

ARKITEKTUR för MILITÄRA LEDNINGSSYSTEM

Ämnet för dagen är ju Arkitektur då, nu och sedan. I inledningen till den kommande diskussionen vill jag koncentrera mig på ledningssystemen inom försvaret.

Den vedertagna betydelsen av ordet *arkitektur* torde vara byggnadskonst. (Arkitekt kan härledas från de två grekiska orden arki och tekton som betyder förnämlig respektive timmerman.) Till följd av att språken inte längre tycks utvecklas i samma takt som behovet av att beskriva nya upptäckter, fenomen och produkter tvingas vi att använda gamla ord på sätt som inte avsågs från början. Det gör språket oklart och leder ofta till missförstånd. Exempel på sådana ord är system, design, nätverk, patterns etc. Egentligen borde man kunna ”kvittera ut” ett helt nytt ord från någon global språkinstans när ett behov bevisligen uppstått. Men vi får nog tyvärr leva med dessa språkliga problem även i fortsättningen

Från att bara betyda byggnadskonst har ordet arkitektur inom datatekniken kommit att först betyda en dators inre uppbyggnad, såväl hård- som mjukvara, för att nu mer övergå till att omfatta hela strukturen av ett system där datorer ingår i mer eller mindre omfattning. Det aktuella systemet kan vara alltifrån ett mycket överordnat sådant till ett mindre delsystem inom ett större system. Arkitektur i vidare bemärkelse är således inte bara IT-system och än mindre bara mjukvara.

Vad är då ett *militärt ledningssystem*? Jag skulle vilja definiera det som ett system vars uppgifter är att skapa och överföra information om motståndarens och mina egna förbands tillstånd, bearbeta och sammanställa information från olika källor, presentera information för beslutsfattare, ge dessa stöd för beslut, överföra order till verkställande enheter såsom informationskällor, kommunikationssystemens ledning och främst till ledare av olika luft-, sjö, och lantstridskrafter.

Ledningssystem finns på olika nivåer alltifrån högkvarterets strategiska, operativa nivå ned till taktisk ledning av enskilda förband och enheter. Som exempel på den operativa nivån kan ledningen av luftförsvaret från ett flygkommando gälla. Ledning från luftförsvarets stridsledningscentraler, STRIC och från kustkorvetterna samt ledning inom ett jaktstridsförband kan exemplifiera ledningssystem på den taktiska nivån liksom det system en förare använder sig av i ett Gripenflygplan. Om vi i fortsättningen kommer att kunna samarbeta med Nato-förband tillkommer ytterligare en nivå.

Det totala ledningssystemet består alltså av olika ledningssystem på olika nivåer. Alla dessa måste kommunicera med varandra medelst kommunikationssystem. Systemen kan vara mer eller mindre beroende av varandra. Ledningssystemen kan också vara integrerade i olika stridsförband, med sina arkitekturer, på olika nivåer. I kommande system kommer möjligheterna till information vara mycket stor; naturligtvis under förutsättning av robusta kommunikationssystem. Det gäller dock fortfarande att utnyttja tekniken på rätt sätt, bland annat genom att fastställa vem som har rätt till information och vem som har rätt att utfärda order till olika förband med hänsyn till erforderlig delegering av ansvar. Detta är inte ett tekniskt problem utan snarare ett organisatoriskt.

Man kan skilja på ledningssystem på övergripande nivå där besluten oftast inte behöver fattas sekundsnabbt och stridsledningssystem som arbetar mer eller mindre i real-time. I det senare fallet kan ledningssystemet snarast karakteriseras som ett servosystem. Ett exempel på detta är luftförsvaret med jaktflygplan. Länkarna i servokedjan utgörs av motståndarflygplanen, mark- och flygburna radarstationer, stridsledningscentralen med sina datorer för beräkning av optimala flygbanor samt jaktflygplanen. När så jaktflygplanen närmar sig målen bildas en ny servokedja bestående av mål, jaktflygplanets radar, dess styrsystem etc.

I Sverige måste Flygvapnet anses ha haft en ledande roll vid uppbyggnad av ledningssystem. Även med internationella mått har man varit på framkanten. Följande exempel kan nämnas: Flygplan J35 var antagligen det första datastridsledda jaktflygplanet i världen. Det var STRIL60 med sina datorer och datalänken upp till flygplanen som möjliggjorde detta. AJ37 var det andra krigsflygplanet i

världen som fick en dator inbyggd i sitt avioniksystem. Ordet dator var inte uppfunnit på den tiden, dvs tidigt 1960-tal. AJ37's dator fick därför benämningen central kalkylator CK37. Den har använts ända in i våra dagar. JA37 modifierades tidigt med en sk jaktlänk, innebärande att inte bara STRIL kunde skicka data till jaktflygplanen utan att dessa kunde sända data ner till STRIL och sinsemellan, vilket var ett stort steg framåt avseende jaktflygplanens effektivitet. Försvarets telenät byggdes också upp från 1950-talet och framåt i samarbete med Televerket och består av olika radio-, radiolänk- och kabelförbindelser i vad som nu så populärt kallas nätverk.

Även beträffande administrativa datasystem var Flygvapnet tidigt ute, till exempel reservdelsförsörjningssystemet.

Beträffande försvarets olika sk stabsledningssystem får man nog säga att födslovändorna varit stora. Det har nog inte så mycket varit tekniska problem utan problem med ledning av framtagningen av dessa ledningssystem.

Men i det stora hela måste man anse att många effektiva system skapats till rimliga kostnader inom vårt försvar. Orsaken till detta var tillgången på kvalificerad personal både vid industrin och i förvaltningen samt en långsiktande forskning och framsyn i övrigt.

Men nu gäller det framtiden. Vi måste bygga vidare på existerande system, men givetvis också skapa nya och därvid utnyttja ny teknik på ett rationellt sätt för att förändra vårt försvar så att det även kan möta nytillkomna hot.

Varje hot kräver en viss typ av försvar sammansatt av olika stridsförband (eller motsvarande). Dessa måste i sin tur bestå av personal, organisation och materielsystem. Dessa förband kan ofta utnyttjas i flera hotsituationer. Det ekonomipolitiska läget i landet innebär att vi inte anses ha råd att möta alla hotsituationer med tillräcklig kvantitet av försvarsresurser. En prioritering baserad på bedömd sannolikhet för olika hot måste göras. Exempelvis anser man nu att risken av en stort upplagd invasion mot vårt land är låg. Just nu, borde man tillägga. Om denna prioritering visar sig felaktig tror de styrande politikerna att det finns tid att rusta upp. Det fanns det inte förra gången.

Av säkerhetspolitiska skäl bör förändringar ske inom vårt försvar. Det är nog alla överens om. Men hur det skall ske finns det delade meningar om, även om regering, ÖB och högkvarteret gett ut riktlinjer.

Vad är då det nya? Till följd av Sovjetunionens och Warszawapaktens upplösning och det utökade säkerhetspolitiska samarbetet inom EU har tre väsentliga ändringar skett:

*Dels har det säkerhetspolitiska läget förbättrats i vår närhet, men latent risker för konflikter finns dock kvar..

*Dels har det nu blivit möjligt att samverka med andra demokratiska nationers försvarsorganisationer på ett helt annat och omfattande sätt än som var förenligt med vår utrikespolitik under det kalla kriget. Det är mycket positivt och bidrar till vår säkerhet och till bevarande av freden i vår närzon. Men det bör dock påpekas att vi inte tagit steget fullt ut mot ett solidariskt ansvar, utan fortfarande står utanför genom vår alliansfria politik.

*Dels innebär denna samverkan en viss integration med exempelvis Nato's ledningssystem och kommunikationssystem samt krav på sk interoperability mellan våra förband och materielsystem och Nato's motsvarande enheter.

Ovanpå detta kommer att nya hot, som förut betraktades mer hypotetiska, nyligen har visat sig högst reella.

Även om vi på många områden, särskilt materielområden, raskt skulle vilja skrota befintliga system och ständigt omsätta dem med nya måste vi inse att detta varken effektivitetsmässigt, ekonomiskt eller praktiskt är vare sig optimalt eller möjligt. Vi har ett antal materielsystem och ledningssystem som är effektiva i flera hotsituationer. I vissa fall krävs nya. *Men vi måste alltid leva med det faktum att försvarets materiel alltid kommer att förnyas successivt.* Även de nya måste konstrueras så att de kan samverka med existerande system. Detta är ett oavvisligt krav och ett mycket svårt krav att ta hänsyn

till vid nykonstruktioner. En annan försvårande faktor är att materielen måste kunna underhållas och i vissa fall uppgraderas under flera decennier, detta trots IT-branschens tendens till generationsväxlingar med kortare tidsintervall.

Dagsläget är att vi beträffande verkanssystem (flygplan, stridsvagnar etc) och stridsledningssystem har ett ganska bra läge, i varje fall kvalitativt. Däremot krävs en snar förnyelse inom stabsledningssystemen. Kommunikationssystemen, de som förr kallades sambandssystem, måste byggas på och framförallt göras mer stryktåliga.

Försvaret skall alltså genomgå en ganska stor omstrukturering, eller för att tala med dagens språk: Arkitekturen måste ändras. Det erfordras en bättre balans mellan verkansenheter, stridsförbanden å ena sidan och informations- och ledningssystemen å andra sidan. Detta måste förberedas genom optimeringsstudier. Dessa studier bör baseras på hotbilden, dvs olika konfliktsituationer och uppgifter för försvaret, möjlig teknisk utveckling samt ekonomiska ramar. Det mest osäkra här är naturligtvis hotbilden. Vi kan ställas inför konfliktsituationer i vår närhet, dvs hot mot oss eller våra grannar, där solidaritet krävs av oss, eller mer i periferin på större avstånd eller t.o.m inom vårt land.

Studierna måste bedrivas *top-down på en övergripande nivå* för att få balans mellan försvarets olika delar, fördelat på de olika tänkbara konfliktsituationerna. Men samtidigt måste idéer angående nya materielsystem skapas, grundade på den möjliga *tekniska utvecklingen*. Det måste ske en iteration mellan de övergripande systemstudierna och studierna av materielsystem. Några exempel: Luftförsvarets resurser och kostnader måste vägas mot fjärrstridsförbandens. Inom luftförsvaret måste balans skapas mellan markbundna och luftburna radarstationer, stridsledningscentraler, jaktflygplanprestanda, vapenprestanda samt luftvärnssystem. En komplikation vid avvägningen, fast operativt en stor fördel, är att flera materielsystem är användbara för olika försvarsuppgifter. Ett fall är flygplan 39 Gripen, som ingår både i luftförsvaret och fjärrstridsförbanden

Det finns olika verktyg för att arbeta med detta arkitekturarbete. Modellering och simulering har använts ända sedan 1950-talet inom försvaret. Datorutvecklingen har betytt att simuleringar med tiden har kunnat gjorts mer realistiska och omfattande. Goda resultat har erhållits på materielsystemnivå. Redan för JA37 användes hybridsimuleringar av jaktuppdrag där Stril60 eller en simulator för detta system kopplades ihop med JA37-flygplan eller dess systemsimulator. På mer övergripande nivåer såsom det militära försvaret eller totalförsvaret blir modellerna mer svårhanterliga. De tar lång tid att utveckla, för att inte tala om att verifiera. Modellbyggarna ställs inför valet att åstadkomma mindre relevanta modeller eller att arbeta mycket långsiktigt och kostsamt. Det har varit och kommer att vara en svår avvägning även i framtiden. Inte desto mindre är modellering och simulering ett av de kraftigaste verktyg vi har för optimering på alla nivåer.

Inom det svenska försvaret har alltså optimeringsstudier bedrivits i ganska stor omfattning. Ledningen av dem har inte alltid varit rationell. Framförallt har man inte haft någon enhet som kontinuerligt kunnat ägna sig åt detta arbete och därvid kunnat samla på sig successivt ökad erfarenhet.

Men simulering kan utnyttjas inte bara under studier av framtida system utan även under ett systems hela livslängd. När man väl valt ett system, definierat i stora drag, måste man optimera dess ingående delsystem mot varandra samt specificera mätbara kontraktskrav. Simulering utnyttjas också vid utprovning och modifieringar, taktisk optimering, utbildning och i framtiden förhoppningsvis även som beslutsstöd.

Rent administrativt kan man strukturera arbetet med ny arkitektur enligt det mönster som nu skapas inom USA's försvar. Flera styrande dokument har framkommit såsom JTA (Joint Technical Architecture), C4ISR (Command, Control, Communication, Computation, Surveillance, Reconnaissance), TRM (Technical Reference Modell), ADL (Architecture Description Language) m fl. Här delar man in försvarsuppgifterna i olika domäner och underdomäner. Inom dessa och i vissa fall mellan dem förväntar man sig göra avvägda strukturer, arkitekturer. Systemen antages byggas upp i noder med definierade samfunktioner. Gränsskikt inom ett system mellan noderna och inom noderna

samt till samverkande system förväntas definieras på ett standardiserat sätt inte minst när det gäller mjukvaran.

Detta är väl egentligen inget nytt sätt, utan mer ett sätt att bättre ordna sitt arbete. På lägre nivåer kan dock viktiga standarder komma fram som kan bli styrande även för oss, inte minst om vi beaktar kraven på interoperability med Nato-förbanden.

Den nya tekniken ger onekligen stora möjligheter. Bättre möjligheter för att kunna utnyttja information från flera datakällor finns nu, datafusion. Vi kan bygga kommunikationssystem med mycket stor kapacitet för att överföra information.

Säkerheten måste dock beaktas bättre i fortsättningen. Det krävs åtgärder på alla nivåer mot intrång, störning, förstöring (data och hårdvara), vilseledning etc. Det kanske verkar tjatigt att påpeka detta, men erfarenheten visar att nya metoder att störa och förstöra ständigt utvecklas. Vi måste skaffa mer robusta system och införa en högre grad av redundans. Personligen tycker jag att problemet delvis också är av organisatorisk karaktär. Teknisk kan informationsflödet öka enormt, men borde vi inte i stället försöka begränsa en del krav?

Ett annat område som jag uppfattar som bekymmersamt är möjligheten till *beslutsstöd*. Det har pratats mycket om detta och artificiell intelligens. Men få användbara resultat har kommit fram. Eftersom den mänskliga hjärnan inte mätbart ändrat sig på flera tusen år borde en trängd beslutsfattare verkligen få bättre stöttning i sina avgöranden när han nu riskerar att formligen översköljas med information.

Vilka resurser krävs det då? För att kunna skapa och vidmakthålla ledningssystem, och även annan materiel, på ett effektivt sätt inom försvaret krävs alltså att grundstrukturen, arkitekturen kan specificeras tillräckligt bra med hänsyn till hotbild, tekniska möjligheter, kostnader, samverkan med andra system och försvarsmakter. För att sedan skapa systemen erfordras skicklig personal vid vår industri men även inom förvaltningen och försvaret i övrigt. Man får hoppas att åtminstone IT-delen av vår försvarsindustri fortfarande kan upprätthålla en tillräcklig kapacitet för att till stor del utveckla och producera dessa viktiga delar av vårt försvar. IT-industrin finansieras ju till största delen av civila kunder varför den inte blir så beroende av militära kunder som den övriga försvarsindustrin.

Utökad samverkan med andra nationers försvar och minskad kapacitet hos vår försvarsindustri medför att vi måste samarbeta med andra länders industri vid framtagning av försvarsmateriel. Frågan om när samarbete är mer lönsamt än egen tillverkning eller direktköp blir nu mer aktuell. Samarbete har sina för- och nackdelar för försvaret och för vår industri. Det är ej möjligt att vidare utveckla detta spörsmål här. Frågan är mycket komplicerad.

Under många gånger har relationerna mellan försvarets förvaltningsmyndigheter och försvarsindustrin diskuterats. Pendeln har svängt mellan ett starkt ömsesidigt beroende med långsiktiga anskaffningsplaner till att endast de gällande kortsiktiga beställningarna varit bindande för parterna. Vid utformningen av de olika arkitekturerna på de olika nivåerna måste ekonomiska och andra kommersiella hänsyn tas vid utformningen och specificerandet av nya system. För att en leverantör skall kunna ges ansvar för en viss produkt, hårdvara likväl som mjukvara, måste hans åtagande kunna definieras och resultaten verifieras. Att arbeta i sk nätverk synes praktiskt när det gäller forskning. Men det verkar inte särskilt realistiskt för utveckling och tillverkning, utan mer traditionella hierarkiska organisationer blir nog nödvändigt även i fortsättningen om prestanda, tid och kostnader skall innehållas.

Inom försvaret vill man nu lägga mer vikt vid informations- och ledningssystem än förut, vilket är rätt. Märk dock att det fortfarande gäller att ha rätt balans mellan dessa och de sk verkanssystemen. Hur stora medel finns då tillgängliga inom en viss framtid? Det borde på något sätt, åtminstone grovt, antydast för aktuell industri vilken storleksordning det rör sig om.

Slutledning: Arkitektur, strukturering behövs på alla systemnivåer inom försvaret inklusive ledningssystemen. Struktureringen och optimeringen av försvaret är en viktig utgångspunkt för utformning av ledningssystem.

En evolutionär uppbyggnad av ledningssystemen är nödvändig på grund av den successiva materielomsättningen inom försvaret. Förvarssystem inom IT-sektorn har en längre livslängd än vad som åtminstone tills vidare gäller den civila marknaden.

Den tekniska utvecklingen skapar stora möjligheter. Ledningssystemen måste dock byggas med stor vikt på att de skall vara robusta och stryktåliga. Härvid är också organisatorisk strukturering av informationen (behörighet, begränsningar etc) viktig.

Olika former av beslutsstöd bör om möjligt skapas.

Nya krav ställs på samverkan med andra nationers försvar, vilket påverkar utformningen av våra försvarsmaterielsystem.

Utveckling och tillverkning av ledningssystem bör åtminstone till viss del ske inom landet.

Speciell uppmärksamhet bör ägnas åt de erforderliga personella resurserna inom industrin och försvaret.

Gunnar Lindqvist
2001-10-24