fokus på att beskriva karaktären på de hot som icke-reguljära aktörer utgör i moderna lågintensitetskonflikter. De militärtekniska sätter fokus dels på att beskriva våra insatsförbands förmågor i internationella insatser idag, dels på att undersöka vilka nya tekniska förmågor de kan och bör tillföras för att bättre kunna verka mot de icke-reguljära hoten. Uppsatsen avslutas med att sammanväva de två perspektiven och dra slutsatser om vilka taktiska fördelar nya tekniska förmågor ger våra insatsförband när de ska verka i dessa moderna lågintensitetskonflikter.

Arbetet har bedrivits som en beskrivande studie med förändringsstrategi. Tiden används som jämförelsepunkt genom att undersöka förändring mellan förmågor idag och möjliga förmågor i nära framtid, vilka kan göras operativa inom en femårsperiod. Uppsatsen har följt den övergripande metod som beskrivs i figur 1. Kapitel 2 inleds med en krigsvetenskaplig grund som i huvudsak beskriver de moderna lågintensitetskonflikternas uppkomst, indelning och allmänna karaktär. Därefter ska ett antal fallstudier av utvalda lågintensitetskonflikter undersökas i syfte att mer detaljerat identifiera förekommande hot och medel som får konsekvenser för vår förmåga till elektronisk krigföring. Nästa kapitel inleds med en beskrivning av omställningen av Försvarsmakten från invasionsförsvar till insatsförsvar samt vilka konsekvenser detta fått för vår operativa förmåga i allmänhet. Därefter undersöks vilka förmågor avseende elektronisk krigföring som de svenska insatsförbanden har idag. I kapitel 4 jämförs de identifierade lågintensitetshoten med befintliga förmågor. Sammanfattande slutsatser dras om vilka brister i förmågor som har identifieras. Nästa kapitel beskriver vilken befintlig teknik som är möjlig att göra operativ inom en femårsperiod för att komplettera insatsförbandens bristande förmågor. Här fokuseras på sådan teknik som kan möta de identifierade hoten från icke-reguljära aktörer. I kapitel 6 genomförs en undersökning i syfte att identifiera *taktiska fördelar*. Vilka taktiska fördelar kan nya tillförda tekniska förmågor ge våra insatsförband som ska sättas in i moderna lågintensitetskonflikter? De sex grundläggande förmågorna utgör i denna undersökning grunden för de variabler som representerar operationella indikatorer på den teoretiska definitionen *taktisk fördel*. Analysenheterna i analysen representeras av möjliga nya tekniska förmågor vilka hämtas ur kapitel 4 och 5. Avslutningsvis värderas uppsatsens resultat i en diskussion.



Figur 1 Övergripande metodbeskrivning

1.6 Material

I lågintensitetskonflikter finns två problem som försvårar eller hindrar saklig analys, data kan vara otillgängliga eller otillförlitliga. Under en pågående konflikt är data svåra att få tillgång till dels för att parterna har intresse av att hemlighålla den, dels för att media eller annan representant för allmänintresset inte finns på plats för att dokumentera händelser.[13] I en koalition eller allians kan olika nationer dessutom ha politiskt intresse av att selektera informationsspridningen.[14] Hemligstämplat material är svårt att få tillgång till. Dessutom skapar sekretess problem för hela examinationsprocessen som tidigare nämnts. I denna uppsats används därför endast **öppna** källor.

Ett annat problem ur källkritiksynpunkt är att parterna i en konflikt inte har organisation och metoder för att hantera dokumentering och arkivering enligt en noggrann och omfattande metod. Memoarer eller dagböcker skrivna av individer som deltagit i en konflikt kan var av intresse, men måste ifrågasättas. Han eller

[13] Ångström, Jan (2002), ”Lågintensiva konflikter som forskningsområde: En introduktion”, Baudin, Arne; Hagman, Thomas och Ångström, Jan (eds.), *En ny medeltid? En introduktion till militärteori i lågintensiva konflikter* (Stockholm: Försvarshögskolan), s. 16.
[14] Jakobsson, *Terrorism och extremism som hotbild*, s. 61–62.

hon har ofta ett intresse av att framställa sig själv på ett så fördelaktigt sätt som möjligt.[15]

De viktigaste källorna i denna uppsats är olika forskare och sakkunniga experter från universitet, högskolor och andra statliga och fristående forskningsinstitut. Även statliga myndigheter och standardiseringsinstitut har utgjort viktiga källor. Samtliga dessa källor har hög tillförlitlighet och utgör därför grunden i empirin.

Källor som kan vara tendensiösa är media och kommersiella företag. Dessa hanteras med ett noggrannare kritiskt förhållningssätt. Om möjligt kompletteras de med andra källor. När det gäller teknisk utrustning bedöms rimligheten i prestanda och användbarhet utifrån författarens egen erfarenhet och tekniska kompetens.

1.7 Tidigare forskning

Forskning om lågintensitetskonflikter har varit eftersatt under en längre tid eftersom fokus har legat på traditionella *mellanstatliga* krig. Detta till trots att antalet mellanstatliga konflikter de senaste 60 åren reducerats till en tiondel samtidigt som andelen *inomstatliga* väpnade konflikter ökat från cirka 50 procent till över 90 procent. Men forskningen har nu kommit en bit på väg och bedrivs inom ett tiotal vetenskapliga discipliner, exempelvis statsvetenskap, juridik, historia, militärteori, sociologi, psykologi och ekonomi. Detta gör den både omfattande och mångfacetterad. Särskilt tydligt visar sig detta i den rent begreppsliga oreda och brist på konsensus som råder. De frågor som omfattas av vetenskaplig forskning hittills är många, i vissa fall ytterst beroende på vilken vetenskapsteoretisk ansats forskare valt. Många frågor återstår att forska på, så debatten kring lågintensitetskonflikter kommer att fortsätta de närmaste åren.[16]

Forskningen om elektronisk krigföring har i Sverige genomförts på bred front på Totalförsvarets forskningsinstitut, FOI. Den har oftast ett stort teknologisk djup inom IT-säkerhet och hela det elektromagnetiska spektret, exempelvis radarsensorer, signaturanpassningsteknik, plattformsskydd, CNO, optronik, HPM-vapen och sambands- och telekrigföringssystem.

Även om forskningen nu kommit en bit på väg så kvarstår en del kunskapsluckor. Forskning som gör direkta kopplingar mellan moderna lågintensitetshot och taktiska konsekvenser av Försvarsmaktens förmåga till elektronisk krigföring har inte gått att finna. Tankar och idéer finns inom mindre och spridda delar av Försvarsmakten och dess anknutna myndigheter, men här finns en lucka, en upplevd kunskap som inte är vetenskapligt belagd.

[15] Ångström, ”Lågintensiva konflikter som forskningsområde: En introduktion”, s. 17.
[16] Ibid, s. 2–3 och 14–16.

Kapitel 2
LÅGINTENSITETSKONFLIKTER

Det ligger i sakens natur att ett så utspritt motstånd inte lämpar sig för större aktioner, som är koncentrerade till tid och rum. […] ju större spridning denna har, desto större verkan har folkbeväpningen. Den förstör liksom en sakta pyrande glöd den fientliga arméns grundvalar.[17]

Carl von Clausewitz

2.1 Inledning

För att våra svenska insatsförband ska vara så effektiva som möjligt krävs att vi förstår konflikternas dynamik och natur. Det vore förödande om vi exempelvis inte gör en korrekt identifiering av konfliktens tyngdpunkt och avgörande punkter och ur ett underrättelseperspektiv inte ställer rätt frågor. Då får vi inte rätt information och går in i en konflikt utan fullständig förståelse för den.[18] En komplicerande faktor i alla slags konflikter idag är att de i västvärlden har en mycket stark politisk koppling. Våra västliga demokratier är känsliga för förluster av egna soldater. Omotiverat kraftigt våld och våld som drabbar oskyldiga civila kan lätt bli kontraproduktivt. Därför ökar kraven på tydliga ROE och förmågan till precisionsbekämpning av militära mål. Trenden är att icke-dödliga vapen som kan neutralisera människor eller materiel får ett ökat intresse i strävan att nå graderad verkan. Essensen är att de valda ledarna står och faller med befolkningens stöd, vilket yttrar sig i att de detaljstyr både militären och andra aktörer i ett konfliktområde.[19] Detta kapitel kommer att beskriva lågintensitetskonflikter i allmänhet men framför allt med djupare fokus på elektronisk krigföring. Kapitlet sammanför fakta från en mängd olika källor och därmed många analyser gjorda av andra, vilka alla pekar på det stora behovet av en väl fungerande underrättelsetjänst på plats i ett konfliktområde.

2.2 Vad är en lågintensitetskonflikt? – En krigsvetenskaplig grund

Vad är då låg intensitet i en konflikt? Vad består intensiteten i? Är det antal stupade, antal bomber som fälls, storleken på bomberna, i vilket tempo som striderna förs, över vilken yta som konflikten utspelar sig, storleken på de styrkor som deltar, eller kvaliteten på de styrkor som deltar? Inom vetenskapen finns inget entydigt svar på dessa frågor. Tvärtom råder en begreppslig oreda inom vetenskapen där begrepp såsom ”små krig” (small wars), ”gerillakrig”, ”terrorism”, ”nya krig”, ”inbördeskrig”, ”asymmetrisk konflikt”, ”andra militära

[17] Clausewitz, Carl von (1991), *Om kriget* (Stockholm, Bonnier Fakta bokförlag AB), s. 479.
[18] Marcusson, Björn (2002), ”Kärt barn har många namn? Lågintensiva konflikter och de militärteoretiska klassikerna”, Baudin m.fl. (eds.), *En ny medeltid? En introduktion till militärteori i lågintensiva konflikter* (Stockholm: Försvarshögskolan), s. 59.
[19] Karlsson, Lars (2002), ”Behov och krav på förmågor för markstridskrafter vid lågintensiva konflikter”, Baudin, Arne; Hagman, Thomas och Ångström, Jan (eds.), *En ny medeltid? En introduktion till militärteori i lågintensiva konflikter* (Stockholm: Försvarshögskolan), s. 99–100.

operationer än krig" (military operations other than war, MOOTW), "lågintensiv konflikt" och "uppror" bara är några i mängden vilka beskriver samma eller liknande fenomen. En orsak till detta är att så många olika vetenskapliga discipliner forskar om *lågintensitetskonflikter*. En annan är att politiska motiv ofta ligger bakom varför en konfliktgrupp kallas terrorister eller frihetskämpar.[20] Alla dessa begrepp har det gemensamt att de försöker beskriva väpnade konflikter som inte är liktydigt med storskaliga *mellanstatliga* krig i traditionell mening.

Den vetenskapliga forskningen har hanterat det *mellanstatliga* kriget som norm, men med tanke på att det moderna statssystemet bara är cirka 350 år gammalt så är det missvisande att betrakta *mellanstatliga* krig som normen och lågintensitetskonflikter som undantaget. Sett över de senaste 50–60 åren visar statistik dessutom att antalet *mellanstatliga* krig successivt har sjunkit. Siffran har sjunkit till en tiondel av de fyrtiotal som existerade i slutet på 1940-talet. Det totala antalet väpnade konflikter har dock fördubblats under samma tidsperiod med en topp i slutet av 1990-talet. Detta förklaras av att antalet *inomstatliga* väpnade konflikter har en stadigt uppåtgående trend. Av dessa *inomstatliga* konflikter ökar dessutom andelen som internationaliserats. Väpnade konflikter är inte längre en angelägenhet mellan stormakter utan snarare mellan eller inom små och medelstora stater. Andelen civila döda jämfört med stupade kombattanter har gått från 1:8 för 100 år sedan till 8:1 under 1990-talet.[21] Kriget har förändrats, lågintensitetskonflikter dominerar idag över mellanstatliga krig.

"Asymmetrisk konflikt" är ett vanligt förekommande begrepp. Asymmetri betyder i sig olikhet eller obalans. Begreppet syftar alltså på att parterna i konflikten inte är jämlika, exempelvis en rebellorganisation mot en regim. Men i vad består olikheten – organisationsformer, storleken på styrkorna, skillnad i relativ makt, eller teknologisk nivå? Klart är dock att begreppet inte omfattar två rebellfraktioner som tävlar om makten i en *inomstatlig* konflikt eftersom det då inte råder en påvisbar asymmetri. Därmed kan slutsatsen dras att begreppet asymmetri inte omfattar alla konflikter som inte är *mellanstatliga* krig.[22]

Begreppet "intern konflikt" innebär att minst en av aktörerna inte är en stat samt att våldet ska äga rum inom en stat. Detta begrepp omfattar inte heller det alla konflikter som inte är *mellanstatliga* krig eftersom konflikten mellan al-Qaida och USA utesluts.[23]

Ett annat uppmärksammat begrepp är Mary Kaldors "nya krig". Hon menar att skillnaderna mellan krig i traditionell mening, organiserad brottslighet och systematiska kränkningar av mänskliga rättigheter suddats ut samt att globaliseringen med dess nätverk minskat skillnaderna mellan intern och internationell. Globaliseringen har förskjutit fokus från geopolitiska och ideologiska målsättningar till identitetspolitik. Kaldor menar att anspråk på makt bygger på en skenbar traditionell tillhörighet som kan vara nationell, klanbunden, religiös eller språklig. Territorium erövras genom att politiskt behärska befolkningen varvid personer med avvikande identitet och åsikter ogillas, vilket leder till etnisk rensning och folkmord. Förbanden i de nya krigen är en brokig mångfald av paramilitära grupper, lokala krigsherrar, förbrytarligor, polisstyrkor, legotrupper och reguljära arméer vilka samtliga ofta har inslag av avancerad

[20] Ångström, "Lågintensiva konflikter som forskningsområde: En introduktion", s. 3, 15 och 17.
[21] Ibid, s. 24. Se även Jakobsson, *Terrorism och extremism som hotbild*, s. 12 och 57.
[22] Ångström, "Lågintensiva konflikter som forskningsområde: En introduktion", s. 4–5.
[23] Ibid, s. 5.

teknologi.[24] Begreppet verkar fånga alla väpnade konflikter som inte är *mellanstatliga* krig. Dock har väpnade konflikter mellan stater och icke-statliga aktörer förekommit sedan det moderna statssystemets födelse 1648 varför det är problematiskt att prata om *nya* krig. Det är en fördel om ett begrepp är giltigt även i framtiden.[25]

Både erkända militärteoretiker och olika staters doktriner använder snarlika begrepp som exempelvis low-intensity conflict, lågintensiv konflikt och lågintensitetskonflikt.[26] I vår svenska militärstrategiska doktrin används begreppet lågnivåkonflikt med betydelsen konflikter som inte når upp till kriterier för krig.[27] Denna doktrinära definition omfattar i princip alla konflikter utom krig med betoning på just **alla**, även två huliganer som slåss under en fotbollsmatch.

I Doktrin för markoperationer talas både om lågintensitetskonflikter och lågintensiva konflikter. Här blandas två begrepp vilka förknippas med inomstatliga väpnade konflikter som kännetecknas av att vara utsträckta i tid och att ha en mycket diffus gräns mellan politiskt, ekonomiskt, militärt och kriminellt agerande. Markdoktrinen menar vidare att begreppen omfattar enskilda missioner bestående av observatörer eller fredsbevarande förband som en stabiliserande faktor med varierande grad av auktoritet i området. Säkerheten för samhällsviktiga funktioner måste skapas, upprätthållas och skyddas. Minor kan behöva röjas. Uppdraget kan även innefatta åtgärder av humanitär karaktär där transporter av såväl människor som förnödenheter kan behöva eskorteras. [28]

Det akademiska begreppet ”lågintensiv konflikt” (low-intensity conflict) föreslås av militärteoretikern Martin van Creveld och omfattar konflikter i vilka båda sidor sällan utgörs av reguljära förband utan snarare en blandning av huliganer, brottslingar, krigsherrar, miliser eller andra icke-reguljära aktörer. Båda parter använder sig dessutom huvudsakligen av eldhandvapen eller annan materiel med låg teknologisk nivå.[29] Begreppet omfattar alltså inte en terroristorganisation med högteknologiska vapen och medel, exempelvis satellitkommunikation eller kärnvapen.

Enligt Nils Marius Rekkedal, professor vid Försvarshögskolan i Stockholm, är lågintensitetskonflikter ett samlingsbegrepp för exempelvis gerillakrig, uppror och terror, där gerillakrig med sin typiska karaktär av reguljära trupper mot icke-reguljära kanske är den vanligaste formen. Med asymmetrisk krigföring menar Rekkedal en konflikt med asymmetriska förhållanden där en angripare utnyttjar motpartens svagheter och sårbarheter i syfte att undgå motpartens huvudstyrka och därmed tvinga striden att ske enbart på sina egna villkor.[30]

De akademiska begreppen är slutprodukter av vetenskapliga undersökningar där man försöker uttala sig så precist som möjligt. De doktrinära begreppen har däremot medvetet en bredare definition för att slippa kontinuerliga revideringar

---

[24] Kaldor, Mary (1999), *Nya och gamla krig: Organiserat våld under globaliseringens era* (Göteborg: Bokförlaget Daidalos AB, översättning av Joachim Retzlaff), s. 11–17, 81–90 och 125–126.
[25] Ångström, ”Lågintensiva konflikter som forskningsområde: En introduktion”, s. 5–6. Se även Karlsson, ”Behov och krav på förmågor för markstridskrafter vid lågintensiva konflikter”, s. 97.
[26] Ångström, ”Lågintensiva konflikter som forskningsområde: En introduktion”, s. 6.
[27] Försvarsmakten, *Militärstrategisk doktrin*, s. 103.
[28] Försvarsmakten, *Doktrin för markoperationer* – 2004, s. 22.
[29] Ångström, ”Lågintensiva konflikter som forskningsområde: En introduktion”, s. 6.
[30] Rekkedal Nils Marius (2004), *Modern krigskonst* (Stockholm, Försvarshögskolan, tredje upplagan), s. 150 och 341–343.

och för att ge den militäre chefen så stor handlingsfrihet som möjligt. Typiskt för de doktrinära definitionerna är att de anger att intensiteten i det våld som utövas är lägre än i krig. Detta är tvetydigt eftersom våldet i en konflikt sällan är lågintensiv på taktisk nivå.[31] Soldaten längst ut på linan som är den som står i skottfältet i en eldstrid upplever sällan att konflikten är låg i intensitet.

I denna uppsats används begreppet lågintensitetskonflikt i betydelsen som väpnad konflikt där hoten mot våra svenska insatsförband utgörs av icke-reguljära aktörer exempelvis terroristgrupper, rebellorganisationer, krigsherrar, miliser, organiserad kriminalitet eller en blandning av dessa. Kopplingarna mellan aktörerna kan vara både öppna och dolda. Deras syften kan vara politiska, religiösa och/eller ekonomiska. Aktörernas metoder är ofta okonventionella och därför svåra att förutse och de kan inte förväntas följa mänskliga rättigheter och internationell rätt. Intensiteten i våldet på taktisk nivå kan därför vara hög. Nivån på olika vapen och medel kan vara högteknologisk, särskilt avseende utrustningar som bygger på billig informationsteknologi. Enklare vapensystem är dock dominerande såsom eldhandvapen, egenhändigt tillverkade bomber av olika slag och minor. Konflikten kan vara intern, men kan lika gärna vara internationell. Våra svenska insatsförband har till skillnad från sin motståndare skyldigheter gentemot den fredligt sinnade delen av befolkningen vars säkerhet måste tillgodoses. De måste självklart följa internationell rätt och mänskliga rättigheter.

2.3 Hotbilden

Allmänt

Den vanligaste beväpningen av icke-reguljära styrkor är gevär, maskingevär, handgranater, landminor, lätt artilleri och kortdistansraketer. De högteknologiska inslagen är modern kommunikationsteknologi vilken har blivit mycket viktigt, främst mobiltelefoni men även moderna radiosystem.[32] Matthew Aid, amerikansk signalspaningsexpert, fastslår att militära styrkor med största sannolikhet kommer att behöva sofistikerad teknologi för att klara av att avlyssna dessa moderna kommunikationssystem som de facto är frekvent förekommande.[33]

Ju mer västvärlden digitaliseras, desto mer sårbar blir den för elektroniska angrepp. Möjliga angreppssätt för terroristaktioner mot nationell infrastruktur kan vara både fysiska och elektroniska. Alla de olika angrepp av datavirus som skett under senare år är bara början på vad som komma skall.[34] Olika extremistgrupper har egna hemsidor på Internet och länkar till varandras sidor.[35] Detta är en indikation på att de har kunskapen och förståelsen för teknikens möjligheter.

Nya teknologier har blivit lättillgängliga och enkla att köpa vilket medfört att olika ondskefulla aktörer idag har tillgång till ett klart bättre sortiment av

---

[31] Ångström, ”Lågintensiva konflikter som forskningsområde: En introduktion”, s. 6–8.
[32] Kaldor, *Nya och gamla krig: Organiserat våld under globaliseringens era*, s. 111.
[33] Aid, Matthew (2004), ”Intelligence Collection Capabilities for Peacekeeping”, Heide, Rachel Lea m.fl. (eds.) *Peacekeeping Intelligence: New Players, Extended Boundaries* (Ottawa: Carlton University), rapport från den andra konferensen ”Peacekeeping Intelligence”, Kanada 4 december 2003, s. 12 [www]. Hämtat från <http://www.carleton.ca/csds/pki/doc/PKI_conference_report_2003.pdf> 25 april 2005.
[34] Rekkedal, ”Nye trender innen krigføringen: Men kriger er i dag som i tidligere tider, vanskelige å forutse”, s. 37.
[35] Jakobsson, *Terrorism och extremism som hotbild*, s. 49.

vapen och annan teknologi. Avancerad teknologi är inte längre exklusivt förbehållet supermakter och andra rika länder. Exempelvis anskaffade colombianska narkotikakarteller avancerade och ”säkra” kommunikations-system.[36] Särskilt bör uppmärksammas att olika extremistgrupper har mycket kortare ledtider för anskaffning av ny materiel än de militära byråkratierna i väst. Slutsatsen blir krav på egen underrättelsetjänst med ökad förmåga att undersöka, analysera och kartlägga dessa hot.[37]

Ett av de allvarligaste hoten i en lågintensitetskonflikt är olika burna luftvärnsrobotsystem så kallade MANPAD (man-portable air defence missile), exempelvis FIM-92 Stinger och SA-7/14/16/18. De är utrustade med IR-målsökare och erbjuder liten möjlighet till förvarning. Mujaheddin i Afghanistan har använt denna typ av luftvärnsrobotar med framgång.[38] Andra exempel är: FARC–gerillan i Colombia skjuter i november 1999 ner en civil DC-3:a, saudiska säkerhetsvakter hittar i maj 2002 en använd MANPAD i närheten av flygplatsen i Ryad i Saudiarabien, ett civilt transportplan (DHL) attackerades i Irak 2003.[39]

Rekkedal beskriver även en annan del av hotbilden som består i att styra striden till miljöer där det är svårt att effektivt använda konventionella styrkor och mycket svårt att använda precisionsvapen. Exempel på sådana miljöer är storstäder och otillgängliga djungler. Dessa hot har ökat dramatiskt de senaste femton åren och det nya är att det ger marginaliserade grupper möjlighet att förverkliga fanatiska visioner.[40] Det är ett dilemma i sig att vi i storstäder vill använda precisionsvapen för att undvika skador på oskyldiga civila, samtidigt som det är mycket svårt att använda dessa vapen i den miljön.

Tempot i en lågintensitetskonflikt är svårkontrollerat. Aktörerna väljer själv tid och plats för sina attacker samt hur länge de ska pågå. Detta leder till att vi kommer i efterhand och att våra motåtgärder riskerar komma för sent och bli verkningslösa.[41] Att förutse vad motståndarens ska göra blir därför centralt.

Det är viktigt att inte tolka världen enbart utifrån ett västligt perspektiv. Vårt västliga synsätt krockar med det synsätt som andra kulturer har, exempelvis i mellanöstern och fjärran östern. Vår tradition innebär principiellt en gentlemanna-mässig strid man mot man tills någon ger upp och man sluter ett fredsavtal, medan man i flera andra kulturer har föga förståelse för vår så kallade ”code of conduct”. I dessa andra kulturer kan bruket av våld vara naturligt och nödvändigt samtidigt som det kan vara legitimt att köpa sig fri från polis och lokalt rättsväsen.[42] Krigen på Balkan och i Afrika är tydliga exempel på konflikter där internationell rätt och

---

[36] Jakobsson, *Terrorism och extremism som hotbild*, s. 60.
[37] Rekkedal, ”Nye trender innen krigføringen: Men kriger er i dag som i tidligere tider, vanskelige å forutse”, s. 23–24, 40 och 44–48.
[38] Global Security.org (2005), *Man Portable Air Defense Systems (MANPADS)* (Alexandria: Global Security.org) [www]. Hämtat från <http://www.globalsecurity.org/military/intro/manpads.htm> 8 september 2005.
[39] Sjöqvist, Lars, forskare vid FOI, *Laserteknik för skydd av flygande plattformar* (presentationsunderlag i Power Point).
[40] Rekkedal, ”Nye trender innen krigføringen: Men kriger er i dag som i tidligere tider, vanskelige å forutse”, s. 44.
[41] Karlsson, ”Behov och krav på förmågor för markstridskrafter vid lågintensiva konflikter”, s. 99.
[42] Rekkedal, ”Nye trender innen krigføringen: Men kriger er i dag som i tidligere tider, vanskelige å forutse”, s.26–31.

mänskliga rättigheter inte har vägt tungt. Vi måste alltså vara beredda på att en motståndare medvetet eller omedvetet bryter mot dessa lagar och konventioner.[43]

Ett annat område som skiljer västvärlden från andra kulturer är ledningsmetoden. I väst använder vi klassisk militär hierarki medan extremister idag strävar efter långtgående decentralisering i nätverk som exempelvis terrornätverket al-Qaida. Detta leder till att mer eller mindre spontana aktioner initieras på mycket låg nivå mot vad man uppfattar som motståndaren, enligt vad man kallar det ledarlösa motståndets princip, ”leaderless resistance”. Detta utgör därmed en större fara för våra insatsförband eftersom en order att skjuta på en företrädare för en internationell styrka inte ges från centralt håll. Utvecklingen av informationsteknologi har lett till att extremister lättare kan kommunicera för att koordinera och leda insatser. Det ledarlösa motståndets princip medför att beslut fattas av lägre nivåer om huvudpersonerna i nätverket faller bort. Fattade beslut måste då delges inom nätverket, vilket enklast sker med modern informationsteknologi. Terrornätverket al-Qaida har i så stor utsträckning som möjligt använt sig av satellittelefoner och offentliga kommunikationer som exempelvis vanlig e-post från internetcaféer. Täckord i form av vardagliga fraser och falska identiteter har använts. Efter Talibanstyrets fall har högsta ledningen för al-Qaida rent fysiskt tvingats till att flytta sig oftare. Det är främst risken för att västliga underrättelseorgan spårar kommunikationsutrustningen som medfört att de flyttar runt ledningen med sina satellittelefoner och bärbara datorer.[44]

Man kan konstatera att den gamla sanningen ”förstå sin motståndare”, inte minskat i betydelse vid lågintensitetskonflikter, snarare blivit mer komplex. Johan Jacobsson, forskare vid FOI, uttrycker det på följande sätt.

> Förståelse för lokala förhållanden är vid varje internationell insats utomordentligt viktig. Förmågan att vid sidan av inhämtade fakta och analyser också förstå stämningarna i konfliktområdet, lokala styresmäns ställning, rivalitet mellan olika grupper av människor m.m. kan många gånger visa sig vara den mest värdefulla komponenten i underrättelsearbetet.[45]

För att uppnå denna förståelse krävs en mycket god inhämtnings- och analysförmåga, både före och under genomförandet av en svensk insats i ett konfliktområde.[46] För att öka analysförmågan krävs att de traditionellt militära analysmetoderna samordnas med metoder från andra områden såsom de finansiella, tekniska och polisiära.[47] Kartläggning enbart **kort** tid före ett svenskt deltagande internationellt riskerar ge en ofullständig bild av en konflikt och dess karaktär och i värsta fall helt intetsägande. Att kartlägga alla pågående och möjliga konflikter i världen är dock en uppgift som är en enda nation övermäktig. Kontinuerligt internationellt samarbete är därför mycket viktigt. Särskilt viktigt är

---

[43] Siljebråten, Björn (2002), ”Fredsstøttende operasjoner og lavintensitetskonflikter: Noen utfodringer og sentrale problemstillinger”, Baudin m.fl. (eds.), *En ny medeltid? En introduktion till militärteori i lågintensiva konflikter* (Stockholm: Försvarshögskolan), s. 159.
[44] Jakobsson, *Terrorism och extremism som hotbild*, s. 29–30, 33–34 och 59.
[45] Ibid, s. 65. Se även Siljebråten, ”Fredsstøttende operasjoner og lavintensitetskonflikter: Noen utfodringer og sentrale problemstillinger”, s. 160.
[46] Siljebråten, ”Fredsstøttende operasjoner og lavintensitetskonflikter: Noen utfodringer og sentrale problemstillinger”, s. 160.
[47] Frisell, Mikael (2002), ”Lågintensiva konflikter och deras krav på insatsstyrkor och doktriner”, Baudin, Arne; Hagman, Thomas och Ångström, Jan (eds.), *En ny medeltid? En introduktion till militärteori i lågintensiva konflikter* (Stockholm: Försvarshögskolan), s. 170.

det när det gäller att kartlägga internationell terrorism och extremism, vilket **måste** ske i ett internationellt perspektiv. Det kan dock vara förödande att förlita sig enbart på andra nationers underrättelser då olika nationer kan ha politiskt intresse av att exempelvis överdriva eller tona ned olika hot.[48] Slutsatsen blir att ett deltagande internationellt kräver en mycket god egen underrättelseförmåga såväl som ett långtgående internationellt samarbete på området.

Med utgångspunkt i Kevin O'Briens och Joseph Nusbaums artikel i Jane's Intelligence Review pekar Rekkedal på att underrättelsetjänsten idag fortfarande är starkt präglad av invasionshotet från Sovjetunionen. Klassisk militär högteknologi måste kompletteras med exempelvis inhämtning från mänskliga källor (human intelligence, HUMINT) och öppna källor (open sources intelligence, OSINT).[49] Johan Jacobsson föreslår i samma anda att man kombinerar signalspaning (signal intelligence, SIGINT), HUMINT, OSINT och bilateralt utbyte mellan olika nationers underrättelsetjänster. Dessutom bör man erhålla stöd från underrättelseorganisationer i Sverige.[50] Teknologin förefaller alltså vara en viktig delkomponent i att övervaka kommunikationer och annan elektronisk aktivitet, exempelvis för att lokalisera terroristbaser.

Konflikter på Balkan

Krigen på Balkan under 1990-talet är historien om den jugoslaviska nationella arméns sönderfall. Den föll samman i både reguljära och icke-reguljära styrkor med inslag av kriminella, frivilliga och legoknektar. Det fanns tre huvudgrupper av icke-reguljära styrkor: paramilitära styrkor, utländska legotrupper och lokala polistrupper förstärkta med beväpnade civila. Det fanns ett åttiotal olika paramilitära grupper i krigen i Bosnien och Kroatien omfattande omkring 35–65 000 man och de samarbetade ofta med de reguljära styrkorna. Bland legotrupperna var Mujaheddin, med sina krigsveteraner från Afghanistan, den mest kända. De reguljära styrkorna besköt ett område tills motståndet var tillräckligt försvagat och terroriserat. Då ryckte icke-reguljära styrkor in för att slutföra den etniska rensningen genom att plundra och förstöra hus och kulturella minnesmärken. Hela familjer utplånades, särskilt de med stort inflytande på den lokala befolkningen. Familjer kunde klara livhanken om de lämnade ifrån sig alla sina besparingar till plundrarna och gav sig av från sina hus. Metoderna från Bosnienkrigen upprepades igen i Kosovo. På kosovoalbanska sidan fanns då det paramilitära "Ushtria clirimtare e Kosoves" (UCK) som var beväpnade med eldhandvapen av typen Kalasjnikov från tömda vapengömmor efter den albanska statens sammanbrott sommaren 1997.[51] I Kosovo har det interna våldet mellan olika grupper varierat i karaktär. Exempelvis har aktörer använt sig av bomber som fjärrutlösts via radiosignaler.[52] I december 1997 dödades fem personer när UCK-rebeller sköt ner ett transportplan med MANPAD.[53]

Tidigt på morgonen den 6 juli 1995 anföll bosnisk-serbiska styrkor den av FN deklarerat skyddade zonen kring staden Srebrenica. Det serbiska anfallet var i

[48] Jakobsson, *Terrorism och extremism som hotbild*, s. 61–62.
[49] Rekkedal, "Nye trender innen krigføringen: Men kriger er i dag som i tidligere tider, vanskelige å forutse", s.37.
[50] Jakobsson, *Terrorism och extremism som hotbild*, s. 62.
[51] Kaldor, *Nya och gamla krig: Organiserat våld under globaliseringens era*, s. 55–59, 174–176.
[52] Andén, Håkan, MUST. Uttalande vid föreläsning på Högkvarteret i Stockholm 2005-05-20.
[53] Sjöqvist, *Laserteknik för skydd av flygande plattformar*.

själva verket en välplanerad operation med mål att etniskt rensa Srebrenica. Massakern som följde krävde tusentals bosnisk-muslimska civila dödsoffer, 23 000 kvinnor och barn fördrevs. Den underbemannade holländska FN-bataljonen stod maktlös i sin uppgift att avskräcka från anfall i syfte att skydda zonen. En avgörande anledning till misslyckandet var mycket bristande underrättelser.[54] Hollands dyrköpta erfarenheter från Srebrenica understryker behovet av signalspaningsenheter och skydd av egen kommunikation såväl som ökat underrättelsesamarbete med andra nationer. Underrättelseförmåga är numer **alltid** en del av en holländsk insatsstyrka.[55]

I december 1995 förändrades situationen och det militära ansvaret övergick från FN till Nato, UNPROFOR[56] avlöstes av IFOR[57]. Med IFOR introducerades ett nytt starkare FN-mandat uppbackat av massiva resurser, främst från Nato. Avseende underrättelsetjänst blev skillnaden enorm. En stor anledning till UNPROFOR:s dåliga underrättelsetjänst var FN:s traditionella ogillande av underrättelser vilket man associerade till spionage i en negativ betydelse.[58] IFOR:s underrättelseenheter var däremot under Nato-flagg och kunde övervaka parterna i konflikten dygnet runt i alla väder vilket definitivt inte var fallet i UNPROFOR. Brott mot fredsavtalet, Daytonavtalet, upptäcktes snabbt och lämpliga åtgärder från IFOR påvisade viljan att fullfölja uppdraget. Detta kom att verka avskräckande från aggressioner. Kärnan i IFOR:s underrättelseförmåga var USA:s satellitspaning och telekrigföringskapacitet i kombination med brittiska och franska HUMINT-enheter.[59]

IFOR disponerade flygburen syntetisk aperturradar (SAR) för övervakning av markmål, JSTARS (joint surveillance target attack radar system). Systemet hade sina begränsningar. Den bergiga terrängen skapade radarskuggor i dalgångar och systemet kunde inte skilja egna styrkor från parternas styrkor eller civila rörelser. Systemets största fördel var att inrikta HUMINT och markspaningsenheter. Man disponerade olika typer av obemannade flygfarkoster (unmanned aerial vehicles, UAV), med kortare räckvidd på taktisk nivå och med längre räckvidd på operativ nivå. De användes framgångsrikt bestyckade med videokameror för övervakning av kommunikationslinjer, demonstrationer och upplopp. Underrättelseinhämtning med bildutrustningar (imagery intelligence, IMINT) förstärktes med både spaningsflyg och satellitspaning. På lägsta taktiska nivå användes videokameror av olika slag flitigt, dock utan effektiv analys och dokumentering. Dessa användes dock framgångsrikt för att i detalj orientera piloter om deras mål inför attackuppdrag. Molnigt väder och fysiska hinder satte vissa begränsningar i användning av IMINT-resurser, men mängden av olika sensortyper och plattformslösningar kunde komplettera varandra för att nå bästa

[54] Honig, Jan Willem och Both, Norbert (1996), *Srebrenica: Record of a War Crime* (London: Penguin Books), s. 4–6 och 175–176.
[55] Weibes, Cees och Svensson, Jan-Inge (2004), ”Peacekeeping and its Intelligence Requirements – National Experiences”, Heide, Rachel Lea m.fl. (eds.) *Peacekeeping Intelligence: New Players, Extended Boundaries* (Ottawa: Carlton University), rapport från den andra konferensen ”Peacekeeping Intelligence”, Kanada 4 december 2003, s. 6–7 [www]. Hämtat från <http://www.carleton.ca/csds/pki/doc/PKI_conference_report_2003.pdf> 25 april 2005.
[56] United Nations Protection Force enligt FN-resolution 743, 21 februari 1992.
[57] Implementation Force enligt FN-resolution 1031 från 15 december 1995. Mandat till NATO.
[58] Weibes och Svensson, *Peacekeeping Intelligence: New Players, Extended Boundaries*, s. 6.
[59] Wentz, Larry (ed) (1997), *Lessons from Bosnia: The IFOR Experience* (Washington: DoD Command and Control Research Program), s. 57 och 60.

möjliga effekt. Signalspaningsresurser fanns både markbaserade och i luften. Problemet var att systemen var skräddarsydda för taktisk användning mot militära system i konventionellt krig vilket innebar att de inte kunde exploatera signaler och utvinna underrättelser från civila högteknologiska system som de stridande parterna använde exempelvis mobiltelefoner. De viktigaste aktörerna använde alltså inte det traditionella frekvensbandet för radiokommunikation (very high frequency, VHF, 30–300 MHz). Det amerikanska systemet Guardrail med kapacitet för både teknisk signalspaning (electronic intelligence, ELINT) och kommunikationsspaning (communication intelligence, COMINT) fungerade tillfredställande och kunde lokalisera enheter. Handburna utrustningar för att skanna höga frekvensområden spreds via specialenheter till låg nivå för att möjliggöra upptäckt av olika hot. De amerikanska attackhelikoptrarna utgjorde en användbar sensor med både ELINT-utrustning och videokamera. Signalspaningen fungerade bäst som förvarning om konventionella hot. Fjärrstyrda marksensorer användes framgångsrikt för att övervaka parternas rörelser utan att ha egna soldater i området. Underhåll och minfält satte vissa begränsningar på dessa system.[60] I områden med omfattande kriminalitet är också risken stor att de stjäls.

Konflikter i Afrika

Trupperna ingående i FN:s mission i Kongo, MONUC[61], har lågteknologisk utrustning. De har problem med att upptäcka och följa sina mål och listan på önskade förmågor och förband är lång. I avsaknad av exempelvis högteknologiska sensorer förlorar FN-trupperna kontrollen på milisen från mörkrets inbrott på eftermiddagen till gryningen nästa morgon. Inte bara IR-sensorer, men även signalspaning kunde ha bidragit till att följa milisen under dygnets mörka timmar. Väpnad milis och andra väpnade grupperingar använder både enkla handburna radiostationer och sofistikerad kommunikationsutrustning i form av mobiltelefoner och satellittelefoner. Signalspaning till varje brigad är därför ett av de många listade önskemålen.[62]

Somalia är ett exempel på ett samhälle som är indelat i olika klaner, vilka traditionellt har ett territorium kopplat till sig. När FN:s mission i Somalia, UNOSOM II[63], inleddes 1993 efter två tidigare framgångsrika missioner, ökade spänningarna mellan den lokala milisen och FN. FN:s försök att avväpna milisen fick den att övergå till att strida i bebyggelse. Milisen beblandade sig med kvinnor och barn, och lyckades mobilisera folksamlingar. Detta innebar stora svårigheter för FN-trupperna att särskilja kombattanter från vanliga civila och konsekvensen blev ett stort antal oskyldiga civila offer. Underrättelsetjänsten fick ägna sig mer åt att fastställa *vem som var* motståndare istället för att på klassiskt manér *analysera* honom. Ulf Högström drar slutsatsen i sin essä om lärdomar från Somalia att underrättelseförmågan är av central betydelse vid fredsframtvingande operationer. Han menar även att den måste ha kompetens att analysera i ett vidare

[60] Wentz, *Lessons from Bosnia: The IFOR Experience*, s. 102–111.
[61] Mission de l'Organisation des Nations Unies en RD Congo enligt FN-resolution 1279, 30 november 1999.
[62] Isberg, brigadgeneral Jan-Gunnar, ställföreträdande militär chef (Deputy Force Commander) och brigadchef i FN:s mission i Kongo, MONUC, 2004–2005. Uttalande som föreläsare vid den tredje konferensen "Peacekeeping Intelligence – The Way Ahead" på Karlbergs slott i Stockholm 2004-12-02 och som seminarieledare på Försvarshögskolan i Stockholm 2005-04-07.
[63] United Nations Operation in Somalia II enligt FN-resolution 814, 26 mars 1993.

spektra än den traditionellt militära.[64] En av de mest kända milisledarna i Somalia var general Mohamed Farah Aideed. Han hade stöd från nomadgrupperingar i ett område norr och väster om huvudstaden Mogadishu samt ledde en egen icke-reguljär styrka. Aideed drev också sin egen radiostation med vilken han sände ut sitt politiska budskap till befolkningen. Denna användes exempelvis för att kritisera FN och USA och för att organisera demonstrationer i huvudstaden Mogadishu.[65] När 24 pakistanska FN-soldater dödades av Aideeds styrkor i juni 1993 svarade FN med att förstöra hans högkvarter och hans ökända radiostation. Aideed fortsatte dock att sända sin propaganda på kortvågsradio.[66] Amerikanernas sofistikerade signalspaning hade en avgörande begränsning som bestod i att de inte kunde avlyssna milisens mobiltelefonkommunikation.[67] Det finns dessutom uppgifter som talar om att Aideed i kritik mot amerikanska styrkor hänvisar till bevis från egen avlyssning av radiokommunikation mellan amerikanerna och annan milisledare.[68] En sällsynt uppgift, men inte alls osannolik då det inte kräver mer än en billig skannande radiomottagare. Har man kunskapen att driva en radiostation är steget inte långt till att även förstå och nyttja radioavlyssning.

I Sierra Leone var radiokommunikation en naturlig del av livet. Därför var signalspaning absolut nödvändigt för att övervaka hot mot FN-styrkorna.[69]

På olika håll i Afrika finns ett antal exempel på användning av MANPAD. I april 1994 skjuts en Falcon-50 ned med presidenterna från Rwanda och Burundi som passagerare. I oktober 1998 träffar en rebellrobot motorn på en Boeing 727 (Congo Airline) med 40 passagerare, planet kraschar efter start. I december 1999 skjuter UNITA-rebeller från Angola ner en FN-transport med C-130, 14 döda. I juni 2001 försöker UNITA-rebeller skjuta ner en Boeing 727. Flygplanet skadas men kan landa. I Mombasa, Kenya i november 2002 avfyrar terrorister SA-7 som missar ett israeliskt passagerarflygplan vid start.[70]

Al-Qaida i Afghanistan

Som ett svar på attackerna den 11 september initierade USA den 7 oktober 2001 ”Operation Enduring Freedom” i Afghanistan. Ett av målen var att avlägsna al-Qaidas baser och aktiviteter i området. En av de största operationerna mot al-Qaida var ”Operation Anaconda” våren 2002. Motståndarens operativa tyngdpunkt under operationen utgjordes av de styrkor ur al-Qaida som försvarade de östra delarna av Afghanistan. De uppträdde i svårtillgänglig terräng, ofta inne i bergsgrottor, och drog sig inte för att använda den vanliga civilbefolkningen som sköldar. Underrättelsetjänsten fick en helt avgörande betydelse för att under operationen identifiera vem som var al-Qaida, var de befann sig samt med vilken

---

[64] Högström, Ulf (2002), ”Behov och förmågor för fredsframtvingande insatsstyrkor: i lågintensiva konflikter: Lärdomar från Somalia”, Baudin m.fl. (eds.), *En ny medeltid? En introduktion till militärteori i lågintensiva konflikter* (Stockholm: Försvarshögskolan), s. 147–148 och 150.
[65] Clarke, Walter och Herbst, Jeffrey (eds) (1997), *Learning from Somalia: The Lessons of Armed Humanitarian Intervention* (Boulder: Westview Press), s. 130–132.
[66] Stevenson, Jonathan (1995), *Losing Mogadishu: Testing U.S. Policy in Somalia* (Annapolis, Naval Institute Press), s. 83 och 93.
[67] Kaldor, *Nya och gamla krig: Organiserat våld under globaliseringens era*, s. 111.
[68] Clarke och Herbst, *Learning from Somalia: The Lessons of Armed Humanitarian Intervention*, s. 130–132.
[69] Aid, *Peacekeeping Intelligence: New Players, Extended Boundaries*, s. 12.
[70] Sjöqvist, *Laserteknik för skydd av flygande plattformar*.

militär förmåga. Under veckor av förberedelser fotograferades deras rörelser och deras kommunikationer avlyssnades.[71]

Al-Qaida är en i huvudsak modern organisation vilken utnyttjar modern teknik, exempelvis krypterade hemsidor för kommunikation.[72] I fallet Afghanistan användes mobiltelefoner, satellittelefoner och kortvågsradio. Även senare under Madridattentaten i mars 2004 använde al-Qaida mobiltelefoner, denna gång för att fjärrstyra detonationen av bomberna.[73] Att fjärrutlösa bomber på detta sätt upprepades igen vid attentaten i London i maj 2005.

Under operationen i Tora-Bora upptäckte al-Qaida att deras radiokommunikation kunde spåras varför de allt oftare använde sig av radiotystnad. Följande veckor förstärktes underrättelseinhämtningen i området med HUMINT och UAV. När operationen drog igång använde amerikanerna laser- och GPS-styrda bomber. Koordinater på målen kunde sändas från markförbandens GPS-utrustning direkt till attackflyget. Attackflygplanen tog också emot bilder direkt från UAV:er. Teknologiska framsteg inom datanätverk och bredbandig satellitkommunikation möjliggjorde kombination av multipla sensorer såsom UAV:er, JSTARS, signalspaning och satellitbilder.[74] De kombinerade dessa sofistikerade spaningsutrustningar med afghanska soldater med god terrängkännedom för att med hög noggrannhet lägesbestämma enheter ur al-Qaida i området. Exempelvis användes spaningsflyg med värmekänsliga infraröda kameror för att upptäcka al-Qaida i uppvärmda bergsgrottor. Koordinaterna sändes sedan direkt ned till markförbanden. Enligt en artikel i Washington Post användes flygstridskrafter för att spana på och bekräfta att elektroniska sändningar kom från al-Qaida. När man läser dragna lärdomar står det klart att kommunikation och underrättelser är funktioner som måste prioriteras. Syftet var att det ansågs viktigt att komma innanför motståndarens beslutscykel, den så kallade OODA-loopen[75].[76]

Analys och delgivning av underrättelser var de områden som särskilt behövdes förbättras. Man konstaterar dessutom att signalspaningsutrustning på flygplan kunde ha använts bättre för att lokalisera enheter ur al-Qaida än vad som gjordes. Ett problem som påverkade beslutscykeln negativt var att skilja al-Qaida från vanlig civilbefolkning och rädslan att träffa civila mål.[77]

Amerikanerna köpte även ensamrätten till bilder från satelliten Ikonos, vilken kan ta bilder med 1 meters upplösning.[78] Anledningen till detta kan man

---

[71] Håkansson, Kersti (2002), ”Taktik och stridsteknik i lågintensiva konflikter: en fallstudie av Operation Anaconda”, Baudin, Arne; Hagman, Thomas och Ångström, Jan (eds.), *En ny medeltid? En introduktion till militärteori i lågintensiva konflikter* (Stockholm: Försvarshögskolan), s.71–77, 80–85 och 88–90. Se även Håkanssons källhänvisning till artikel i The Times den 6mars 2002.

[72] Gunaratna, Rohan (2002), *Inside Al Qaeda: Global Network of Terror* (New York: Columbia University Press), s. 11.

[73] BBC (2004), *Madrid blasts: Who is to blame?* (London: BBC News World edition, 18 mars 2004) [www]. Hämtat från <http://news.bbc.co.uk/2/hi/europe/3512748.stm> 4 juli 2005.

[74] Vego, Milan (2002), “What Can We Learn from Enduring Freedom?”, *US Naval Institute Proceedings*, Vol 128, No 7, s. 33.

[75] En beslutscykel innehåller fyra faser för att komma från upptäckt till handling; Observation, Orientation, Decision, Action, förkortat OODA.

[76] Håkansson, ”Taktik och stridsteknik i lågintensiva konflikter: en fallstudie av Operation Anaconda”, s.71–77, 80–85 och 88–90. Se även Håkanssons källhänvisning till artikel i The Times.

[77] Ibid.

[78] Ibid.

spekulera i eftersom de sannolikt hade egna satelliter. Kanske ville de skaffa sig ensamrätten på alla satellitbilder över området och därmed neka al-Qaida möjligheten till underrätterser om koalitionen.

Sammanfattningsvis kan man dra slutsatsen att kombinationen av flera olika typer av sensorer var en framgångsfaktor för amerikanerna i sökandet efter stridande enheter ur al-Qaida i Afghanistan.

Kapitel 3
FÖRSVARSMAKTEN IDAG

Det är även helt uppenbart att den högsta ledningsnivån för kriget, från vilken de övergripande besluten utgår, inte kan vara annat än politisk.[79]

Carl von Clausewitz

3.1 Inledning

Motiverade av säkerhetspolitiska intressen har länderna i västvärlden under lång tid förberett sig för ett konventionellt mellanstatligt krig, främst beroende på att det i Sovjetunionen fanns en klart definierad motståndare.[80] Riksdagsbeslutet våren 2000 ”Det nya försvaret” innebar för Sveriges del att invasionsförsvaret som var anpassat efter det kalla krigets förutsättningar skulle överges för gott och ersättas av insatsförsvaret.[81] Det tog alltså tiotalet år sedan muren fallit, Sovjetunionen upplösts och Europa härjats i lika många år av krig på Balkan innan ett sådant beslut kunde tas i vårt land. Frågan är hur länge det kommer att ta att verkställa detsamma, doktrinärt, materiellt, utbildningsmässigt och framför allt mentalt för de äldre generationer officerare som skolats i skuggan av kalla kriget?

Kanske är det viktigaste just nu att medvetandegöra de möjliga problem som väntar när vi sätts i situationer som är okonventionella i relation till den utbildning och erfarenhet som soldater och officerare har. Denna mentala förberedelse borde vara en fördel när våra svenska insatsförband sätts in i lågintensitetskonflikter.[82]

I detta kapitel undersöks vilka förmågor avseende elektronisk krigföring som de svenska insatsförbanden har idag. Inledningsvis beskrivs Försvarsmaktens omställning till insatsförsvar samt vilka konsekvenser detta fått i allmänhet.

3.2 En försvarsmakt under omställning

Sverige har en lång tradition av de moderna fredsfrämjande operationerna under FN-flagg. Tanken att internationalisera den svenska försvarsmakten ytterligare har funnits i drygt 10 års tid. Nato skapade i januari 1994 det nya europeiska samarbetet, Partnerskap för fred (Partnership for Peace, PfP). Sverige gick med redan i maj samma år.[83] Vi stod då fortfarande utanför EU och statsminister Ingvar Carlson proklamerade vår fortsatta militära alliansfrihet syftande till neutralitet i krig.[84] I försvarsbeslutet 1996 var invasionsförsvarstanken kvar och modeordet var anpassning, vilket syftade till att återta storleken på

[79] Clausewitz, *Om kriget*, s. 618.
[80] Siljebråten, ”Fredsstøttende operasjoner og lavintensitetskonflikter: Noen utfodringer og sentrale problemstillinger”, s. 155.
[81] Karlsson, ”Behov och krav på förmågor för markstridskrafter vid lågintensiva konflikter”, s. 93.
[82] Ångström, ”Lågintensiva konflikter som forskningsområde: En introduktion”, s. 11.
[83] Regeringen (1997), *Regeringens skrivelse 1997/98:29:Euro-atlantiska partnerskapsrådet och det fördjupade Partnerskap för fred-samarbetet* (Stockholm: Regeringskansliet), s. 1 [www]. Hämtat från <http://www.regeringen.se/content/1/c4/14/04/4093cd1a.pdf> 27 april 2005.
[84] Regeringen (1994), *Regeringsförklaring 7 oktober 1994* (Stockholm: Regeringskansliet), s. 6–7 [www]. Hämtat från <http://www.regeringen.se/content/1/c6/01/14/66/7dcdb8ae.pdf> 27 april 2005.

invasionsförsvaret. Internationella insatser gavs större vikt, men omnämndes som en sekundär uppgift, efter primäruppgiften att försvara landet mot väpnat angrepp.

> Totalförsvarets resurser skall även kunna användas för fredsfrämjande verksamhet […]. För att stärka möjligheterna på detta område skall ett internationellt kommando bildas inom Försvarsmakten. I denna skall bl.a. en snabbinsatsstyrka ingå.[85]

I september 1996 proklamerade statsminister Göran Persson att Sveriges mål var en alleuropeisk säkerhetsgemenskap.[86] Viktiga beståndsdelar i detta ansågs vara PfP och dess fördjupade samarbete Euro-atlantiska partnerskapsrådet (Euro-Atlantic Partnership Council, EAPC). Steget in EAPC togs i maj 1997 och syftade till bättre krishantering. Detta ledde till att Sverige ökade sitt engagemang i olika Nato-högkvarter samt deltog i uppbyggandet av en snabbinsatsstyrka som stod till FN:s förfogande.[87] Men det dröjde ända till kontrollstationen 1999 innan invasionsförsvaret definitivt avskrevs som den dominerande grunden för försvarets utformning. I regeringens proposition till riksdagen samma år uttalas tydligt att invasionsförsvaret ska ställas om till ett insatsförsvar. Regeringen säger att alla insatsförband ska kunna användas för internationella insatser, men de ska vidareutvecklas successivt. Omställningen ska prioriteras, men styrande för utvecklingstakten ska dels vara när och i vilken omfattning som resurser kan avdelas, dels inom vilka områden som efterfrågan kan förväntas bli stor.[88] Det var alltså frågan om en långsam process anpassad efter plånboken.

Våra ”gamla” krigsförband skulle alltså successivt utvecklas och ges hög operativ rörlighet och kvalitet för att kunna sättas samman i operativa insatsstyrkor efter utlandsstyrkans behov och därigenom delta i internationella insatser.[89] Ett antal nya förbandstyper pekades särskilt ut att utgöra betydelsefulla komponenter för förmågan att möta framtida hot och risker och därmed en viktig del av omställningen. Dessa viktigare nya förband var signalspaningsbataljon, IT-säkerhetsförband, divisionsunderrättelsebataljon, tre säkerhetsbataljoner, två jägarbataljoner, NBC-insatsstyrka, luftburen bataljon och åtta flygbasbataljoner. Flertalet av dessa förband skulle vara organiserade och operativa 2004, men några sattes på undantag till 2011.[90]

Regeringen anger på hösten 2001 ett antal förbandstyper ur insats-organisationen som ska vidareutvecklas under perioden 2001–2004 i syfte att

---

[85] Regeringen (1996), *Regeringens proposition 1996/97:4: Totalförsvar i förnyelse - etapp 2* (Stockholm: Regeringskansliet), s. 22.
[86] Regeringen (1996), *Regeringsförklaring 17 september 1996* (Stockholm: Regeringskansliet), s. 2 [www]. Hämtat från <http://www.regeringen.se/content/1/c6/01/14/59/3903a8d0.pdf> 27 april 2005.
[87] Regeringen, *Regeringens skrivelse 1997/98:29: Euro-atlantiska partnerskapsrådet och det fördjupade Partnerskap för fred-samarbetet*, s. 3 och 7-9. Se även Regeringen (1997), *Regeringsförklaring 16 september 1997* (Stockholm: Regeringskansliet), s. 3 [www]. Hämtat från <http://www.regeringen.se/content/1/c6/01/14/55/bab34f35.pdf > 27 april 2005.
[88] Regeringen (1999), *Regeringens proposition 1999/2000:30: Det nya försvaret* (Stockholm: Regeringskansliet), s. 12 och 37–39.
[89] Ibid s. 39, 53–54 och 165–167.
[90] Regeringen (2001), *Regeringens proposition 2001/02:10: Fortsatt förnyelse av totalförsvaret* (Stockholm: Regeringskansliet), s. 146.

anmälas till FN:s respektive EU:s styrkeregister[91], men de är inte de enda styrkeregistren. De aktuella styrkeregisterna är Nato (PfP), EU (Helsinki force catalogue, HFC), FN (The United Nations stand-by arrangements system, UNSAS), NORDCAPS (Nordic coordinated arrangement for military peace support) och SHIRBRIG (Standby Force High Readiness Brigade).

I 2004 års regeringsförklaring proklameras att Sverige ska ta ansvar för upprättandet av en multinationell snabbinsatsstyrka i EU:s regi, även kallad Nordic Battle Group. Intressant att notera är att ordalydelsen ”syftande till neutralitet i krig” inte längre finns kvar i regeringsförklaringen. Det proklameras kort och gott att Sverige är **militärt** alliansfritt.[92]

Så hur ser det då ut i Försvarsmakten? Har vi ställt om från invasionsförsvar till insatsförsvar? Vi har tidigare kunnat konstatera att vi ställs inför diversifierade krav vid lågintensitetskonflikter. Exempel på dessa är interoperabilitet, samverkan med andra än militära enheter och förmåga till anpassning av egenskyddet efter konfliktens karaktär. Sammansättningen av ett förband och dess förmågor ska spegla konflikten och vara så flexibel att handlingsfriheten inte blir lidande.[93]

Tabell 1 Sammanställning över insatsförband anmälda till olika styrkeregister 2004. [94]

Förband	**Precisering**
Ledningsresurs	50 personer (delvis insatta)
CIMIC-kompani	civil-militär samverkan, ”civil military cooperation”, CIMIC (delvis insatta, exempelvis i Afghanistan)
Observatörer	40 personer (delvis insatta)
Mekaniserad bataljon	pansarterrängbil (delvis insatt i Kosovo)
Mekaniserad bataljon	stridsfordon 90 (delvis insatt i Liberia)
Ingenjörkompani med EOD-förmåga	(delvis insatta)
Militärpoliskompani	(delvis insatta)
Minkrigsförband	3 fartyg typ Landsort + underhållsfartyg
Ubåtsförband	1 ubåt typ Gotland + stödenhet
Korvettförband	2 korvetter typ Stockholm + underhållsfartyg
Spanings- och jaktflygförband	8 JAS 39
Transportflygplan	4 TP 84 Hercules
S 102B	1 Gulfstream, signalspaningsflygplan

[91] Regeringen, *Regeringens proposition 2001/02:10: Fortsatt förnyelse av totalförsvaret*, s. 142–143. Se även riksdagen (2000), *Ministerrådspromemoria Den europeiska säkerhets- och försvarspolitiken (ESDP) inför Europeiska rådet i Nice* (Stockholm: Regeringskansliet) [www]. Hämtat från <http:// www.riksdagen.se/eu/Riksdagen/EUN/MinisterPm/Ministerpm_0001_09_ allmesdp.htm> 28 april 2005.

[92] Regeringen (2004), *Regeringsförklaring 14 september 2004* (Stockholm: Regeringskansliet), s. 1 [www]. Hämtat från <http://www.regeringen.se/content/1/c6/02/96/52/e5f3b8fa.pdf> 27 april 2005.

[93] Karlsson, ”Behov och krav på förmågor för markstridskrafter vid lågintensiva konflikter”, s. 103.

[94] Statskontoret (2005), *Försvarets styrning – styrkedjan från statsmakternas beslut till verklighet* (Stockholm: Statskontoret), s. 101 [www]. Hämtat från <http://www.statskontoret.se/upload/ Publikationer/2005/2005109.pdf 28 april 2005. Se även Försvarsmakten (2001), *Försvarsmakten och Sveriges ordförandeskap i EU* (Stockholm: mil.se) [www]. Hämtat från <http://www.mil.se/ ?c=news&id=925> 28 april 2005.

Man kan konstatera att de förmågor som våra förband har idag fortfarande är framtagna i första hand för ett konventionellt mellanstatligt krig[95], möjligen med CIMIC-kompani, observatörer och delar av ingenjörkompaniet för röjning av hemmagjorda bomber (improvised explosive device **disposal**, IEDD) undantaget. Högkvarteret uttrycker själv följande i samma anda om den kommande Nordic Battle Group.

> Den förändring som nu pågår är den största i Försvarsmaktens historia på 500 år. Försvarsmakten har alltid sysslat med att försvara territoriet. Nu kopplar vi för första gången loss försvaret från territorietänkandet för att skapa gemensam säkerhet ute i världen genom att tillsammans med andra dämpa konflikter.[96]

Det är alltså först med Nordic Battle Group som vår utveckling av Försvarsmakten i realiteten inte längre kommer dimensioneras av försvaret av vårt territorium mot en invasion. Försvarsbeslutet 2000 innebar en omställning av vår befintliga krigsorganisation. Krigsförbanden i det så kallade arvet skulle vidareutvecklas till att bli en insatsorganisation. Nordic Battle Group är något helt annat. Det innebär att vi utvecklar helt nya förband och förmågor. Det är alltså nu, i och med försvarsbeslut 2004, som vi startar en utveckling av insatsförband som i första hand kan, om vi kan släppa arvet, dimensioneras mot moderna lågintensitetskonflikter.

Låt oss gå vidare och närmare undersöka förmågan avseende elektronisk krigföring i den organisation som är fastställd och gällande idag och som vi tar med oss in i det nya försvarsbeslutet, vår insatsorganisation 2004 varav ett antal förband är anmälda till olika styrkeregister.

3.3 Förmågor för elektronisk krigföring idag

Vilka förband i insatsorganisation 2004 från regeringens proposition från 1999 är idag att betrakta som insatsförband? Definitionen säger exempelvis att de ska bestå av kompletta enheter, personalen ska vara anställd eller ha kontrakt, vara färdigutbildade och ha 0–90 dagars beredskap, men kan också vara i tjänst vid förbandet. Utlandsstyrkan består av personal och förband som är insatta i internationella insatser runt om i världen och räknas alltså till våra insatsförband. Vi har för tillfället 770 man i utlandsstyrkan fördelat på ett antal observatörer, monitorer, gränsövervakare, verifikatörer, delegater, stabsofficerare, samverkans-officerare, och mindre förbandsenheter av kompanis storlek i Kosovo och Liberia.[97] Alla i utlandsstyrkan ingående enheter kommer ur de förband som är anmälda till de olika styrkeregisterna. Samtliga förband som är anmälda till dessa register uppfyller också definitionen för insatsförband. Övriga delar av Försvarsmakten är inte att betrakta som insatsförband, främst eftersom de inte har den beredskap som krävs (1 april 2005).

Vilken förmåga avseende elektronisk krigföring har då dessa insatsförband, vilka antingen redan är insatta runt om i världen eller står i beredskap som

---

[95] Karlsson, ”Behov och krav på förmågor för markstridskrafter vid lågintensiva konflikter”, s. 99.
[96] Moore, generalmajor Michael (2005), *EU:s insatsstyrka bäddar för svensk yrkesarmé* (Stockholm: DN.se), Dagens Nyheter, nätupplagan 17 april 2005 [www]. Hämtat från <http://www.dn.se/DNet/jsp/polopoly.jsp?d=1042&a=404306> 28 april 2005.
[97] Försvarsmakten (2005), *Personal i utlandsstyrkan 1 april 2005* (Stockholm: mil.se) [www]. Hämtat från <http://www.mil.se/int/attachments/us-april-2005.pdf> 28 april 2005.

anmälda till de olika styrkeregisterna? Televapentroppen som är insatt i Kosovo är ett tydligt exempel och det enda förbandet där elektronisk krigföring är en huvuduppgift.

Televapentropp 04 INT är en del i den telekrigbataljon som ingår i insatsorganisation 2004 och är organiserad med materiel ur ett avvecklat Televapenkompani 87R som till del har modifierats. Troppen är en interimslösning för att säkerställa telekrigsförmåga vid internationella insatser intill ett nytt telekrigsförband tagits fram. Televapentroppen ska kunna understödja annat svenskt eller allierat insatsförband och dess huvuduppgift är telekrigföring inom kommunikationsområdet, främst i form av signalspaning men även emissionskontroll av egna signalkällor (emission control, EMCON) och störning i begränsad omfattning. Målet kan utgöras av militära radiosystem eller civila enkla handburna radiostationer med fixfrekvens inom VHF- och UHF-området[98]. Troppen ska vara en del i det understödda förbandets integrerade underrättelse- och bekämpningssystem och ska främst bidra till skydd av egna och allierade styrkor (force protection). Troppen ska dessutom kunna bidra till kontroll över egna och allierade förbands positioner i syfte att undvika vådabeskjutning, så kallat ”combat identification” (combat ID). Den hotbild som beskrivs i troppens målsättningsdokument omfattar exempelvis milis, gerillaförband, kriminella och andra grupperingar med lättare utrustning inklusive IED (improvised explosive device). Civila mobbar som uppviglas till stenkastning, plundring och lynchning ingår också. Målsättningen säger också att om televapentroppen under lång tid, mer än sex månader, ska kunna lösa sina huvuduppgifter krävs en återkommande anpassning för att möta konfliktens utveckling avseende aktörernas kommunikationssystem, exempelvis nya frekvensområden och överförings-former.[99]

Av marinens insatsförband, SWENARAP, är det framför allt internationella korvettstyrkan och internationella ubåtsstyrkan som har avancerade sensorer. Ubåten är av Gotlandsklassen och korvettstyrkan består av Stockholmsklassen. Marinens insatsförband har tillsammans en rad olika sensorer ombord, exempelvis navigationsradar, spanings- och eldledningsradar mot luftmål, aktiv och passiv sonar för sökning respektive klassificering, och passiv signalspaningsutrustning för upptäckt och klassificering av radarsignaler.[100] Beskriven hotbild påverkar inte SWENARAP avseende elektronisk krigföring mer än i mycket begränsad omfattning. SWENARAP bedöms därför ha tillräcklig förmåga i detta avseende.

Flygvapnets insatsförband SWAFRAP är anmält till olika register i spanings- och jaktrollen. Förbandet ska dels kunna skydda angivet luftrum, territorium, flygbas och flygföretag, dels kunna genomföra begränsade flygspaningsföretag (radarspaning). I SWAFRAP ingår JAS 39-A Gripen vilken är utrustad med PS-05 pulsdopplerradar med multimod, FLIR (forward looking infra red) och laserpekare. Gripen har en låg signatur mot både radar- och IR-målsökare men är i internationell tjänst också utrustad med varnings- och motverkanssystem (VMS) innehållande en kompetent radarvarnare, remsor och

[98] Very High Frequency, VHF, omfattar 30–300 MHz. Ultra High Frequency, UHF, omfattar 0,3–3 GHz.
[99] Försvarsmakten (2004), *Preliminär taktisk, organisatorisk och ekonomisk målsättning för TELEVAPENTROPP 2004 INT PTOEM TVA-to 04 INT* (Stockholm: Högkvarteret).
[100] Försvarsmakten (2005), *Beredskapsenheter* (Stockholm: Försvarsmakten), flera sidor kopplade till artikel [www]. Hämtat från <http://www.mil.se/int/article.php?id=274#> 24 oktober 2005.

facklor.[101] Facklorna har dock begränsad verkan mot MANPAD-hotet, delvis beroende på bristande robotskottvarning.[102] Samma problem med skydd mot MANPAD gäller även VMS för TP 84 Hercules. Under flygningar med Hercules i Afghanistan kompletterades befintligt VMS med optisk spaning i tre riktningar. Besättningspersonal hade utkik efter robotskott och kunde manuellt aktivera facklor via en knapptryckning.[103]

S 102B ingår som en till registerförbanden anmäld nationell resurs. Flygplanet bedöms ha mycket god kapacitet för signalspaning mot radarsignaler och radiokommunikation. Tekniska prestanda på signalspaningsutrustningen i S 102B är i övrigt sekretessbelagd. Nackdelen med flygplansbaserad signalspaning är uthålligheten i luften, vilket för kommunikationsspaning gör det svårt att få långa sammanhängande avlyssningstider. Fördelarna är den ökade räckvidden som den avsevärt högre antennhöjden ger. Därför bör S 102B användas i kombination med markbaserad signalspaning vilken har uthålligheten, men kortare räckvidd. S 102B bedöms minst ha samma begränsningar i skydd mot MANPAD som övriga flygande enheter.

[101] Försvarsmakten, *Beredskapsenheter*, flera sidor kopplade till artikel.
[102] Sjöqvist, övlt Sten, Högkvarteret, föreläsning för chefsprogrammet på F 21 2005-09-05.
[103] Björs, övlt Christer, Flygtaktiska kommandot, föreläsning vid Försvarshögskolan 2005-09-16.

Kapitel 4
SAMMANFATTANDE SLUTSATSER

[…] man får inte av humanitet efter hand göra de insatta vapnen overksamma intill dess någon åter uppträder med skarpt svärd och hugger av armarna av oss.[104]

Carl von Clausewitz

4.1 Inledning

I det här kapitlet jämförs de identifierade lågintensitetshoten med befintliga förmågor i våra insatsförband. Utifrån empirin i kapitel 2 och 3 görs en bedömning av vilka brister avseende elektronisk krigföring som våra insatsförband har idag när de ska verka mot icke-reguljära aktörer i en modern lågintensitetskonflikt. Bristerna redovisas här nedan som sammanfattande slutsatser.

4.2 Brister och behov - slutsatser

Utvecklingen av förband och förmågor i Försvarsmakten har ända fram till idag varit en vidareutveckling av vår traditionella krigsorganisation, det så kallade arvet. Våra insatsförband idag är alltså inte i grunden dimensionerade för lågintensitetskonflikter och visar därför på betydande brister, särskilt belyst i denna uppsats avseende förmågan till elektronisk krigföring. Bristerna omfattar dessvärre en del dyrare högteknologiska sensorer exempelvis satellitspaning, höghöjds-UAV och SAR. Den samlade bilden pekar på att det finns ett stort behov av nya tekniska förmågor.

De icke-reguljära hoten i en lågintensitetskonflikt vilar på en grund av lågteknologiska vapen exempelvis handeldvapen och hemmagjorda bomber. Det ledarlösa motståndets princip med organisering i nätverk har lett till att motståndaren kommunicerar med modern billig informationsteknologi för att koordinera och leda insatser. De högteknologiska inslagen domineras alltså av civila kommersiella kommunikationssystem exempelvis Internet, mobiltelefoni och satellittelefoni. Mobiltelefoni såväl som annan radiokommunikation används både för talkommunikation och för att fjärrstyra detonering av bomber. Våra insatsförband vilar idag på arvet av optimering mot det gamla invasionshotet vilket enbart omfattade sovjetiska reguljära förband med analoga och specifikt militära materielsystem. Trots denna optimering mot analoga radiosystem saknar våra insatsförband idag kapacitet att verka mot kortvågsradio. När det gäller de civila kommersiella systemen har vi i princip ingen förmåga alls. Kontentan av detta är att förmågan att verka mot äldre analoga system måste utvecklas, men framför allt måste insatsförbanden ges förmågan att verka mot civila kommersiella system.

Varje lågintensitetskonflikt är unik till sin karaktär. Att idag förutsäga karaktären på en konflikt om ett år är mycket svårt, även om går att göra sannolika bedömningar av en del tekniska karaktäristika. Förståelse för vem motståndaren

[104] Clausewitz, *Om kriget*, s. 236.

är, de lokala förhållandena och stämningarna i konfliktområdet blir här helt centralt. Underrättelsetjänsten måste alltså fokusera mer på de olika lokala och kulturella förutsättningarna. De traditionellt militära analysmetoderna måste samordnas med metoder från andra områden såsom de finansiella, tekniska och polisiära. När man drar det till sin spets framstår det som särskilt viktigt att med god precision kunna skilja kombattanter från oskyldiga civila. Annars når vi inte den verkan med våra system som vi önskar. Ledstjärnan i allt detta är att kombinera flera olika typer av underrättelseförmågor såsom SIGINT, IMINT, HUMINT, OSINT inklusive direktriktat stöd från olika underrättelse-organisationer hemma i Sverige. Här ingår även ett brett nyttjande av olika plattformar exempelvis farkoster i luften och i rymden. Framför allt SIGINT men även IMINT i form av fotospaning, satellitspaning och syntetisk aperturradar lämpar sig väl till att inrikta andra tekniska sensorer med högre precision såväl som HUMINT. Den elektroniska krigföringen med sina olika tekniska sensorer är alltså i detta sammanhang en mycket viktig delkomponent. Slutsatsen blir att det finns ett stort behov av en ökad inhämtnings- och analysförmåga både före och under en svensk insats. Detta uppnås **både** genom ökat **internationellt samarbete** och en mycket god **egen underrättelseförmåga**, vilket inte minst understryks av Hollands dyrköpta erfarenheter från Srebrenica 1995.

Typiskt för icke-reguljära aktörer i en lågintensitetskonflikt är att de har initiativet. De kan ofta bestämma tid och plats för sina attacker samt hur länge de ska pågå. Vi måste därför hela tiden sträva efter att komma innan för motståndarens beslutscykel och därmed möjliggöra att vi kan ta initiativet. Det innebär att vår förmåga att kunna förutse vad motståndaren ska göra blir helt central. En förutsättning för detta är god kunskap om motståndaren och förståelse för hans doktrin och taktik. En annan förutsättning är att processerna i vår egen beslutscykel är effektiva både vad gäller snabbhet och kvalitet. En viktig del i detta är förstås en väl fungerande underrättelsetjänst med kombination av flera olika typer av underrättelseförmågor som ledstjärna. Slutsatsen om behovet av en ökad inhämtnings- och analysförmåga både före och under en svensk insats som uppnås **både** genom ökat **internationellt samarbete** och en mycket god **egen underrättelseförmåga** accentueras därmed ytterligare.

Motståndaren kan komma att styra striden till miljöer där det är svårt för våra insatsförband att effektivt använda konventionella vapen och moderna precisionsvapen. Exempel på sådana miljöer är storstäder, industriområden med farliga ämnen, bergsgrottor och otillgängliga djungler. I stadsterräng är det särskilt viktigt att inte oskyldiga civila skadas. Sensorer som kan lägesbestämma med hög precision i dessa typer av terräng blir vitala för att vi ska kunna nå avsedd verkan. Alternativet är att tvinga motståndaren att lämna den svåra miljön och därmed göra honom bekämpningsbar. Sensorer med hög precision är dock ofta i behov av invisning från mera yttäckande sensorer och sensorer som har förmågan att exempelvis ”se genom vegetation”. Detta sätt att kombinera sensorer snabbar upp både underrättelsecykeln och beslutscykeln vilket medger snabb respons. Både snabb respons och insatser som verkar med såväl hög precision som väl avvägd styrka (graderad verkan) bidrar till effektivitet, trovärdighet och därmed legitimitet. Det kan även verka avskräckande och därmed de-eskalerande. Återigen kan man konstatera ett behov av att kombinera flera olika typer av underrättelseförmågor där olika tekniska sensorer utgör en viktig del. Återigen accentueras slutsatsen om behovet av en ökad inhämtnings- och analysförmåga

både före och under en svensk insats som uppnås **både** genom ökat **internationellt samarbete** och en mycket god **egen underrättelseförmåga**.

Våra västliga demokratier är känsliga för förluster av både egen trupp och oskyldiga civila. Detta utnyttjas av de icke-reguljära aktörerna, olika bombdåd är ett uttryck för detta. Genom att satsa på förmågor som inte kräver soldater i olika intresseområden reducerar vi motståndarens möjligheter att utnyttja detta faktum. Slutsatsen blir att satsningar på sensor- och verkanssystem på obemannade fjärrstyrda plattformar ska prioriteras, exempelvis satellitspaning, SIGINT, SAR och optisk spaning från UAV. Om möjligheten finns ska rättigheten till alla satellitbilder från civila satelliter köpas för att neka motståndaren tillgång till denna typ av högteknologisk sensor.

MANPAD-hotet begränsar av samma anledning både civil och militär flygverksamhet. Tidig varning är ett stort problem och facklor som skydd har begränsad verkan mot moderna MANPAD-system. Kontentan blir att egenskyddet av flygande plattformar behöver förstärkas.

Många icke-reguljära aktörer har förstått effekterna av västvärldens högteknologiska sensorsystem. De har därför undvikit stationära ledningsfunktioner och vidtagit åtgärder för att dölja sig, exempelvis radiotystnad och kryptering av information. För oss innebär det att vi måste nyttja flera sensorer för att kunna upptäcka och lägesbestämma. För motståndaren har det blivit viktigt att snabbt kunna förflytta sig utan att väsentligt degradera ledningsförmågan. Trådlös kommunikation är här överlägsen och den snabba utvecklingen inom informationsteknologi erbjuder många sådana möjligheter, exempelvis satellittelefoni och mobiltelefoni. Uppgifter som finns om Internetanvändning säger inget om det är trådlösa utrustningar som används, men sannolikheten torde vara hög att så varit fallet. Kontentan är alltså en bred uppsättning med olika typer av sensorer som samverkar i syfte att göra det svårt för motståndaren att lyckas med sina motåtgärder. Återigen upprepas slutsatsen om behovet av en ökad inhämtnings- och analysförmåga samt **både** ökat **internationellt samarbete** och en mycket god **egen underrättelseförmåga**.

Kapitel 5
VAD MEDGER TEKNIKEN?

Att politiken skulle ställa krav på kriget, som detta inte kan infria, vore mot förutsättningen att politiken kände det instrument, som det avsåg att utnyttja – det vore alltså emot en naturlig och helt oavvislig förutsättning.[105]

Carl von Clausewitz

5.1 Inledning

När det nu konstaterats att våra insatsförband har stora brister avseende elektronisk krigföring väcker det många frågor. Hur mycket känner den politiska nivån till om detta? Förstår dom sitt eget verktyg? Hur agerar vi på ett professionellt sätt? Hur ärliga är vi mot politikerna, och mot oss själv och våra soldater? Men den fråga som detta kapitel ska svara på är: Hur kan vi möta de brister som våra insatsförband har avseende elektronisk krigföring? Det naturliga svaret är kanske att köpa nya utrustningar. Nog så riktigt och viktigt som detta svar är ska man alltid se insatsförbanden som hela system med både människor och teknik. Saker som systemintegration, färdigheter, doktriner, motivation och vilja spelar stor roll. Ibland låter vi oss styras av framtidsutsikter i sådan stor utsträckning av vi glömmer det vi redan kan, vårt arv. Dessutom finns den ekonomiska verkligheten som vi lever i. Den är kanske den mest styrande faktorn för Förvarsmaktens utveckling idag. I detta kapitel ska dessa begränsande faktorer frikopplas till förmån för en strikt teknisk undersökning om vad som är möjligt att realisera inom en femårsperiod. Vad finns redan idag att anskaffa till våra insatsförband? De fakta som presenteras är hämtade från en mängd olika källor. De viktigaste har dock varit olika forskare och standardiseringsinstitut.

5.2 Sambandssystem

GSM (Global System for Mobile Communications)

Mobiltelefonsystemen är olika från land till land. De kan ha system från olika teknikgenerationer, men andra generationens mobiltelefonsystem (GSM) är med sina mer än 200 länder det klart dominerande.[106] Även om de är av samma generation kan de ha olikheter, exempelvis olika frekvensutnyttjande, krypteringsalgoritmer och säkerhetslösningar. Det är därför viktigt att kunna anpassa signalspaningssystemet så att det optimeras mot den aktuella systemlösningen som gäller i ett konfliktområde.

GSM har uppvisat ett antal svagheter vad gäller säkerheten: det är fullt möjligt att via en falsk basstation göra aktiva attacker, kryptonycklar och autentiseringsdata överförs oskyddade mellan och inom nätverk, radiolänktrafiken mellan basstation och in till det övriga mobiltelefonnätet är oskyddad, kryptering används inte i alla uppbyggda system och mobiltelefonens identitetsnummer

[105] Clausewitz, *Om kriget*, s. 618.
[106] GSM World (2005), *GSM Global Networks on Air* (London: GSM Association) [www]. Hämtat från <http://www.gsmworld.com/news/statistics/networks_complete.shtml> 8 juli 2005.

(IMEI) är inte skyddat. Dessutom har GSM sådana brister i systemuppbyggnaden att säkerhetslösningar inte kan uppgraderas och förbättras.[107]

En metod för avlyssning av GSM är att utnyttja de befintliga operatörernas egna system. Personalen sätter sig helt enkelt hos operatören och sköter avlyssningen med minimalt med egen utrustning. Denna metod erbjuder också med rätt utrustning och mjukvara att mobiltelefoner kan lokaliseras via triangulering från flera basstationer.[108] Troligtvis är detta inte aktuellt då det involverar lokalbefolkning i en verksamhet som man vill ha så dold som möjligt. Dessutom finns alltid risk för läckor via operatörens egen personal vilken kan ha egna intressen i den lokala konflikten eller utsättas för påtryckningar av de icke-reguljära styrkorna och dess ledare. Vidare så blir den egna personalen väldigt stationär, vilket försvårar att i samverkan med andra förbandsenheter förfölja ett mål som förflyttar sig före, under och efter ett samtal.

En annan metod är att upprätta en egen basstation mellan aktuella mobiltelefoner och operatörens basstation. Varken operatören eller mobiltelefonen upptäcker den falska baststationen, en så kallad ”man in the middle”. Samtal länkas sedan vidare mellan mobiltelefonen och operatören vilket gör det enkelt att avlyssna utan att blanda in andra mobiltelefoner i området. Identifiering sker via abonnemangets/SIM-kortets identitetsnummer (IMSI) alternativt ett tillfälligt tilldelat sådant (TMSI), abonnemangets identitetsnummer som krävs för internationella samtal (MSISDN) vilket innehåller abonnemangets telefonnummer, och/eller IMEI.[109] Den egna basstationen får lätt plats i en bil och kan alltså vara rörlig.

En tredje metod är att avlyssna den oskyddade radiolänktrafiken mellan basstationer och operatörens övriga nätverk.[110] Här är trafiken helt okrypterad och lätt att exploatera. Nackdelen är att det blir en statisk gruppering, vilket gör det mycket svårt att taktiskt följa en mobiltelefon som förflyttar sig.

En fjärde metod för avlyssning av GSM är att fånga signalerna mellan mobiltelefoner och basstationer. Ett sådant signalspaningssystem arbetar helt passivt och kan detektera båda trafikkanalerna under ett mobiltelefonsamtal, upp- och nerlänk, för att utvinna underrättelser. Signalspaningssystemet kan även detektera kontrollkanalerna vilket är nödvändigt för att kunna fullfölja avlyssning då ett samtal byter basstation. Denna typ av system finns för olika multiplextyper, exempelvis FDMA/TDMA (GSM) och WCDMA (3G). Systemen skannar automatiskt samtliga kanaler och låter användaren sortera ut intressant trafik. SMS kan också detekteras.[111] Identifiering sker också här via IMSI, TMSI, MSISDN och/eller IMEI. Denna typ av signalspaningssystem upptar väldigt litet utrymme och ryms därför lätt i en bil och den nödvändiga dekrypteringen är integrerad i systemen. Med rundstrålande antenner kan signaler från basstationen detekteras på några mils avstånd, men signaler från mobiltelefoner kräver korta avstånd

---

[107] 3GPP (1999), *3G TR 33.120 version 3.0.0* (Frankrike: 3GPP), s. 6–7.
[108] Homeland Security Strategies, *Cellular Intercept Systems* (USA: Security Intelligence Technology Group), flera sidor på hemsidan [www]. Hämtat från <http:// www.cellularintercept.com/default.aspx> 8 juli 2005.
[109] Pagliusi, Paulo S. (2002), ”A Contemporary Foreword on GSM Security”, Davida, George; Frankel, Yair och Rees, Owen (eds.) *Infrastructure Security: International Conference, InfraSec 2002 Bristol, UK, October 1-3, 2002 Proceedings* (Berlin: Springer), s. 139 [www]. Hämtat från <http://www.isg.rhul.ac.uk/msc/teaching/ic3/GSM_ Security_v4.pdf> 8 juli 2005.
[110] Pagliusi, ”A Contemporary Foreword on GSM Security”, s. 137.
[111] Homeland Security Strategies, *Cellular Intercept Systems,* flera sidor på hemsidan.

mindre än en kilometer.[112] Denna metod innebär dessutom att man blir starkt beroende av terränghinder, höghusbebyggelse och annat som påverkar vågutbredningsförhållandena.

Störning är det klassiska sättet att hindra all radiotrafik. GSM är enkel att störa ut om fixfrekvens används, men om frekvenshopp utnyttjas krävs lite mer av störutrustningen. GSM:s frekvenshopp är dock både långsam och begränsad till ett smalt frekvensband. Därför är bredbandig störning med hundratals watt på avstånd upp till en kilometer från abonnenten tillräckligt. Ett alternativ är en falsk basstation som tar över en abonnent och blockerar all trafik till/från.[113]

3G

När säkerhetslösningarna för 3G togs fram byggde man vidare på GSM-systemet i grunden, men korrigerade de svagheter som man upptäckt med tiden. Framför allt förbättrades kryptering och autentisering mellan mobiltelefon och basstation. Kryptonycklarna har exempelvis ökat från 54-bitars till 128-bitars.[114] Till skillnad från GSM har 3G dock inbyggd funktionalitet för laglig avlyssning via operatörernas nät.[115] Slutsatsen blir att man i 3G stängt de allvarligaste säkerhetsluckorna som fanns i GSM samtidigt som man gjort möjligheten till laglig avlyssning mer kontrollerad och synlig för operatörerna.

Det finns trots allt svagheter med 3G: alla hot mot en vanlig Internetansluten pc i hemmet existerar även för en mobiltelefon i 3G, IMSI sänds i klartext när en användare registrerar sig för första gången i ett nät, och en abonnent kan tas över av en falsk basstation.[116] Om man inte vill utnyttja möjligheten till laglig avlyssning via operatören utan göra det ”olagligt”, krävs att krypteringen knäcks eller att en komprometterad krypteringsnyckel används i kombination med en falsk basstation.[117]

För att störa ut 3G krävs en störmetod som har verkan mot den frekvenssprida signalen (WCDMA). Mobiltelefonen kommer att reagera med att vilja få mer signaleffekt från sin basstation, vilket bara är en tillfällig förbättring. När signaleffekten ökar påverkas andra abonnenter i närheten. Deras interferensnivå ökar och om basstationen ger mer signaleffekt kan det leda till att nätets totala signaleffekt inte räcker till alla abonnenter. En mobiltelefon som nås av flera basstationer när den ska anslutas till ett nät väljer den som hörs bäst. Men om störningsnivån är hög vid mobilen får den svårt att hitta signalen som släpper in den på nätet.[118] På samma sätt som för GSM kan en falsk basstation ta över en abonnent och därmed blockera all trafik till och från abonnenten.[119]

---

[112] Accelerated Promotions (2005), *Cellular Phone GSM TDMA Interceptor Pro System* (USA: Accelerated Global Inc.) [www]. Hämtat från <http://www.accelerated-promotions.com/consumer-electronics/cellular-interception-gsm-system-specifications.htm> 8 juli 2005.
[113] Pagliusi, ”A Contemporary Foreword on GSM Security”, s. 140.
[114] Ibid, s. 141–142.
[115] ETSI (2005), *ETSI TS 133 107 V6.5.0* (Frankrike: ETSI), s. 6.
[116] Campbell, professor Roy m.fl. (2002), *Analysis of Third Generation Mobile Security* (Chicago: University of Illinois at Urbana-Champaign), presentationsmaterial från Motorolas årliga projektrapportering 28 juni 2002 [www]. Hämtat från <http://srg.cs.uiuc.edu/MobilSec/posted_docs/3G_Security_ Annual_Report.ppt> 10 juli 2005.
[117] 3GPP (2000), *3G TR 33.900 version 1.2.0* (Frankrike: 3GPP), s. 9–12.
[118] Fors, Karina och Stenumgaard, Peter (2003) ”Elektronisk vådaskott viner i luften”, *Framsyn*, 2003, nr 2 (Stockholm: Totalförsvarets forskningsinstitut), s. 31–33.
[119] 3GPP, *3G TR 33.900 version 1.2.0*, s. 8–9.

Satellitkommunikation

Satellitkommunikation har fördelen att olika användare förutom att vara mobila dessutom kan befinna sig i områden där det inte finns fasta marknät exempelvis på hav, i ökenområden och i regnskogar. Varje satellit är i praktiken en relästation. Satellitens kommunikationskärna är transpondern som är en kombinerad sändare och mottagare vilken tar emot på en frekvens och som efter bearbetning och förstärkning ombord återutsänder på en något ändrad frekvens. En satellitsändare kan lätt nå ett mycket stort antal mottagare och ombordbearbetning medger ökade möjligheter till kryptering. De geostationära satelliterna på 35 800 km över ekvatorn är dominerande för kommunikationssatelliter, men även lägre höjder används. Fördelen med de geostationära satelliterna är att en och samma satellit skenbart står stilla över en och samma punkt på ekvatorn. Hela jorden kan då täckas med endast tre satelliter. För att täcka polarområdena krävs dock minst tre satelliter till i den så kallade Molniyabanan. Vid överföring av data som kan förbehandlas är kryptering ett bra informationsskydd. Vanlig civil satellittelefoni har dock inte samma hårda säkerhetskrav som de militära. Det som tydligast skiljer satellittelefoner åt är typen av antenn. För de geostationära systemen används riktantenner (paraboler) och för systemen med lägre banhöjder oftast rundstrålande eftersom dessa satelliter hela tiden rör sig i förhållande till jordytan, de kan lika gärna vara rakt över huvudet som precis i horisonten. Det är dock ganska lätt att räkna ut en låghöjdssatellits läge, vilket gör att riktantenner är möjliga att använda. Sändareffekten på upplänken varierar från tiondels watt till tiotals watt beroende på system. Det finns i dag flera civila satellit-kommunikationssystem i bruk. Iridium och Globalstar är exempel på civila låghöjdssystem för telefoni och små datamängder.[120] Inmarsat är ett exempel på ett civilt geostationärt satellitkommunikationssystem för telefoni och dataöverföring via bredband.

Signalspaning mot satellitkommunikation kan genomföras på flera sätt: exploatera sidlober från aktuell markstation, tappa av radiolänktrafik mellan markstationer i aktuellt system, exploatera signaler direkt från satellittelefoner, men vanligast är att rikta signalspaningssystemets antenn mot aktuell satellit. Det berömda avlyssningssystemet Echelon är uppbyggt efter just denna metod. Efter mottagning analyseras den bredbandiga signalen vilken delas upp i sina respektive kanaler. Kanalerna delas normalt in i tre intressekategorier: telefoni, fax och analog modemtrafik. Trafikanalys tar vid vilken exempelvis ger information om både uppringande och uppringd abonnent. Vidare görs analys av trafikmönster. När läsbara textmeddelanden extraherats vidtar igenkänning av nyckelord via en ordboksdator (dictionary computer) vilket leder till en grovsortering av stora mängder meddelanden. En mer avancerad metod för analys av textmeddelanden är så kallad N-gram. N-gram ignorerar nyckelord och baserar istället sin analys på valda skrivna dokument för att räkna fram sannolikheten för att ett annat dokument avhandlar samma ämne. Det bör noteras att handskrivna faxmeddelanden undgår denna typ av analys. System för att analysera tal på

[120] Ekblad, Ulf (2005), *Elementa om rymdteknik – Satelliter, spaning och kommunikation* (Stockholm: Totalförsvarets forskningsinstitut), s. 11–13, 45–47 och 55.

samma sätt med igenkänning av nyckelord eller ämne, eller andra tekniker som exempelvis röstigenkänning av individer, är inte tillräckligt tillförlitliga i dag.[121]

Satellitkommunikation kan störas på två sätt: satellitens mottagare eller markmottagarna. När det gäller geostationära satelliter är störning av satellit-mottagaren det mest effektiva eftersom alla markmottagare då störs ut samtidigt. Denna typ av störning kräver hög sändareffekt. För störning av markmottagare krävs visserligen lägre sändareffekt, men störningen måste oftast riktas mot en specifik mottagare i taget. Markmottagare för låghöjdssystem är känsligare för störning än för de geostationära, främst beroende på att rundstrålande antenner underlättar både upptäckt och störeffekt jämfört med riktantenner med smala lober. Genom att utrusta mottagarna med gruppantenner kan störriktningar släckas ut och därmed reducera störsändningens inverkan.[122] På samma sätt som olagliga intrång är möjliga i datorer är det möjligt i satelliters datorer, antingen för att hindra kommunikation (jämför störning) eller implementera virus. Ett mer sofistikerat sätt är att förvanska utgående trafik till mottagare på jorden, men detta kräver djupgående kunskap om det aktuella satellitsystemet.[123]

Kortvågsradio

Kortvåg används för långa förbindelseavstånd genom att radiovågorna reflekteras i jonosfären tillbaka till jordytan. Mycket långa räckvidder kan uppnås genom upprepade reflektioner. I militära samanhang är det vanligt med snabbsändande radiosystem i syfte att hindra en motståndares signalspaning att upptäcka och exploatera nyttosignalen. Det tar bara ett par sekunder att sända iväg en A4-sida med text. Kortvågstrafiken kan därför betraktas som en "djungel" där man lätt kan gömma illegala snabbsändare. För att upptäcka snabbsändande emittrar krävs att ett signalspaningssystem använder filterbankmottagare. Annars blir sannolikheten att upptäcka signalen inom spaningsbandbredden alltför liten. Filterbankmottagare utnyttjar det smalbandiga systemets fördelar med liten brusbandbredd och god signalseparation, men också förmågan att momentant övervaka ett mycket brett frekvensområde. Mycket avancerade signalspaningssystem har utvecklats på FOI för att upptäcka och pejla in snabbsändande emittrar. [124]

För kortvåg används modulationstyperna AM (amplitudmodulering) och SSB (single side band). För att störa ut dessa krävs högre effekter än de vanliga radiobanden som nyttjar FM (frekvensmodulering). Ju mer amplitudlinjär demodulationstekniken är desto högre effekter krävs. SSB är den mest amplitudlinjära demodulationen av de tre och kräver cirka 20 dB starkare störsignal än nyttosignal. AM kräver cirka 10 dB starkare och FM cirka 3 dB.[125] Duktiga telegrafister som nyttjar kortvåg anses dock mycket svåra att störa ut.[126]

---

[121] Campbell, Duncan (1999), *Development of Surveillance Technology and Risk of Abuse of Economic Information*, part 2 (Luxemburg: European Parliament), s. 4–6, 11–15, 19–20 samt Technical Annexe, s. i–vi [www]. Hämtat från <http://www.europarl.eu.int/stoa/publi/pdf/98-14-01-2_en.pdf> 13 juli 2005.
[122] Ekblad, *Elementa om rymdteknik – Satelliter, spaning och kommunikation*, s. 48.
[123] Höstbeck, Lars (ed.) (2003), *Space and Defence* (Stockholm: Totalförsvarets forskningsinstitut), s. 39.
[124] FOI (2005), *FOI orienterar om: Telekrig*, 2005, nr 5 (Stockholm: Totalförsvarets forskningsinstitut), s. 11–12 och 24–25.
[125] Arnsby, Jan (2004), *Radiomotmedel: Störning av radiokommunikation* (Linköping: Totalförsvarets forskningsinstitut, rev 4.7), s. 28–29.
[126] FOI, *FOI orienterar om: Telekrig*, s. 28.

5.3 IEDD (Improvised Explosive Device Disposal)

Radiosignaler som utlöser en bomb är svåra att hitta med signalspaning då de kan vara mycket kortvariga och dessutom gömma sig i en bakgrund av likartade men fullt legala signaler, exempelvis GSM. Men det är fullt möjligt att skydda ett objekt genom att i **preventivt** syfte störa ut **kända** signaler som exempelvis GSM och enkla analoga radiomottagare. Kommersiella produkter finns på marknaden för montering i byggnader, stora arenor, UAV:er, bilar och attachéväskor samt i ryggsäcksutförande. De sänder störsignaler på ett stort frekvensband med särskild förstärkning på frekvenser som är vanligt använda för fjärrutlösning, exempelvis mobiltelefoni, satellittelefoni, handburna analoga radioutrustningar och radiostyrda leksaker. Några system är kombinerade med signalspaningsdelar för upptäckt, klassificering och lokalisering av radiosignaler. Dessutom finns system för att detektera elektronisk utrustning i en misstänk bomb. De använder samma teknik som används för att hitta dolda mikrofoner eller lavinoffer i skidbackar där man under bestrålning av ett objekt söker efter andra och tredje övertonen (non linear junction detection, NLJD).[127] Samma teknik används även för stöldlarm i klädbutiker. Att störa fjärrutlösare på detta sätt ger oss dock inte några garantier. Hur vet man att inte bomben är så konstruerad att den utlöses om brusineffekten når tillräckligt hög nivå? Det är tänkbart att använda denna teknik som en försåtsminering, ett slags motmedel mot våra störutrustningar. Att störa i preventivt syfte är fullt möjligt, men det finns alltså all anledning att fundera över det taktiska uppträdandet.

5.4 CNO (Computer Network Operations)

Internet

Underrättelseinhämtning om en motståndare som använder Internet kan i princip genomföras från tre olika platser i ett datornätverk: en länk, en nod eller en klient. De finns flera olika sorters *länkar* exempelvis fiberkabel, satellitkommunikations-länk och radiolänk. Länken avlyssnas, data utvinns och analyseras i syfte att finna information om motståndaren och dennes verksamhet. Echelon som beskrivits ovan är ett exempel på inhämtning från en satellitkommunikationslänk. Inhämtning från en *nod* är mjukvarubaserad och sker vanligen från en server i ett nätverk, exempelvis en ISP (internet service provider). IP-paketen i datatrafiken filtreras och analyseras, vilket leder till att innehåll i e-post, filöverföringar och hemsidor kan utvinnas. Inhämtning från en *klient* baseras på olika sorters sökmotorer. Det finns tre huvudskaliga grupper: webrobotar, katalogiserande sökmotorer och meta-sökmotorer. Ytterligare en sofistikerad metod är att dolt installera en programvara som beordras leverera resultat till beordrande dator, en så kallad trojan. Webrobotar söker kontinuerligt av Internet i syfte att bygga upp en databas om befintliga hemsidor och dess innehåll, exempelvis Google. Möjligheten finns att söka efter särskilda filtyper, exempelvis alla textfiler. En webrobot som Google kan också användas för att undersöka strukturen hos en server innan man genomför ett intrångsförsök. Katalogiserande sökmotorer söker efter utvalda resurser och grupperar dom i kategorier, exempelvis Yahoo.

[127] Security Intelligence Technologies Group, *Bombjammer.com* (USA: Security Intelligence Technology Group), flera sidor på hemsidan [www]. Hämtat från <http://www.bombjammer.com/default.aspx> 12 juli 2005.

Sökningen kan då snabbt smalnas av till aktuellt intresseområde. Meta-sökmotorer har normalt ingen egen databas utan använder flera andra sökmotorer. Ett exempel på en meta-sökmotor är Copernic. Ett problem är att informationen på Internet är föränderlig. För att överbrygga detta kombineras flera metoder. En metod är att använda flera sökmotorer samtidigt. En annan metod är att koppla upp sig mot en intressant källas hemsida. Särskilt svårt är att inhämta information från P2P (peer-to-peer) där användare kopplar upp sig direkt mot varandra via Internet och utbyter filer med varandra, exempelvis Kazaa. För detta måste speciella sökmotorer användas, exempelvis Moglo. De delar av Internet som inte är direkt åtkomligt kallas det osynliga nätet. Vanliga sökmotorer når inte de databaser som endast presenterar sitt innehåll som ett resultat av en direkt fråga. Här krävs speciella ”verktyg”. Ett alternativ är att köpa information från kommersiella leverantörer, exempelvis nyhetsleverantören Factiva.[128]

WLAN (Wireless Local Area Network, radio-LAN)

Det finns tre principiella transmissionstekniker för WLAN: infraröda signaler, bredbandiga radiosignaler och smalbandiga radiosignaler. Bluetooth är också teknik för trådlösa nätverk men klassificeras ofta som WPAN (wireless personal network). Bluetooth används för enkla **tillfälliga** (ad-hoc) uppkopplingar på **mycket** korta avstånd (5–10 meter) med mobiltelefoner, bärbara pc och andra bärbara elektroniska utrustningar. Bluetooth ska ses som ett komplement till WLAN vilket istället används för mer **permanenta** uppkopplingar på **relativt** korta avstånd (30–150 meter) i standardiserade LAN där resurser delas mellan klienterna.[129] Problemet med alla trådlösa nätverk är att det inte finns fysiska länkar mellan noderna. Noderna i nätverket sänder över ett gränssnitt i luften, alltså kan att alla inom räckvidden detektera signalerna. Detta innebär att alla standardrisker i datornätverk existerar **plus** risken för avlyssning.

IEEE 802.11 är en familj av standarder för WLAN. Anslutning i ett WLAN sker via en anslutningspunkt (access point, AP). Varje AP konfigureras med ett SSID (service set identifier), vilken sänds ut i klartext med jämna intervall. Klienter måste också vara konfigurerade med SSID för att kunna identifiera och välja AP i nätet. SSID är mycket enkel att identifiera med avlyssning i nätet och därefter konfigurera sin egen klient med. För att öka säkerheten kan nätverket konfigureras med listor över de specifika utrustningar som har tillstånd för uppkoppling. Listorna innehåller de MAC-adresser (medium access control) som respektive utrustning får av fabrikaten vid tillverkning. Krypteringstekniken som används kallas WEP (wired equivalent privacy), men är en option som går att stänga av. WEP har flera svagheter, exempelvis är funktionen avstängd när kortet installeras. Men framför allt återanvänds en del av kryptonyckeln alltför ofta. Nyckeln har också knäckts av kända forskare och anses osäker oberoende av nyckellängd. Exempelvis knäcks en 128-bitars nyckel normalt inom 15 minuter. Dessa svagheter innebär att ett antal typer av attacker är möjliga mot WLAN: koppla upp en egen klient, koppla in en egen AP, avlyssna datatrafiken, kapa och manipulera datatrafik mellan klienter. Självklart kan datatrafiken störas ut av en

[128] Krohné, mj Stig-Olof (2004), *CNI – en metod för terroristernas underrättelsetjänst?* (Stockholm: Försvarshögskolan, C-uppsats 19 100:2071), s. 30–36.
[129] Wireless LAN Association (2005), *What is a Wireless LAN?*, flera sidor på hemsidan [www]. Hämtat från http://www.wlana.org/learn/educate.htm 25 oktober 2005.

störsändare. Standarden IEEE 802.11i har bättre säkerhet, exempelvis har WEP bytts ut mot en ny standard.[130]

5.5 Radar

Syntetisk aperturradar (SAR)

SAR-tekniken ger oss möjligheten till bilder av jordytan från flygplan eller satelliter med upp till 10 cm upplösning. Genom att kombinera flera mätpunkter längs en rät linje bildas en stor antennapertur på syntetisk väg, därav namnet. SAR finns både med och utan förmåga att upptäcka rörliga mål (ground moving target indicator, GMTI). Med en lågfrekvent (omkring 20–90 MHz) SAR uppnås förmågan att ”se genom” vegetation och kamouflage.[131] Både militära och civila satelliter har SAR-förmåga ombord. SAR är en aktiv sensor vilket ger verkan både i dagsljus och i mörker.[132]

Stridsfältsradar

En stridsfältsradar används för att upptäcka rörliga markmål, bandfordon, hjulfordon, trupp och lågtflygande helikoptrar. De flesta system är av pulsdopplertyp med GMTI och en typisk räckvidd på 10 km.[133] Räckvidder på olika system är terrängberoende. Fordonsmonterad stridsfältradar ger bättre möjlighet till höga effekter och kan därför upptäcka människor och fordon i rörelse på ett avstånd upp till 60 km.[134] Helt öppen terräng och höjdöverläge krävs dock för att nå så stora räckvidder. Den ”praktiska” räckvidden är sannolikt lägre än så. För insatsförband i okänd terräng skulle stridsflätsradar vara lämplig för exempelvis intrångsskydd, inbrottslarm eller liknande. Det gäller då sådan radar inte lätt kan luras. Nackdelen är att stridsfältradarn aktivt sänder ut effekt och därmed kan upptäckas med signalspaning. Förbanden riskerar alltså att röjas vid användning. Dock kan inte undersökningen av hotbilden i kapitel 2 peka på att de icke-reguljära aktörerna har använt sig av signalspaning mot radarsystem (ELINT).

Optiska sensorer

Optiska sensorer erbjuder goda möjligheter att upptäcka, klassificera och identifiera mål. Det finns både passiva och aktiva sensortyper. TV-kameror, IR-system, bildförstärkare och robotvarnare i IR- eller UV-området är exempel på passiva typer. De aktiva typerna innehåller både en belysande strålkälla, vanligen

---

[130] Reinema, Dr Rolf (2004), ”Security Management – Part 2: Wireless Security”, föreläsningsunderlag, Computer Society Malta och Fraunhofer Institut Sichere Informations-Technologie *IT Security Management*, konferens 29–30 januari 2004, Sliema, Malta [www]. Hämtat från http://www.csm.org.mt/pdf/Fraunhofer/Mobile_Sec_Part2_v2.pdf 25 oktober 2005.

[131] FOI (2004), *FOI orienterar om: Sensorer*, 2004, nr 3 (Stockholm: Totalförsvarets forskningsinstitut), s. 66–67.

[132] FOI (2005), *FOI orienterar om: Rymden – nytta och teknik*, 2005, nr 4 (Stockholm: Totalförsvarets forskningsinstitut), s. 12–14 och 55.

[133] FOI, *FOI orienterar om: Sensorer*, s. 64.

[134] Parsons, Robert (2004), ”Intelligence Collection Capabilities for Peacekeeping”, Heide, Rachel Lea m.fl. (eds.) *Peacekeeping Intelligence: New Players, Extended Boundaries* (Ottawa: Carlton University), rapport från den andra konferensen ”Peacekeeping Intelligence”, Kanada 4 december 2003, s. 11 [www]. Hämtat från <http://www.carleton.ca/csds/pki/doc/PKI_conference_report _2003.pdf> 25 april 2005.

en laser, och en mottagare/detektor. Exempel är på aktiva optiska sensorer är laseravståndsmätare, avbildande laserradar och optikspanare.[135]

En lämplig typ av plattform för optiska sensorer är UAV:er. Global Hawk och Predator ger lång uthållighet, men är dyra och kräver välutbildad personal och preparerade landningsbanor. UAV:er med kortare uthållighet har räckvidder på omkring 50 km med flygtid på upp till 13 timmar. Mini-UAV:er flyger på 15–30 meters höjd och kan se upp till 10 km med videokamera. De kan även detektera kemiska och biologiska vapen.[136]

Satelliter är en annan lämplig typ av plattform för optiska sensorer. Civila satellitsystem erbjuder bilder från optiska sensorer till försäljning. Detta är ett förhållandevis billigt sätt att skaffa sig egen satellitspaningsförmåga. Nackdelen är att de är utom vår egen kontroll.[137] Ett annat sätt är förstås att få tillgång till annan nations militära kapacitet genom samarbete. Låghöjdssatelliter ger hög upplösning för upptäckt av exempelvis fordon, flygplan, byggnader och folksamlingar. Nackdelen är att de inte upptäcker snabba kortlivade förändringar. Kombinationen av geostationära och låghöjdssatelliter ger snabb överblicksbild med låg upplösning respektive bilder över ett litet område med hög upplösning efter lite väntan.[138]

DIRCM

MANPADS arbetar i princip uteslutande med IR-målsökare och utgör framför allt ett hot i samband med start och landning av flygplan samt mot helikoptrar på låg höjd. De motverkanssystem som finns och utvecklas kallas för DIRCM (directed infra red countermeasures). Dessa består av en robotskottvarnare tillsammans med någon form av motmedelsinsats, exempelvis riktad IR-bestrålning från blinkstörare eller laser. Robotskottvarnaren detekterar robotflamman och ger en grovinriktning. Varnaren är antingen UV-baserad vilken kan detektera roboten under den inledande delen av dess bana (boost-fasen), eller IR-baserad vilken kan detektera den förhöjda skaltemperatur som uppstår vid luftens friktion mot robotskalet. Traditionella facklor används fortfarande och är verksamma mot äldre generationers målsökare. Utvecklingen går dock mot målsökare som använder flera våglängder eller är bildalstrande, vilket innebär att facklor inte fungerar. Detta motiverar användning av laser mot MANPADS. Operativa system finns idag för helikoptrar och transportflygplan, för taktiskt flyg bedöms de vara operativa före 2010.[139]

5.6 Nya tekniska förmågor - slutsatser

System för signalspaning och störning av GSM, 3G, satellitkommunikation och kortvågsradio är fullt möjligt att implementera i våra insatsförband. Det finns exempel på både rörliga systemlösningar och mer stationära. Förmåga att signalspana mot dessa system erbjuder även en väg in i Internet. Stöd för att knäcka kryptering kan vara aktuellt. På kortvågsområdet finns möjligheten att

[135] FOI, *FOI orienterar om: Sensorer*, s. 66–67
[136] Parsons, ”Intelligence Collection Capabilities for Peacekeeping”, s. 11.
[137] Höstbeck, *Space and Defence*, s. 34–35 och 46.
[138] FOI, *FOI orienterar om: Rymden – nytta och teknik*, s. 12–14, 23 och 55.
[139] FOI, *FOI orienterar om: Telekrig*, s. 77.

dölja sig genom att använda snabbsändare. Därför är filterbankmottagare ett krav i signalspaningssystem för kortvåg.

Informationen på Internet är ständigt under förändring och flera metoder och tekniker måste därför kombineras. Eftersom Internet är ett globalt nätverk kan inhämtningen rent geografiskt utföras från i princip var som helst. Flera tekniker finns redan idag, men det är alltså inte nödvändigt att genomföra denna typ av inhämtning från en gruppering i konfliktområdet.

För WLAN är räckvidderna korta vilket av taktiska skäl kan göra det svårt att ha kontinuerlig inhämtning från en stationär gruppering. Detta ställer krav på en rörlig systemlösning. Sannolikt behövs även stöd från annan sensor för att inrikta signalspaningen, exempelvis fast grupperad inhämtning på Internet.

IEDD-system för att störa bomber med fjärrutlösning i preventivt syfte för att skydda objekt finns redan idag på marknaden. Detsamma gäller system för att detektera elektronik i bomber (NLJD).

DIRCM är den lämpligaste lösningen som plattformskydd mot MANPAD-hotet. DIRCM-system för långsamt gående flygfarkoster finns redan idag och är möjliga att implementera även i stridsflygplan före 2010.

Satellitspaning med olika optiska sensorer och SAR har överlägsna räckvidder. För de optiska sensorerna är en kombination av geostationära satelliter med låg upplösning och låghöjdssatelliter med hög upplösning är att föredra. Det finns både militära och även civila kommersiella system operativa idag.

Spaning med optiska sensorer och SAR från flygande plattformar kan utgöra ett bra komplement till satellitsystemen, och till del ersätta dom. Sådana system skulle med sin goda räckvidd avsevärt kunna förbättra lägesbilden och underrättelserna. De är även mycket lämpliga för att invisa andra sensorer. Flera system är operativa redan idag och särskilt intressant är att lågfrekventa SAR-system kan ”se genom” vegetation.

Stridsfältsradar är särskilt användbar i okänd terräng som indikator på misstänkt verksamhet och för övervakning av områden eller objekt. Den kan se erbjuda enheter på lägsta nivå en möjlighet att se bortom egen visuell räckvidd. Flera operativa system finns idag.

Sammanfattningsvis är följande nya tekniska förmågor möjliga att tillföra våra insatsförband före 2010: signalspanings- och störförmåga mot sambandssystem (GSM/3G/satellitkommunikation/kortvågssystem), rörlig signalspanings- och störförmåga mot WLAN, IEDD, DIRCM, spaning med flygburna sensorer (optiska sensorer och SAR), övervakning med stridsfältradar, CNO (mot ”fasta”[140] Internet) och satellitspaning (optiska sensorer och SAR).

[140] Benämningen ”fasta” Internet används i uppsatsen för att skilja det från WLAN.

Kapitel 6
ANALYS - TAKTISKA FÖRDELAR

taktiken [utgör] läran om stridskrafternas användning i strid och strategin läran om stridens utnyttjande för att nå krigets syfte. […] endast stora taktiska framgångar kan leda till stora strategiska vinster. […] taktiska framgångar är av dominerande betydelse i krigföringen .[141]

Carl von Clausewitz

6.1 Inledning

I det här kapitlet genomförs en teoretisk analys i syfte att identifiera vilka taktiska fördelar nya tillförda tekniska förmågor ger våra insatsförband som ska sättas in i moderna lågintensitetskonflikter. Kapitlet avslutas med en syntes där samtliga variabler sammanförs i en datamatris. Utifrån denna syntes dras slutsatser.

6.2 Analysmodell

Vilka förmågor krävs för att vinna en lågintensitetskonflikt? Vilka är framgångsfaktorerna? I den klassiska militärteorin betonas vikten av vissa grundelement för att gå segrande ur ett enskilt slag, fälttåg eller hela krig. Problemet är att lågintensitetskonflikterna följer ett annorlunda mönster. Ofta är det konventionellt utbildade soldater och officerare som tvingas möta okonventionella situationer, alltså kan andra faktorer vara avgörande. Bekämpningsförmågan kan relativt sett vara mindre betydelsefull i jämförelse med det konventionella *mellanstatliga* kriget.[142]

Några olika angreppssätt har valts vid tidigare analyser av lågintensitetskonflikter. En sorts fri diskussion kring fallstudier utan något egentligt analysverktyg förekommer. Andra analyser av de förmågor en insatsstyrka behöver för att lyckas i en lågintensitetskonflikt har utgått ifrån de tidigare fem grundelementen: bekämpning, ledning, underrättelser, rörlighet och uthållighet.[143] Kersti Håkansson, forskningsassistent vid Försvarshögskolan, fokuserar på interaktionen mellan ledning, teknik och bekämpning när hon analyserar taktik och stridsteknik i insatsen i Afghanistan 2003.

I denna uppsats har jag valt följande angreppssätt. Skillnader mellan insatsförbandens förmåga idag och den förmåga som tillförda tekniker kan ge i en nära framtid ska identifieras. Enkelt uttryck ska behoven ställas mot den verkliga förmågan. Syftet är att mäta vilka *taktiska fördelar* tillförsel av nya tekniska förmågor ger våra insatsförband.

---

[141] Clausewitz, *Om kriget*, s. 88 och 202.
[142] Ångström, ”Lågintensiva konflikter som forskningsområde: En introduktion”, s. 11.
[143] Ibid, s. 19.

För att kunna identifiera en taktisk fördel har jag definierat det som ett centralt begrepp, se nedan. Begreppet tilldelas också ett antal operationella indikatorer i syfte att göra det mätbart i en teoretisk analys.

Med begreppet *taktisk fördel* menas i denna uppsats gynnsam inverkan på de svenska insatsförbandens taktiska verksamhet vid deltagande i internationella insatser. Inverkan kan även vara indirekt av operativ eller strategisk karaktär. Den gynnsamma inverkan kan vara av tre huvudtyper. Dessa utgör samtidigt de operationella indikatorerna på begreppet.

1. Ökning av en eller flera av de sex grundläggande förmågorna.
2. Ökning av egna alternativa taktiska handlingsmöjligheter och därmed ökad flexibilitet och robusthet. Detta kan omvänt tolkas som motverkad degradering av taktisk förmåga.
3. Möjlighet till nya kombinationer av olika sensor- och/eller verkanssystem som sätter en motståndare i en mycket svår valsituation, ett dilemma, även kallat kombinerade vapen (combined arms).

Analysenheter representerar normalt olika fall som ska undersökas. I denna uppsats utgörs de av de olika tekniska förmågorna som är möjliga att tillföra våra insatsförband enligt kapitel 5 (behovet): signalspanings- och störförmåga mot sambandssystem (GSM, 3G, satellitkommunikation och kortvågssystem), rörlig signalspanings- och störförmåga mot WLAN, IEDD, DIRCM, spaning med flygburna sensorer (optiska sensorer och SAR), övervakning med stridsfältradar, CNO (mot ”fasta” Internet) och satellitspaning (optiska sensorer och SAR).

För att avgöra om de nya tekniska förmågorna ger någon *taktisk fördel* måste relevanta egenskaper hos dessa analysenheter observeras och värderas. Egenskaperna görs mätbara genom att definiera relevanta *variabler*. Variablerna ska beskriva hur egenskaper hos analysenheterna varierar mellan analysenheterna. De tas fram ur de operationella indikatorerna vilka i denna uppsats utgörs av de av tre huvudtyperna för gynnsam inverkan på taktisk verksamhet. Variablernas mätbarhet uppnås i två steg. I ett första steg utvecklas och preciseras variablerna genom att definiera värderingskriterier som mer detaljerat beskriver deras innebörd. Värderingskriterierna hjälper också till att skilja ut relevanta fakta i undersökningen. I ett andra steg används värderingskriterierna som grund för att transformera de empiriska observationerna till ett mätbart värde. Fyra olika variabelvärden definieras vilka representerar olika grader på hur väl respektive variabels värderingskriterier uppfylls. Graden av uppfyllnad kan alltså variera från ingen till hel i fyra nivåer. En variabels värderingskriterier kan vara uppfyllt till del eller vara av indirekt karaktär, se avsnitt 6.4 nedan.

6.3 Variabler och värderingskriterier

I tabell 2 nedan listas definierade variabler med tillhörande värderingskriterier.

Tabell 2 Variabler preciserade med värderingskriterier.

Variabel	Värderingskriterier
Ledning	Variabeln bestäms av effektiviteten i beslutscykeln (tid och kvalitet).
Underrättelser/ information	Variabeln bestäms av 1. räckvidds- och yttäckningsförmåga 2. förmåga att upptäcka objekt 3. förmåga att klassificera och identifiera objekt 4. förmåga att lägesbestämma objekt 5. effektiviteten i underrättelsecykeln (tid och kvalitet).
Verkan	Variabeln bestäms av 1. graden av samverkande effekt med andra vapen (force multiplier) 2. förmåga till graderad verkan 3. förmåga att utvärdera vapenverkan.
Rörlighet	Variabeln bestäms av möjligheten att utan motståndarens påverkan förflytta sig (freedom of movement) till, från och i konfliktområden.
Skydd	Variabeln bestäms av förmåga till skydd mot motståndarens verkanssystem.
Uthållighet	Variabeln bestäms av 1. tidsutsträckningen i förmågan att upprätthålla verksamhet. 2. stridsvärdet som en effekt av motståndarens grad av påverkan.
Taktiska handlings-möjligheter	Variabeln bestäms av flexibilitet i kombination av sensor- och/eller verkanssystem vilket leder till nya alternativ för taktiskt uppträdande. Det kan också omvänt tolkas som motverkad degradering av egen taktisk förmåga.
Kombinerade vapen	Variabeln bestäms av möjligheten att kombinera med annat sensor- och/eller verkanssystem så att motståndarens motåtgärder mot ett av systemen gynnar verkan av det andra (som ett dilemma).

6.4 Analys med slutsatser

Signalspanings- och störförmåga mot sambandssystem

GSM, 3G och/eller satellitkommunikation förefaller ofta vara huvudsambands-medel för icke-reguljära enheter i lågintensitetskonflikter. Tillsammans med kortvågsradio har motståndaren flera alternativa sambandsmedel för taktisk och operativ ledning och samordning. Signalspaningsförmåga mot dessa system ger tydligast taktiska fördelar inom den grundläggande förmågan *underrättelser/ information*. Underrättelser är nödvändigt för att varna för olika hot kan därför förebygga våld och överraskande attacker. De kan användas för att dementera rykten, bygga upp självförtroende och möjliggöra att uppnå humanitära mål. Underrättelser är dessutom nödvändigt för att med tillräckligt stor styrka kunna projicera en militär styrkedemonstration. Det är alldeles uppenbart att denna

förmåga ökas om fler frekvensområden och kommunikationssystem täcks. Nya parametrar kan mätas och därmed kan fler objekt upptäckas, lägesbestämmas, klassificeras och identifieras. Med mer information och fler parametrar att väga in ökar sannolikt förmågan att skilja motståndare från oskyldiga civila. Den ökande mängden information och underrättelser leder dock inte automatiskt till en bättre lägesbild. Personalens kompetenser och metoder måste anpassas till de nya parametrarna och den ökade mängden information. Dock är det otvetydigt så att fler pusselbitar till en god lägesbild och kunskap om motståndaren erhålls. Alltså finns de tekniska förutsättningarna för högre kvalitet. Ur teknisk synvinkel blir alltså underrättelsecykeln effektivare.

Motsvarande störsystem ökar förmågan till *verkan* på samma sätt, fler frekvensområden och kommunikationssystem täcks. I en taktisk situation kan motståndarens ledningsförmåga tas bort. Störsystem ger synergi i samverkan med andra verkanssystem och förstärker därmed den totala verkan på motståndaren (force multiplier). I en större kontext erbjuder de en graderad verkan som ett alternativ till andra verkanssystem, främst de med dödlig verkan. Störsysystem i sig erbjuder också rent tekniskt graderad verkan. Verkan går att styra både geografiskt och i frekvensplanet.

Störning av exempelvis motståndarens taktiska ledningsförmåga försämrar hans möjligheter att verka mot våra enheter. Därmed skulle förmågan till *skydd* av våra egna enheter alltså öka.

När motståndarens förmåga till att verka har neutraliserats är hans möjligheter att påverka våra insatsförband mindre. Våra förbands möjligheter att förflytta sig är då större och deras stridsvärde riskerar inte i lika hög grad nedsättas av motståndarens verkanssystem. Detta innebär alltså att våra förmågor till *rörlighet* och *uthållighet* har ökat.

Störförmågan erbjuder minst ytterligare ett *taktiskt alternativ*. Störning i syfte att förlama motståndarens ledningsförmåga minskar avsevärt hans möjligheter att påverka våra insatsförband. Han får svårt att leda och koordinera sin verkan. Detta innebär exempelvis att vi kan välja en offensivare taktisk lösning, sannolikt i ett högre tempo. Det är även möjligt att bättre underrättelser via signalspaning kan leda till nya lösningar på taktiska problem, exempelvis om en svaghet eller en kritik sårbarhet endast kan detekteras av den nya tekniska förmågan.

Störförmågan ökar även förmågan till *kombinerade vapen*. Om exempelvis en motståndare är grupperad så att verkan med granater inte är möjlig med hänsyn tagen till ROE samtidigt som hans förmåga att kommunicera störs ut, ställs han inför ett dilemma: Stå kvar i skydd med allt sämre lägesbild eller förflytta sig för att kunna kommunicera och därmed blotta sig för bekämpning.

Både störsystem och signalspaningssystem påverkar effektiviteten i beslutscykeln (OODA). Störsystemens sätt att erbjuda fler taktiska möjligheter och att öka vår verkansförmåga gör ”decision” och ”action” effektivare. Signalspaningssystems sätt att öka förmågan till underrättelser/information gör ”observation” och ”orientation” effektivare. Flera typer av sensorer som kompletterar varandra och ger invisning ger oss fler möjligheter att hitta motståndaren, sannolikt då också snabbare. Som nyss konstaterats utgör fler pusselbitar till en god lägesbild och kunskap om motståndaren nödvändiga tekniska förutsättningar för högre kvalitet. De tekniska förutsättningarna finns

alltså då för att processerna i beslutscykeln både går snabbare och får högre kvalitet. Därför ökas även förmågan till *ledning*.

Rörlig signalspanings- och störförmåga mot WLAN

Som komplement till GSM, 3G, satellitkommunikation och kortvågsradio utgör WLAN ytterligare ett alternativt medel för en icke-reguljär motståndare att taktiskt och operativt leda och samordna sina enheter. WLAN ger honom exempelvis förmåga att snabbt omgruppera sina lednings- och sambands-funktioner. Precis som för signalspaningssystem mot sambandssystem ger signalspaning mot WLAN tydligast taktiska fördelar inom den grundläggande förmågan *underrättelser/information*. Räckvidderna är dock avsevärt kortare varför sådana system bedöms vara beroende av invisning och stöttning från andra sensorer. Exempelvis kan HUMINT ge invisning av geografiskt läge, och CNO (fast grupperad) ge invisning med exempelvis tekniska parametrar för att snabbare identifiera och lägesbestämma ett mål. I en sådan situation kan ett signalspanings-system mot WLAN vara den sensor som i direkt samverkan med aktuellt verkanssystem slutligen verifierar målet och därmed skiljer motståndare från oskyldiga civila vid en omedelbart förestående insats. Eftersom systemet då förbättrat kvaliteten i beslutscykeln (OODA), främst ”orientation” och ”decision”, har det ökat förmågan till *ledning*.

Störning av WLAN erbjuder ytterligare ett verkanssystem till insatsförbanden, fler kommunikationssystem täcks. Störning av WLAN kan användas i syfte att hindra en motståndare att rapportera om en mot honom påbörjad insats. Alltså kan hans strategiska och operativa ledningsförmåga på lite längre sikt tas bort. Det är onekligen en ökning av förmågan till *verkan*, men det är svårt att bedöma betydelsen av detta. Men möjligheten finns att en rapportering om vår insats exempelvis avslöjar våra metoder eller verkanssystem så att nya motmedel kan vidtas. Om vi motverkar detta kan det betraktas som att *skyddet* av vår egen verksamhet som ökar. Dock sätts ett frågetecken till hur pass avgörande denna inverkan skulle vara på våra insatsförband.

IEDD

Störning i förebyggande syfte för att hindra att en hemmagjord bomb fjärrutlöses med radiosignaler är ingen garanti för att hindra skador på egen trupp och oskyldiga civila. Däremot är det tveklöst så att det skulle öka förmågan till *skydd* jämfört med insatsförbandens **obefintliga** förmåga idag. Även om det inte är ett effektivt motmedel mot alla slags bomber så har det verkan mot dom som exempelvis utlöses via mobiltelefoner.

Denna störförmåga skulle därmed erbjuda ammunitionsröjningsförband ett nytt taktiskt uppträdande, en ny *taktisk möjlighet* om än bara för detta förband.

Förmåga att detektera elektronisk utrustning i en misstänk bomb (NLJD) ger ammunitionsröjningsförband en möjlighet att värdera om bomben har elektronisk fjärrutlösare. De får ytterligare en pusselbit för att värdera en misstänkt bomb. Alltså har deras förmåga till *underrättelser/information* ökat.

DIRCM

DIRCM skulle avsevärt öka förmågan till *skydd* av egna flygande plattformar mot MANPAD.

När motståndarens förmåga till att verka har neutraliserats är hans möjligheter att påverka våra flygande plattformar mindre. Våra flygande enheters möjligheter att förflytta sig är då större och deras stridsvärde riskerar inte i lika hög grad nedsättas av motståndarens verkanssystem. Detta innebär alltså att våra förmågor till *rörlighet* och *uthållighet* har ökat.

Ökad rörlighet och ökat skydd medger som tidigare konstaterats ovan ett offensivare uppträdande. Alltså kan ytterligare *taktiska alternativ* sannolikt erbjudas.

Detta offensivare uppträdande, exempelvis över motståndarens gruppering, leder också till större möjligheter att nå hans enheter med våra flygande verkanssystem. Alltså har förmågan till *verkan* också ökat. På samma sätt ökar förmågan till *underrättelser/information*.

Spaning med flygburna sensorer

Precis som för signalspaningsförmåga mot sambandssystem och WLAN ger flygburna optiska sensorer och SAR tydligast taktiska fördelar inom den grundläggande förmågan *underrättelser/information*. Återigen handlar det om nya pusselbitar och att flera sensorer kan komplettera och invisa varandra. Genom att kombinera signalspaningsförmåga mot sambandssystem och WLAN med flygburna optiska sensorer och SAR nås verkan på olika våglängdsområden. Denna kombination ökar tillförlitligheten i underrättelserna. Förmågan att skilja motståndare från oskyldiga civila ökar. Det enskilt kanske viktigaste mervärdet som flygburna optiska sensorer och SAR ger består dock i ökade räckvidder och bättre yttäckning.

Av ovan kan man dra slutsatsen att kvaliteten i beslutscykeln (OODA) även den påverkas i positiv riktning. Fler våglängdsområden täcks och nya parametrar kan mätas. Därmed kan fler objekt upptäckas, lägesbestämmas, klassificeras och identifieras. Som tidigare konstaterats ger detta fler pusselbitar till en god lägesbild och kunskap om motståndaren och därmed har faserna ”observation” och ”orientation” i beslutscykeln blivit effektivare. De tekniska förutsättningarna för att processerna i beslutscykeln får högre kvalitet finns och därmed ökar förmågan till *ledning*.

Dessa sensorer är även mycket lämpliga för att utvärdera vapenverkan. Därmed ökar de faktiskt förmågan till *verkan* även om det sker med viss fördröjning.

Man kan tänka sig att dessa sensorer med sin räckvidd, förmåga till överblick och därmed ökade kvalitet i våra taktiska och operativa beslut försämrar motståndarens möjligheter att verka mot våra enheter. Därmed skulle förmågorna till *skydd* av egna enheter samt egen *rörlighet* och *uthållighet* i någon mån öka, även om denna påverkan inte är lika tydlig och direkt som hos ett aktivt verkanssystem.

Övervakning med stridsfältradar

Stridsfältsradarsystem erbjuder taktiska enheter på låg nivå bättre lägesbild, särskilt i okänd terräng. De kan se bortom sin egna visuella räckvidd med de

begränsningar som terrängen ger. De får tillgång till mer information och därmed ökar deras förmåga avseende *underrättelser/information*.

Precis som övriga andra sensorer ovan ökar stridsfältsradarn kvaliteten i beslutscykeln (OODA), främst ”observation” och ”orientation”, och därmed förmågan till *ledning*.

Med god kunskap om motståndarens gruppering och rörelser kan beslut tas som ger taktisk förflyttning med minimerad påverkansmöjlighet från hans verkanssystem. Därmed ökar vår *rörlighet*.

Väl underbyggda taktiska beslut leder indirekt till ökat *skydd* av egna enheter vilket i sin tur, som tidigare konstaterats, leder till ökad *uthållighet*. Det bör nämnas att en förändring av hotbilden så att den i framtiden omfattar signalspaningssystem mot våra radarsignaler däremot får motsatt effekt på vår förmåga till skydd, och därmed också på förmågan till uthållighet.

CNO (mot ”fasta” Internet)

De taktiska fördelarna med förmåga att spana på Internet (CNO) är på samma sätt som för övriga sensorer ovan tydligast avseende den grundläggande förmågan *underrättelser/information*. Nya parametrar erbjuds, fler objekt upptäcks och identifieras, fler pusselbitar erhålls till en god lägesbild och kunskap om motståndaren.

Som tidigare konstaterats flera gånger leder en förbättrad lägesbild och kunskap om motståndaren till att faserna ”observation” och ”orientation” i beslutscykeln blir effektivare. De tekniska förutsättningarna för att processerna i beslutscykeln får högre kvalitet finns och därmed ökar förmågan till *ledning*.

En ökad ledningsförmåga leder sannolikt till kvalitativt bättre taktiska beslut. Detta leder som tidigare konstaterats indirekt till ökat *skydd* av egna enheter, exempelvis kan hot mot våra insatsförband upptäckas i så god tid att motåtgärder kan vidtas. Detta leder i sin tur till att våra förbands stridsvärde inte riskerar nedsättas av motståndarens verkanssystem i lika hög grad, vilket ger en indirekt ökad förmåga till *uthållighet*.

Satellitspaning (optiska sensorer och SAR)

Satellitspaning är oftast en strategisk resurs och sannolikt inte aktuell som en enhet ingående i ett svenskt insatsförband. De får istället tillgång till sådan information via annan nation eller köper den från en civil aktör. Återigen är de taktiska fördelarna som sensor tydligast avseende den grundläggande förmågan *underrättelser/information*. I likhet med SAR och flygburna optiska sensorer består det viktigaste mervärdet i överlägsen räckvidd.

Övriga taktiska fördelar liknar även de som redovisades för SAR och flygburna optiska sensorer. Alltså fås en ökad kvalitet i beslutscykeln (OODA) och ökad förmåga till *ledning*. Även här kan man tänka sig att den överlägsna räckvidden, förmågan till överblick och därmed ökade kvalitet i våra taktiska och operativa beslut försämrar motståndarens möjligheter att verka mot våra enheter. Därmed skulle förmågorna till *skydd* av egna enheter samt vår *rörlighet* och *uthållighet* i någon mån öka.

Satellitspaning är även lämplig för att utvärdera vapenverkan. Därmed ökar även förmågan till *verkan*.

Syntes

De empiriska observationerna och slutsatserna i denna uppsats är en undersökning av en komplex verklighet. För att göra denna komplexa verklighet mätbar sammanfattas och förenklas den i en datamatris enligt tabell 3 nedan. De empiriska observationerna och slutsatserna i uppsatsen ovan transformeras därför till ett värde på respektive variabel. Variabelvärdena som tilldelas baseras på de definierade värderingskriterierna i tabell 2 och presenteras i datamatrisen med följande kodning.

0 = Inget värderingskriterium uppfyllt.
? = Osäkert om värderingskriterium uppfylls.
\+ = Värderingskriterium uppfyllt till del och/eller bedömt uppfyllt på indirekt väg.
++ = Värderingskriterium uppfyllt och bedömt vara av stor betydelse.

Tabell 3 Sammanfattande datamatris.

Nya förmågor \ Variabler	Ledning	Und/Info	Verkan	Rörlighet	Skydd	Uthållighet	Taktiska handlings-möjligh.	Komb. vapen
Signal-spanings- och störförmåga mot sambands-system	++	++	++	+	+	+	++	++
Rörlig signal-spanings- och störförmåga mot WLAN	++	++	+	0	?	0	0	0
IEDD	0	+	0	0	++	0	+	0
DIRCM	0	+	+	+	++	+	+	0
Spaning med flygburna sensorer	++	++	+	+	+	+	0	0
Övervakning med stridsfälts-radar	+	++	0	+	+	+	0	0
CNO (mot ”fasta” Internet)	++	++	0	0	+	+	0	0
Satellit-spaning (optiska sensorer och SAR)	++	++	+	+	+	+	0	0

Slutsatser

Av tabell 3 ovan kan följande slutsatser dras.

Signalspanings- och störförmåga mot olika sambandssystem är den enda tekniska förmågan som påverkar samtliga variabler i positiv riktning. Den är även den tekniska förmåga som på flest variabler ger inverkan av stor betydelse. Störförmågan som ett verkanssystem är dessutom den enda tekniska förmågan i analysen som ger: möjlighet till graderad verkan, synergi i samverkan med andra verkanssystem (force multiplier) och ökade möjligheter till kombinerade vapen. Det är tveklöst så att **signalspanings- och störförmåga mot olika sambands-system** är den tekniska förmåga som **ger störst taktisk fördel** för våra insats-förband när de möter icke-reguljära hot i en modern lågintensitetskonflikt.

De två tekniska förmågor som har störst direkt och omedelbar betydelse för skydd av egen trupp är **IEDD och DIRCM**.

Underrättelser/information är den enskilda variabel som påverkas av flest tekniska förmågor. Dessutom omfattas den av flest taktiska fördelar av stor betydelse i analysen.

Den enskilda variabel som därnäst påverkas av flest tekniska förmågor är **ledning**. Den ökade ledningsförmågan ger betydande taktiska fördelar för våra insatsförband enligt analysen ovan. Mycket av detta hänger ihop med att många av de nya tekniska förmågorna i analysen är sensorer vilka direkt påverkar beslutscykelns alla faser, men kanske främst ”observation” och ”orientation”.

Kapitel 7
DISKUSSION – RESULTATET OCH METODEN

Den kritiska granskningen, dvs ett närmare studium av medlen, leder till frågan, vilka särskilda resultat som vunnits och om dessa resultat varit den handlandes avsikt .[144]

Carl von Clausewitz

7.1 Inledning

I detta kapitel återkopplas till uppsatsens syfte och centrala frågeställning. Först redovisas svaren på den centrala frågeställningen och tillhörande delfrågeställningar. De sistnämnda har varit viktiga för att bygga upp nödvändiga fakta och leda oss fram till svaret på den förstnämnda. Därefter diskuteras uppsatsens resultat med förslag till anskaffning inklusive motiv. Ställning tas till om syftet är uppnått. Nästa avsnitt diskuterar uppsatsens metod genom att peka på och kommentera begränsningar och hinder. Kapitlet avslutas med att redovisa förslag på fortsatt forskning.

7.2 Den centrala frågeställningen

Den centrala frågeställningen var:

1. Vilka taktiska fördelar kan identifieras om nya tekniska förmågor för elektronisk krigföring tillförs våra insatsförband i moderna lågintensitetskonflikter?

Samtliga sex grundläggande förmågor kan ökas genom att tillföra olika tekniska förmågor. De taktiska fördelarna kan vara av stor betydelse eller av indirekt positiv karaktär. Nya taktiska handlingsmöjligheter kan i vissa fall erbjudas och möjligheten till kombinerade vapen kan ökas om störförmåga mot sambandssystem tillförs. De största taktiska fördelarna går att finna inom den grundläggande förmågan *underrättelser/information*. Den tekniska förmåga som ger både flest och störst taktiska fördelar är signalspanings- och störförmåga mot sambandssystem. Sammanfattningsvis kan samtliga tre huvudtyper av gynnsam inverkan på de svenska insatsförbandens taktiska verksamhet uppfyllas, se definitionen av *taktisk fördel* ovan. Svaret på frågan framgår i detalj av tabell 2 och 3 ovan samt analysen med slutsatser som redovisas i avsnitt 6.4. Den enskilt viktigaste slutsatsen som kan dras är: **Tillförsel av nya tekniska förmågor ska ses som en helhet** där flera tekniska sensorer kombineras med andra underrättelseförmågor, se avsnitt 7.3 nedan. Allt annat vore att suboptimera enskilda sensor- och/eller verkanssystem.

Delfrågeställningarna som bidragit till att svara på den centrala frågeställningen har besvarats i olika kapitel ovan. Här nedan redovisas en sammanfattning av svaren:

[144] Clausewitz, *Om kriget*, s. 120.

2. Vilka medel och metoder som nyttjar det elektromagnetiska spektret eller datornätverk har använts operativt av icke-reguljära aktörer i lågintensitetskonflikter under perioden 1991–2004? Med operativt menas de medel som varit nödvändiga för att kunna planera och genomföra väpnade insatser. Med medel menas materielsystem och tekniska utrustningar.

Av kapitel 2 och slutsatserna i kapitel 4 framgår att icke-reguljära aktörer i lågintensitetskonflikter i hög grad har använt sig av moderna kommunikationsmedel, främst mobiltelefoni, satellittelefoni och Internet. Hoten mot människoliv har utgjorts av fjärrutlösta bomber (IED) och burna luftvärnssystem så kallade MANPAD. Det bör även kommenteras att de icke-reguljära aktörerna söker sig till miljöer där våra insatsförband har svårt, både att skilja motståndare från oskyldiga civila och att verka med konventionella vapen.

3. Vilka förmågor för elektronisk krigföring har Försvarsmaktens förband i internationella insatser idag och vilka brister kan, jämfört med lågintensitetshoten, identifieras?

Dagens insatsförband har vissa förmågor för elektronisk krigföring exempelvis signalspaning mot analog radiotrafik, radarvarnare i kombination med remsor och facklor, olika luftvärnsradarsystem och sonarer. Dessa förmågor är dock i mycket stor grad dimensionerade utifrån en gammal hotbild, en konventionell stormakt. Därför är bristerna stora mot den hotbild som icke-reguljära aktörer utgör i lågintensitetskonflikter. Bristerna består i mycket stor utsträckning av avsaknad på olika sensorer, men även verkanssystem i form av störutrustningar. Bristerna redovisas mer detaljerat i kapitel 3 och 4.

4. Vilka tekniska förmågor för elektronisk krigföring mot kartlagda lågintensitetshot och som är operativt realiserbara senast 2010 kan identifieras och därmed komplettera identifierade brister? Med operativt realiserbara senast 2010 menas vilken teknisk utrustning som utan vidare forskning kan upphandlas och integreras i operativa militära tekniska system inom en femårsperiod.

I kapitel 5 framgår att följande nya tekniska förmågor för elektronisk krigföring kan göras operativa för att komplettera bristerna:

- Signalspanings- och störförmåga mot GSM, 3G, satellitkommunikation och kortvågssystem,
- rörlig signalspanings- och störförmåga mot WLAN,
- förmåga att upptäcka elektronik i misstänkta bomber samt störa fjärrutlösning av desamma (IEDD),
- förmåga att skydda flygande plattformar mot IR-målsökande robotar (DIRCM),
- förmåga att spana med flygburna optiska sensorer och SAR,
- övervakningsförmåga med stridsfältradar,
- CNO-förmåga (från fast gruppering i Sverige),
- satellitspaning med optiska sensorer och SAR (ägda av annan aktör).

7.3 Slutsatser och värdering av resultatet

Det är utomordentligt viktigt att tillföra signalspanings- och störförmåga mot olika sambandssystem till våra insatsförband för att bristerna i de befintliga system ska byggas bort. Vi vinner många taktiska fördelar på detta. Förmåga att signalspana mot dessa system erbjuder dessutom en väg in i Internet. Stöd för att knäcka kryptering kan vara aktuellt och borde därför vara tillgängligt för insatsförbanden från hemmaplan. Huruvida våra insatsförband skulle vinna på att ha kapacitet mot kortvåg kan man ju diskutera. Det beror väl på om man misstänker att motståndaren kommunicerar med hjälp av snabbsändare på kortvåg. Verkan av detta ska i sin förlängning vägas mot kostnader. Dock kan man inte utesluta att kortvåg används, varför sådan förmåga ur ett strikt tekniskt och militärt perspektiv bör tillföras.

Det finns flera exempel på att de icke-reguljära aktörerna använder Internet på olika sätt. Informationen är ständigt under förändring och flera metoder och tekniker måste kombineras. Det finns risk för att det blir ganska personalkrävande, inte minst för att informationsmängden som ska analyseras sannolikt blir mycket hög. Eftersom Internet är ett globalt nätverk kan inhämtningen rent geografiskt utföras från i princip var som helst. CNO-förmåga är angelägen att ha och den bör utgå från Sverige som ett direktriktat stöd till insatsförbanden. Fördelarna med detta är många. Personalen får sannolikt en mycket hög grad av expertis både vad gäller tekniskt kunnande, metodik och främmande språk. Erfarenheter från utlandsstyrkan visar att denna typ av kompetens är mycket svårrekryterad i allmänhet, men särskilt svår då de ska tjänstgöra i ett konfliktområde. Personalen bör därför heltidsanställas för uppgiften hemma i Sverige. Det kommer dessutom att ge en hög grad av kontinuitet och kvalitet, samt att problem med personalomsättning var sjätte månad kan undvikas. Påverkan på beslutscykeln bedöms bli lite trögare då personalen sannolikt har normala arbetstidsregler att följa hemma i Sverige. Detta kan dock vid behov motverkas med skiftarbete. Kvalitetsmässigt blir dock påverkan på beslutscykeln (”observation” och ”orientation”) bättre än från sensorer i konfliktområdet beroende på den högre graden av expertis, kontinuitet och kvalitet.

Däremot är det lämpligt att insatsförbanden tillförs system som kan verka mot WLAN i ett konfliktområde, främst för signalspaning men även störning kan vara aktuellt. Här är räckvidderna korta vilket föranleder analys av plattformsval och taktiskt uppträdande. Det kan exempelvis visa sig vara svårt att ha kontinuerlig inhämtning från en stationär gruppering. Sannolikt är det nödvändigt att CNO-förmåga på hemmaplan kan stödja och invisa ett mindre personalstarkt men rörligt signalspaningssystem mot WLAN i ett konfliktområde.

För ammunitionsröjningsförband eller motsvarande enheter är det angeläget att anskaffa störutrustning mot fjärrutlösning av bomber. Genom att störa i preventivt syfte kan många liv sparas. System för att detektera elektronik i bomber (NLJD) kan vara ett bra komplement till de olika teknikerna för röjning som idag finns. Det är en självklarhet att göra vad man kan för att skydda egen trupp. Det är sannolikt anledning nog för att tillföra DIRCM och IEDD (störförmåga och detektion av elektronik i bomber). Men det faktum att våra västliga demokratier är känsliga för förluster av egen trupp, vilket innebär att de lätt lamslås, accentuerar detta ytterligare. Lamslagen politisk ledning ger direkt negativ inverkan på våra

insatsförbands möjligheter att lösa sina uppdrag. Sammantaget finns det därför mycket starka skäl till att tillföra dessa tekniska förmågor till våra insatsförband.

Satellitspaning med olika optiska sensorer och SAR har överlägsna räckvidder, men bara större nationer klarar av att finansiera egen sådan förmåga. Särskilt som en kombination av geostationära satelliter med låg upplösning och låghöjdssatelliter med hög upplösning är att föredra. Dock finns även civila kommersiella system att tillgå. Om det skulle inträffa att Sverige skulle köpa in sig i sådan teknik så kommer den inte att tillföras insatsförbanden utan vara en nationell resurs som stödjer dessa i ett konfliktområde. Slutsatsen blir att insatsförbanden ska stödjas med satellitspaning från annan nation eller via inköpta satellitbilder från civila aktörer.

Optiska sensorer för spaning från flygande plattformar bör istället tillföras insatsförbanden. Försvarsmakten har redan idag ett utmärkt UAV-system och JAS 39. UAV-systemet behöver bara göras operativt i en internationell miljö. Till JAS 39 krävs att en spaningskapsel med optiska sensorer anskaffas. JAS 39 har bättre räckvidder än vårt UAV-system men kan å andra sidan tidvis ges andra prioriteringar i ett konfliktområde. Därför utgör de bra komplement till varandra.

En mycket angelägen anskaffning är ett SAR-system. Ett sådant system skulle med sin goda räckvidd avsevärt kunna förbättra lägesbilden och underrättelserna. Särskilt önskvärt är att insatsförbanden får tillgång till förmågan att med SAR-system ”se genom” vegetation. Betydelsen av SAR ökar om tillgång till satellitspaning saknas. Satellitspaning kan vi inte själv styra över, men ett SAR-system kan vi själva ha kontroll över. SAR är också mycket lämpligt för att invisa andra sensorer.

Stridsfältsradar är särskilt användbar i okänd terräng som indikator på misstänkt verksamhet och för övervakning av områden eller objekt. Den kan utgöra en viktig sensor för mindre taktiska enheter ute på fältet för att se bortom egen visuell räckvidd.

Det är inom den grundläggande förmågan underrättelser/information vi har **mest att vinna** på att tillföra nya tekniska förmågor avseende elektronisk krigföring till våra insatsförband. Många källor pekar på vikten av en bra underrättelsetjänst i lågintensitetskonflikter. Ledstjärnan i allt detta är enligt tidigare att kombinera flera olika typer av underrättelseförmågor såsom SIGINT, IMINT, HUMINT, OSINT inklusive direktriktat stöd från olika underrättelseorganisationer hemma i Sverige. Vi har också tidigare konstaterat vikten av kombinationen av ökat internationellt samarbete och en **mycket god egen underrättelseförmåga**, inte minst baserat på Hollands dyrköpta erfarenheter från Srebrenica 1995. Slutsatsen från tidigare i uppsatsen om att det finns ett stort behov av en ökad inhämtnings- och analysförmåga både före och under en svensk insats förstärkas alltså av resultatet. Den elektroniska krigföringen med sina olika tekniska sensorer är tveklöst en mycket viktig delkomponent i detta sammanhang. Det finns därför alla anledning att se på tillförseln av nya tekniska förmågor till våra insatsförband som **en helhet** hellre än som enskilda autonoma system. Det är bredden, de många alternativa sensorerna och synergin dom emellan som ger det stora mervärdet, **de avgörande taktiska fördelarna**.

Uppbyggnad av en mycket god egen underrättelseförmåga ger dessutom automatiskt goda synergieffekter på ledningsförmågan eftersom den direkt påverkar alla faserna i beslutscykeln, men kanske främst ”observation” och ”orientation”. Detta stärker bara motiven för att satsa på att kombinera flera olika

typer av underrättelseförmågor där den elektroniska krigföringen med sina olika tekniska sensorer utgör en mycket viktig delkomponent.

Det är mycket viktigt att se ovan redovisade slutsatser i den kontext som de dragits. Uppsatsen har stort fokus på det teknologiska perspektivet. Men det kan inte nog påpekas att tekniken inte ensamt är svaret på alla problem, vilket exemplifierats ett flertal gånger genom uppsatsens alla kapitel. Därtill är verkligheten alldeles för komplex. Insatsförbanden måste betraktas som hela system med både människor och teknik. Saker som systemintegration, färdigheter, doktriner, motivation och vilja spelar stor roll för förbandens förmåga och effekt. Detta innebär bland annat att uppsatsen inte analyserat konsekvenserna av ett förändrat personalbehov, exempelvis för att analysera den större mängden inhämtad information. I uppsatsen har bara en typ av hotbild utgjort empiriskt underlag. Endast icke-reguljära aktörer som verkat i lågintensitetskonflikter i perioden 1991–2004 har avhandlats. Dessa aktörer kan i framtiden nyttja fler och andra typer av medel som påverkar den elektroniska krigföringen. Hur påverkas vi av deras försök att styra striderna till miljöer där vi har svårt att verka med våra system? För exempelvis Nordic Battle Group finns en bredare hotbild att ta hänsyn till. Som om detta inte vore nog påverkas insatsförbandens taktiska verksamhet av de av Clausewitz definierade friktionerna, exempelvis slumpens inverkan. Vädrets nyckfullhet, fysisk utmattning och den mänskliga faktorn är några av de oberäkneliga faktorer som kan påverka förmågan och effekten av våra insatsförband. Dessutom finns den ekonomiska verkligheten som vi lever i. Den är kanske den mest styrande faktorn vilken obevekligt framtvingar nödvändiga prioriteringar.

En grundläggande delmängd i uppsatsens resultat är om alla frågor i uppsatsen är besvarade. Avsnittet 7.2 ovan får utgöra belägg för att så är fallet. Därmed har denna grundläggande delmängd i resultatet uppfyllts.

Syftet med uppsatsen var att klarlägga om tillförsel av moderna högteknologiska hjälpmedel för elektronisk krigföring ger några avgörande taktiska fördelar för våra internationella insatsförband i lågintensitetskonflikter. Och svaret blev ”ja”. Flera taktiska fördelar är belagda i uppsatsen, såväl från tillförsel av enskilda tekniska förmågor som från en kombination av sådana. Och det är bredden, de många alternativa sensorerna och synergin dom emellan som ger det stora mervärdet, de **avgörande** taktiska fördelarna. Syftet får därmed anses uppfyllt.

7.4 Värdering av uppsatsens metod

Fundamentet i uppsatsens resultat är den empiri som byggs upp i kapitel 2, 3 och 5 vilka beskriver hotbilden, insatsförbandens förmåga idag respektive teknikens möjligheter. En begränsning här är att hemliga dokument inte varit tillgängliga. Vad innebär detta? Vilka fakta har inte kommit fram? Hur påverkar detta svaren på frågorna? Skulle svaren bli annorlunda? Samma konsekvenser får den begränsade tiden som funnits till förfogande för arbetet med uppsatsen. Det är inte säkert att all information som finns i öppen litteratur kommit fram.

För kapitel 2 skulle ovan kunna innebära att en förmåga för elektronisk krigföring hos de icke-reguljära aktörerna inte har identifierats. Detta är en svaghet i uppsatsen som endast går att kompensera i efterhand inom de organisationer inom och utom Försvarsmakten som berörs. Dessa organisationer sitter sannolikt redan på denna typ av sekretessbelagda information varför

uppsatsen erbjuder dom en jämförelse och ett sammanhang att sätta in sin information i. Uppsatsen erbjuder också dessa organisationer en analysmodell för att värdera vilka taktiska fördelar egna motmedel skulle ge.

En sannolik konsekvens avseende kapitel 3 är att en i uppsatsen redovisad brist i insatsförbandens förmåga faktiskt redan gett upphov till planerad, eller kanske redan genomförd anskaffning. Vad har då uppsatsens resultat för värde? Uppsatsen kan definitivt i dessa fall bekräfta att anskaffningen varit motiverad. Ansvariga för anskaffningen kan också sätta in och värdera den i den helhet som förespråkas i den enskilt viktigaste slutsatsen i avsnitt 7.2 och 7.3 ovan. De ges helt enkelt en möjlighet att se anskaffningen i ett vidare perspektiv.

På vilket sätt är tidsavgränsningen 1991–2004 en begränsning? Uppenbart tas ingen hänsyn till äldre konflikter varför arvet riskerar att utelämnas. Sannolikheten för detta bedömer jag som försumbart liten eftersom de högteknologiska inslagen hos icke-reguljära aktörer i mycket hög grad påverkats av de senaste 10–15 årens snabba teknologiutveckling inom IT-området och de snabbt sjunkande priserna för moderna kommunikationsmedel som mobiltelefoni och Internet. Före denna utveckling var de icke-reguljära aktörerna i princip utan högteknologiska medel. Hur ser framtidsutsikterna ut då? Uppsatsen erbjuder de facto inte någon bedömning av framtiden mer än i den mån högteknologi fortsatt används av icke-reguljära aktörer. Men eventuella nya förmågor för elektronisk krigföring behandlas inte i uppsatsen. Detta är en medveten avgränsning, men ändå en svaghet för anskaffningar på lång sikt. På kort sikt är dock inte konsekvenserna enligt min mening av större betydelse eftersom bristerna redan är så omfattande i dagens insatsförband. Hur mycket värre kan det bli? Att komplettera med kunskaper om framtiden är dock inte svårare än att FOI redan idag har sådana forskningsprojekt. Alltså hade uppsatsen utan avgränsningen riskerat omfatta samma arbete som FOI redan gör. Men i ett helhetsperspektiv för Försvarsmakten finns det sannolikt ingen allvarlig forskningslucka avseende elektronisk krigföring i moderna lågintensitetskonflikter, varken bakåt i historien eller framåt i framtiden. Tvärtom så är förhoppningen att uppsatsen bidragit till att belägga nuläget med en vetenskaplig undersökning som ett komplement till de framtidsstudier som bedrivs inom och utom Försvarsmakten.

7.5 Behov av fortsatt forskning

Situationen i många av länderna i den tredje världen innebär att de har en ineffektiv ledning med mer eller mindre korrupta regimer. Detta leder till slutsatsen att antalet uppror och långvariga interna konflikter fortsatt kommer att vara högt i många år framöver.[145] Om Sverige vill spela en roll, nå framgång i, och därmed få inflytande på hanteringen av dessa konflikter är det angeläget att fortsätta forskning om lågintensitetskonflikter på bred front. Under arbetet med denna uppsats har en mängd frågor väckts som inte kunnat behandlas. Dessa utgör förslag på fortsatt forskning och annat fortsatt arbete. Förhoppningsvis kan de vara inspirationskälla till mer forskning och fler C-uppsatser i framtiden.

1. Hur bygger vi upp och säkerställer kompetens och kunskap om möjliga konfliktområden och dess lokala förhållanden? Hur ska den egna förmågan se ut och hur ska den kopplas till internationellt samarbete?

[145] Rekkedal, ”Nye trender innen krigføringen: Men kriger er i dag som i tidligere tider, vanskelige å forutse”, s.32.

2. Vad utöver klassisk bedömning av en motståndares organisation, taktik och materiel är det som underrättelsetjänsten dessutom ska kunna hantera? Lokala förutsättningar och stämningar? Trafficking? Illegal invandring? Rebellfraktioner? Organiserad kriminalitet? Flyktingsituationen? Farliga ämnen i jord, luft och vatten? Vanligt förekommande sjukdomar?
3. Hur ska stödet till insatsförbanden från underrättelseorganisationer i Sverige organiseras och ledas samt vilka uppdrag ska dessa enheter ha? CNO från fast gruppering i Sverige är bara ett exempel. Ett annat är OSINT som anses utgöra ungefär 95 procent av alla underrättelser.
4. Hur påverkar den icke-reguljära hotbilden i moderna lågintensitetskonflikter officersprofessionen i allmänhet samt officerare med elektronisk krigföring som inriktning? Ser vi en diversifiering av olika officerskategorier?
5. Vilket personalförsörjningssystem är lämpligast för att förse våra framtida insatsförband med kompetens inom elektronisk krigföring? Värnplikt, kontraktsanställningar eller yrkesanställningar? Hur ska ett utbildningssystem för valt system se ut?
6. Vilken språkberedskap ska Sverige ha? Vilka språk är aktuella nu och i framtiden?
7. Utvecklingen av kryptologi, vem vinner?
8. Interoperabilitet och sensorfusion. Hur kan olika sensorer samordnas och fusioneras? Vilka typer av sensorer är lämpliga? Hur hanteras sekretessgraderna?
9. Interoperabilitet och metoder för informationsutbyte inom underrättelsetjänsten. Hur hanteras sekretessgraderna?
10. Interoperabilitet och behov av kommunikationslösningar, gränssnitt och mjukvaror i syfte att kvalitativt förbättra inhämtning, analys och delgivning. Hur hanteras sekretessgraderna?
11. Interoperabilitet och metoder för identifiering på stridsfältet i syfte att undvika vådabeskjutning.
12. Behovet av att kunna anpassa egenskydd till konfliktens karaktär och nivå ställer krav på att kunna välja mellan en blandning av lättare och tyngre enheter och förband. Samtidigt är trenden att Försvarsmakten allt mer krymper både i storlek och i ekonomiska termer. Hur hanteras detta för så exklusiva resurser som de för elektronisk krigföring? Vilken flexibilitet är möjlig att bygga in i systemen?
13. De icke-reguljära aktörerna har mycket kortare ledtider för anskaffning. Hur kan vi hinna med i kapplöpningen och anpassa våra materielsystem så att vi kan ta och behålla initiativet i konfliktområdet och på stridsfältet?
14. Prioritera anskaffning av föreslagna tekniska förmågor utifrån en analys där kostnad vägs mot effekt.
15. Översyn av planerade förmågor för Försvarsmaktens insatsförband.

LITTERATUR- OCH KÄLLFÖRTECKNING

Otryckta källor:

Andén, Håkan, medarbetare på MUST.

Björs, övlt Christer, chef A3 vid Flygtaktiska kommandot.

Isberg, brigadgeneral Jan-Gunnar, ställföreträdande militär chef (Deputy Force Commander) och brigadchef i FN:s mission i Kongo, MONUC, 2004–2005.

Sjöqvist, Lars, forskare vid FOI, *Laserteknik för skydd av flygande plattformar* (presentationsunderlag i Power Point) [CD].

Sjöqvist, övlt Sten, Högkvarteret.

Artiklar och rapporter:

Arnsby, Jan (2004), *Radiomotmedel: Störning av radiokommunikation* (Linköping: Totalförsvarets forskningsinstitut, rev 4.7).

BBC (2004), *Madrid blasts: Who is to blame?* (London: BBC News World edition, 18 mars 2004) [www]. Hämtat från <http://news.bbc.co.uk/2/hi/europe/3512748.stm> 4 juli 2005.

Campbell, Duncan (1999), *Development of Surveillance Technology and Risk of Abuse of Economic Information*, part 2 (Luxemburg: European Parliament) [www]. Hämtat från <http://www.europarl.eu.int/stoa/publi/pdf/98-14-01-2_en.pdf> 13 juli 2005.

Campbell, professor Roy m.fl. (2002), *Analysis of Third Generation Mobile Security* (Chicago: University of Illinois at Urbana-Champaign), presentationsmaterial från Motorolas årliga projektrapportering 28 juni 2002 [www]. Hämtat från <http://srg.cs.uiuc.edu/MobilSec/posted_docs/3G_Security_Annual_Report.ppt> 10 juli 2005.

Ekblad, Ulf (2005), *Elementa om rymdteknik – Satelliter, spaning och kommunikation* (Stockholm: Totalförsvarets forskningsinstitut). ISSN 1650-1942.

Fors, Karina och Stenumgaard, Peter (2003) ”Elektronisk vådaskott viner i luften”, *Framsyn*, 2003, nr 2 (Stockholm: Totalförsvarets forskningsinstitut).

Försvarsmakten (2005), *Beredskapsenheter* (Stockholm: Försvarsmakten), [www]. Hämtat från <http://www.mil.se/int/article.php?id=274#> 24 oktober 2005.

Försvarsmakten (2001), *Försvarsmakten och Sveriges ordförandeskap i EU* (Stockholm: Försvarsmakten) [www]. Hämtat från <http://www.mil.se/?c=news&id=925> 28 april 2005.

Heide, Rachel Lea m.fl. (eds.) (2004), *Peacekeeping Intelligence: New Players, Extended Boundaries* (Ottawa: Carlton University), rapport från den andra konferensen ”Peacekeeping Intelligence”, Kanada 2003-12-04 [www]. Hämtat från <http://www.carleton.ca/csds/pki/doc/PKI_conference_report_2003.pdf> 25 april 2005.

Höstbeck, Lars (ed.) (2003), *Space and Defence* (Stockholm: Totalförsvarets forskningsinstitut). ISSN 1650-1942.

Moore, generalmajor Michael (2005), DN.se (2005), *EU:s insatsstyrka bäddar för svensk yrkesarmé* (Stockholm: DN.se), Dagens Nyheter, nätupplagan DN.se, 17 april 2005 [www]. Hämtat från <http:// www.dn.se/DNet/jsp/polopoly.jsp?d= 1042&a=404306> 28 april 2005.

Jakobsson, Johan (2004), *Terrorism och extremism som hotbild: Terrorism som fenomen samt som hotbild vid internationella insatser. Extremist- och terrorgruppers typologi, modus operandi och organisation* (Stockholm: Totalförsvarets forskningsinstitut). ISSN 1650-1942.

Krohné, mj Stig-Olof (2004), *CNI – en metod för terroristernas underrättelsetjänst?* (Stockholm: Försvarshögskolan, C-uppsats 2004).

Vego, Milan (2002), ”What Can We Learn from Enduring Freedom?”, *US Naval Institute Proceedings*, Vol 128, No 7.

Standardiseringsdokument:

3GPP (1999), *3G TR 33.120 version 3.0.0* (Frankrike: 3GPP).

3GPP (2000), *3G TR 33.900 version 1.2.0* (Frankrike: 3GPP).

ETSI (2005), *ETSI TS 133 107 V6.5.0* (Frankrike: ETSI).

Styrdokument från regeringen och riksdagen:

Regeringen (1994), *Regeringsförklaring 7 oktober 1994* (Stockholm: Regeringskansliet) [www]. Hämtat från <http://www.regeringen.se/content/1/c6/ 01/14/66/7dcdb8ae.pdf> 27 april 2005.

Regeringen (1996), *Regeringsförklaring 17 september 1996* (Stockholm: Regeringskansliet) [www]. Hämtat från <http://www.regeringen.se/content/1/c6/ 01/14/59/3903a8d0.pdf> 27 april 2005.

Regeringen (1997), *Regeringsförklaring 16 september 1997* (Stockholm: Regeringskansliet) [www]. Hämtat från <http://www.regeringen.se/content/1/c6/ 01/14/55/bab34f35.pdf > 27 april 2005.

Regeringen (2004), *Regeringsförklaring 14 september 2004* (Stockholm: Regeringskansliet) [www]. Hämtat från <http://www.regeringen.se/content/1/c6/ 02/96/52/e5f3b8fa.pdf> 27 april 2005.

Regeringen (1996), *Regeringens proposition 1996/97:4: Totalförsvar i förnyelse - etapp 2* (Stockholm: Riksdagen).

Regeringen (1999), *Regeringens proposition 1999/2000:30: Det nya försvaret* (Stockholm: Riksdagen).

Regeringen (2001), *Regeringens proposition 2001/02:10: Fortsatt förnyelse av totalförsvaret* (Stockholm: Riksdagen).

Regeringen (1997), *Regeringens skrivelse 1997/98:29: Euro-atlantiska partnerskapsrådet och det fördjupade Partnerskap för fred-samarbetet* (Stockholm: Regeringskansliet) [www]. Hämtat från <http://www.regeringen.se/content/1/c4/14/04/4093cd1a.pdf> 27 april 2005.

Riksdagen (2000), *Ministerrådspromemoria Den europeiska säkerhets- och försvarspolitiken (ESDP) inför Europeiska rådet i Nice* (Stockholm: Regeringskansliet) [www]. Hämtat från <http://www.riksdagen.se/eu/Riksdagen/EUN/MinisterPm/Ministerpm_0001_09_allmesdp.htm> 28 april 2005.

Statskontoret (2005), *Försvarets styrning – styrkedjan från statsmakternas beslut till verklighet* (Stockholm: Statskontoret) [www]. Hämtat från <http://www.statskontoret.se/upload/Publikationer/2005/2005109.pdf> 28 april 2005.

Militära publikationer och styrdokument:

Försvarsmakten (2004), *Doktrin för markoperationer – 2004* (Stockholm: Försvarsmakten), M7740-774004.

Försvarsmakten (2003), *Försvarsmaktens grundsyn informationsoperationer, IO* (Stockholm: Försvarsmakten, utkast, fastställt för tillämpning 2003-12-11).

Försvarsmakten (2002), *Militärstrategisk doktrin 2002* (Stockholm: Försvarsmakten), M7740-774002.

Försvarsmakten (2004), *Preliminär taktisk, organisatorisk och ekonomisk målsättning för TELEVAPENTROPP 2004 INT PTOEM TVA-to 04 INT* (Stockholm: Högkvarteret), HKV 01 631:771 79.

Försvarsmakten (2003), *Årsrapport från perspektivplaneringen 2002–2003; Målbildsinriktningar inför Försvarsbeslut 2004 – rapport 7* (Stockholm: Försvarsmakten), M7740-779005.

Tryckt litteratur:

Baudin, Arne; Hagman, Thomas och Ångström, Jan (eds.) (2002), *En ny medeltid? En introduktion till militärteori i lågintensiva konflikter* (Stockholm: Försvarshögskolan), ISBN 91-89683-12-9.

Clarke, Walter och Herbst, Jeffrey (eds.) (1997), *Learning from Somalia: The Lessons of Armed Humanitarian Intervention* (Boulder: Westview Press), ISBN 0-8133-2794-6.

Clausewitz, Carl von (1991), *Om kriget* (Stockholm, Bonnier Fakta bokförlag AB, översättning och granskning av Hjalmar Mårtensson, Klaus-Richard Böhme och Alf W Johansson), ISBN 91-34-51163-6.

Davida, George; Frankel, Yair och Rees, Owen (eds.) (2002) *Infrastructure Security: International Conference, InfraSec 2002 Bristol, UK, October 1-3, 2002 Proceedings* (Berlin: Springer), ISBN 3-540-44309-6 [www]. Hämtat från <http://www.isg.rhul.ac.uk/msc/teaching/ic3/GSM_Security_v4.pdf> 8 juli 2005.

FOI (2005), *FOI orienterar om: Rymden – nytta och teknik*, 2005, nr 4 (Stockholm: Totalförsvarets forskningsinstitut).

FOI (2004), *FOI orienterar om: Sensorer*, 2004, nr 3 (Stockholm: Totalförsvarets forskningsinstitut).

FOI (2005), *FOI orienterar om: Telekrig*, 2005, nr 5 (Stockholm: Totalförsvarets forskningsinstitut).

Gunaratna, Rohan (2002), *Inside Al Qaeda: Global Network of Terror* (New York: Columbia University Press), ISBN 0-231-12692-1.

Honig, Jan Willem och Both, Norbert (1996), *Srebrenica: Record of a War Crime* (London: Penguin Books), ISBN 0-14-026165-6.

Kaldor, Mary (1999), *Nya och gamla krig: Organiserat våld under globaliseringens era* (Göteborg: Bokförlaget Daidalos AB, översättning av Joachim Retzlaff), ISBN 91-7173-117-2.

Rekkedal Nils Marius (2004), *Modern krigskonst* (Stockholm, Försvarshögskolan, tredje upplagan), ISBN 91-89683-73-0.

Språkdata Göteborgs universitet (1995), *Nationalencyklopedins ordbok* (Höganäs: Bra böcker AB).

Stevenson, Jonathan (1995), *Losing Mogadishu: Testing U.S. Policy in Somalia* (Annapolis, Naval Institute Press), ISBN 1-55750-788-0.

Wentz, Larry (ed) (1997), *Lessons from Bosnia: The IFOR Experience* (Washington: DoD Command and Control Research Program), ISBN 1-57906-004-8.

World Wide Web:

Accelerated Promotions (2005), *Cellular Phone GSM TDMA Interceptor Pro System* (USA: Accelerated Global Inc.) [www]. Hämtat från <http://www.accelerated-promotions.com/consumer-electronics/cellular-interception-gsm-system-specifications.htm> 8 juli 2005.

Försvarsmakten (2005), *Personal i utlandsstyrkan 1 april 2005* (Stockholm: Försvarsmakten) [www]. Hämtat från <http://www.mil.se/int/attachments/us-april-2005.pdf> 28 april 2005

Global Security.org (2005), *Man Portable Air Defense Systems (MANPADS)* (Alexandria: Global Security.org) [www]. Hämtat från <http://www.globalsecurity.org/military/intro/manpads.htm> 8 september 2005.

GSM World (2005), *GSM Global Networks on Air* (London: GSM Association) [www]. Hämtat från <http://www.gsmworld.com/news/statistics/networks_complete.shtml> 8 juli 2005.

Homeland Security Strategies, *Cellular Intercept Systems* (USA: Security Intelligence Technology Group), [www]. Hämtat från <http://www.cellularintercept.com/default.aspx> 8 juli 2005.

Reinema, Dr Rolf (2004), ”Security Management – Part 2: Wireless Security”, föreläsningsunderlag, Computer Society Malta och Fraunhofer Institut Sichere Informations-Technologie *IT Security Management*, konferens 29-30 januari 2004, Sliema, Malta [www]. Hämtat från http://www.csm.org.mt/pdf/Fraunhofer/Mobile_Sec_Part2_v2.pdf 25 oktober 2005.

Security Intelligence Technologies Group, *Bombjammer.com* (USA: Security Intelligence Technology Group) [www]. Hämtat från <http://www.bombjammer.com/default.aspx> 12 juli 2005.

Wireless LAN Association (2005), *What is a Wireless LAN?* [www]. Hämtat från http://www.wlana.org/learn/educate.htm 25 oktober 2005.

FÖRKORTNINGAR

3G	Tredje generationens mobiltelefonisystem
AM	Amplitudmodulering
AP	Access Point
CIMIC	Civil Military Cooperation
CNA	Computer Network Attack, dator- och nätverksattack
CND	Computer Network Defence, dator- och nätverksförsvar
CNE	Computer Network Exploitation, dator- och nätverksexploatering
CNO	Computer Network Operations, dator- och nätverksoperationer
COMINT	Communication Intelligence
dB	Decibel
DIRCM	Directed Infra Red Countermeasures
EAPC	Euro-Atlantic Partnership Council
ELINT	Electronic Intelligence
EMCON	Emission Control
EOD	Explosives and Ordnance Disposal
EU	Europeiska unionen
FARC	Fuerzas Armadas Revolucionarias de Colombia
FDMA	Frequency Division Multiple Access
FLIR	Forward Looking Infra Red
FM	Frekvensmodulering
FN	Förenta nationerna
FOI	Totalförsvarets forskningsinstitut
GMTI	Ground Moving Target Indicator
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HFC	Helsinki Force Catalogue
HPM	Högeffektpulsad mikrovågsstrålning
HUMINT	Human Intelligence
IED	Improvised Explosive Devices
IEDD	Improvised Explosive Device Disposal
IEEE	Institute of Electrical and Electronics Engineers
IFOR	Implementation Force
IMEI	International Mobile Equipment Identity
IMINT	Imagery Intelligence
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IR	Infra Red, infraröd
ISP	Internet Service Provider
IT	Informationsteknologi
JAS	Jakt, attack, spaning
JSTARS	Joint Surveillance Target Attack Radar System
LAN	Local Area Network
MAC	Medium Access Control
MANPAD	Man-Portable Air Defence Missile
MHz	Megahertz
MONUC	Mission de l'Organisation des Nations Unies en RD Congo
MOOTW	Military Operations Other Than War

MSISDN	Mobile Station Integrated Services Digital Network
Nato	North Atlantic Treaty Organization
NBC	Nuclear Biological Chemical
NLJD	Non Linear Junction Detection
NORDCAPS	Nordic Coordinated Arrangement for Military Peace Support
OODA	Observation Orientation Decision Action
OSINT	Open Sources Intelligence
PfP	Partnership for Peace
ROE	Rules of Engagement
SA	Surface-to-Air, om luftvärnsmissiler
SAR	Synthetic Aperture Radar, syntetisk aperturradar
SHIRBRIG	Standby Force High Readiness Brigade
SIGINT	Signal Intelligence, signalspaning
SMS	Short Message Service
SSB	Single Side Band
SSID	Service Set Identifier
SWAFRAP	Swedish Air Force Rapid Reaction Force
SWENARAP	Swedish Navy Rapid Reaction Force
TDMA	Time Division Multiple Access
TMSI	Temporary Mobile Subscriber Identity
UAV	Unmanned Aerial Vehicle
UCK	Ushtria Clirimtare E Kosoves
UHF	Ultra High Frequency
UNITA	Uniao Nacional para Independencia Total de Angola
UNOSOM	United Nations Operation in Somalia
UNSAS	United Nations Stand-by Arrangements System
UNPROFOR	United Nations Protection Force
UV	Ultraviolett
VHF	Very High Frequency
VMS	Varnings- och motverkanssystem
WCDMA	Wideband Code Division Multiple Access
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network, kallas även för radio-LAN
WPAN	Wireless Personal Network

Swedish National Defence College
Research Paper

Author	**Unit**	**Course**
Maj Niclas Holmquist	Uppland Regiment	Advanced Command Course - Electronic Warfare

SNDC tutors
Ph.D. EE Per Hyberg and Capt (M.Sc. EE) Magnus Astell

Commissioned by
Department of War Studies

Abstract: **Electronic Warfare and Computer Network Operations in Low Intensity Conflicts**

Sensor Fusion for Effective PSO Units

The technical systems of today's Swedish Armed Forces are geared essentially to meet an attack by the regular military forces of a super power of the Cold War era. As a result, Sweden's EW (electronic warfare) and CNO (computer network operations) operational capabilities are not well placed to cope with modern low-intensity conflicts.

The aim of this research paper is to investigate whether provision of modern high-tech means for EW and CNO provides any decisive tactical advantages for our PSO units when they are involved in operations against non-regular actors in the modern low-intensity conflicts of today.

This research paper points out significant shortcomings in our PSO units and emphasises the essential need to provide these units with SIGINT and jamming capabilities in order for them to be able to counter a wide range of communications systems. Furthermore, the basic capability "intelligence & information" will benefit the most from provision of new EW and CNO technology. Work will need to concentrate on integrating the various intelligence capabilities, such as SIGINT, IMINT, HUMINT, and OSINT, including the support provided by different intelligence organisations at home. EW and CNO, with their different technical sensors, will undoubtedly play a very important role in this process. Consequently there is all reason to look at the provision of a new technical capability for our PSO units as a whole rather than autonomous systems.

Key words: Asymmetry, Computer Network Operations, Electronic Warfare, Guerrilla Warfare, Low Intensity Conflicts, Intelligence, Sensor Fusion, Terrorism.