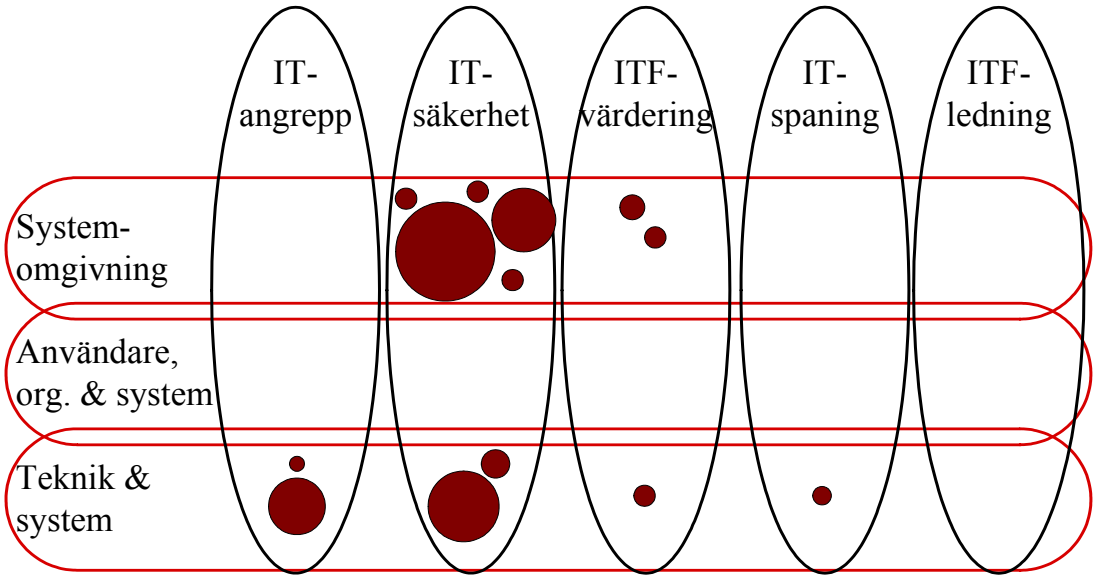
FOI
TOTALFÖRSVARETS
FORSKNINGSINSTITUT

FOI-R--0469--SE
Januari 2002
ISSN 1650-1942
Användarrapport

Jonas Hallberg, Amund Hunstad, E Anders Eriksson, Sören Palmgren

Områdesanalys: IT-försvar



Ledningssystem
581 11 Linköping

TOTALFÖRSVARETS FORSKNINGSINSTITUT

Ledningssystem
Box 1165
581 11 Linköping

FOI-R--0469--SE

Januari 2002

ISSN 1650-1942

Användarrapport

Jonas Hallberg, Amund Hunstad, E Anders Eriksson, Sören Palmgren

Områdesanalys: IT-försvar

Utgivare Totalförsvarets Forskningsinstitut - FOI Ledningssystem Box 1165 581 11 Linköping	**Rapportnummer, ISRN** FOI-R--0469--SE	**Klassificering** Användarrapport
	Forskningsområde 4. Spaning och ledning	
	Månad, år Januari 2002	**Projektnummer** E0618
	Verksamhetsgren 5. Uppdragsfinansierad verksamhet	
	Delområde 41 Ledning med samband och telekom och IT- system	
Författare/redaktör Jonas Hallberg Amund Hunstad E Anders Eriksson Sören Palmgren	**Projektledare** Jonas Hallberg	
	Godkänd av	
	Uppdragsgivare/kundbeteckning Försvarsmakten	
	Tekniskt och/eller vetenskapligt ansvarig	

Rapportens titel

Områdesanalys: IT-försvar

Sammanfattning (högst 200 ord)

Denna rapport innehåller en analys av området IT-försvar, vilken enligt uppdraget ska ”... vara en utgångspunkt för FM att formulera ett program för området och för att inrikta beställningar”. I ett första steg togs en områdesstruktur, bestående av fem IT-försvarsförmågor och tre aspekter på dessa, fram. Strukturen kan användas för att kategorisera verksamhet och kompetens inom området, men också för att visa på områdets stora omfattning och tvärvetenskapliga natur. I ett andra steg identifierades sju problemområden vilka kräver forskningsinsatser. Genom att infoga problemområdena i strukturen erhålls en bild av deras omfång. I ett tredje steg sammanställdes nationell verksamhet med forskningsmässig tyngdpunkt inom området.

En slutsats är att forskning inom området IT-försvar är av mycket stark tvärvetenskaplig natur. Samtidigt är dock fokusering av yttersta vikt för att kunna tillföra något nytt inom området. Därmed framstår behovet av forskningsprogram där fokusering och överblick harmoniserar. Krav på både bredd och djup (fokusering) medför att volymen blir stor, alltså behövs betydande satsningar som involverar *alla* de identifierade problemområdena.

Det är i nuläget inte möjligt att göra någon slags prioritering mellan problemområdena. Alla är viktiga. Ett första mål måste vara att få upp forskningsverksamheten till en rimlig grundnivå inom vart och ett av problemområdena. Därefter kan prioriteringar och omfördelningar göras alltefter behov och resultat.

Nyckelord

IT-försvar, IT-säkerhet, IT-angrepp, IT-spaning, IT-försvarsvärdering, IT-försvarsledning, IT-vapen

Övriga bibliografiska uppgifter	**Språk** Svenska
ISSN 1650-1942	**Antal sidor:** 30 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization	Report number, ISRN	Report type
FOI – Swedish Defence Research Agency Command and Control Warfare Technology P.O. Box 1165 SE-581 11 Linköping	FOI-R--0469--SE	User report
	Research area code 4. C4ISR	
	Month year January 2002	**Project no.** E0618
	Customers code 5. Commissioned Research	
	Sub area code 41 C4I	

Author/s (editor/s)	Project manager
Jonas Hallberg Amund Hunstad E Anders Eriksson Sören Palmgren	Jonas Hallberg
	Approved by
	Sponsoring agency Swedish Armed Forces
	Scientifically and technically responsible

Report title (In translation)

An Analysis of the Computer Network Operations Area

Abstract (not more than 200 words)

This report contains an analysis of the computer network operations area. The purpose is to deliver a basis for the Swedish Armed Forces to decide upon new research programs within the area. First, a structure of the area, consisting of five IT-defence capabilities and three aspects of these capabilities, was developed (four of the capabilities are included in the concept of CNO, which thus in principle equals the area of IT-defence). The structure can be used to categorize work and competence, but also to reveal the size and inter-disciplinary character of the area. Second, seven problem areas requiring research efforts were identified. Placing the problem areas in the structure reveals the size of the respective areas. Third, national research activity within the area of IT-defence was compiled.

An important conclusion is that the area of IT-defence is strongly inter-disciplinary. However, at the same time, focus is required in order to be able to generate new results. Thus, the demand for research programs incorporating both width and focus is apparent. Moreover, all the seven identified problem areas have to be addressed.

Currently, it is not possible to prioritise between the problem areas. First, the activity within each area has to be raised to reach a critical mass. Thereafter, prioritisation and redirections can be done according to current needs and results.

Keywords

Further bibliographic information	**Language** Swedish
ISSN 1650-1942	**Pages** 30 p.
	Price acc. to pricelist

Innehåll

1. Inledning

Denna rapport innehåller en analys av området IT-försvar, vilken enligt uppdraget ska:

> *... vara en utgångspunkt för FM att formulera ett program för området och för att inrikta beställningar mot en överblick av tillgänglig kompetens.*

Distribuerade informationssystem är, eller kommer snart att vara, en viktig del av de flesta organisationer och större tekniska system. Därmed utgör säkerheten hos dessa informationssystem en förutsättning för väl fungerande system, organisationer och samhällen. IT-försvar är en benämning för alla de mekanismer och organisationer som verkar för upprätthållandet av säkerheten hos de distribuerade informationssystemen. Begreppet IT-försvar inkluderar således defensiva såväl som offensiva metoder och tekniker.

Utvecklingsriktningen mot allt större integration mellan informationssystem resulterar i vitt omfattande distribuerade system, vilkas säkerhet med stor sannolikhet kommer att utsättas för omfattande prov. Därför är det av yttersta vikt att helhetsgrepp tas på de faktorer som påverkar säkerhetsnivåerna i de framväxande strukturerna. Punktvisa insatser utan helhetssyn leder snabbt till en kaotisk situation där inte ens grova uppskattningar av säkerhetsnivån är möjliga och där nyttan av ytterligare insatser inte går att validera.

1.1 Arbetets genomförande och avgränsningar

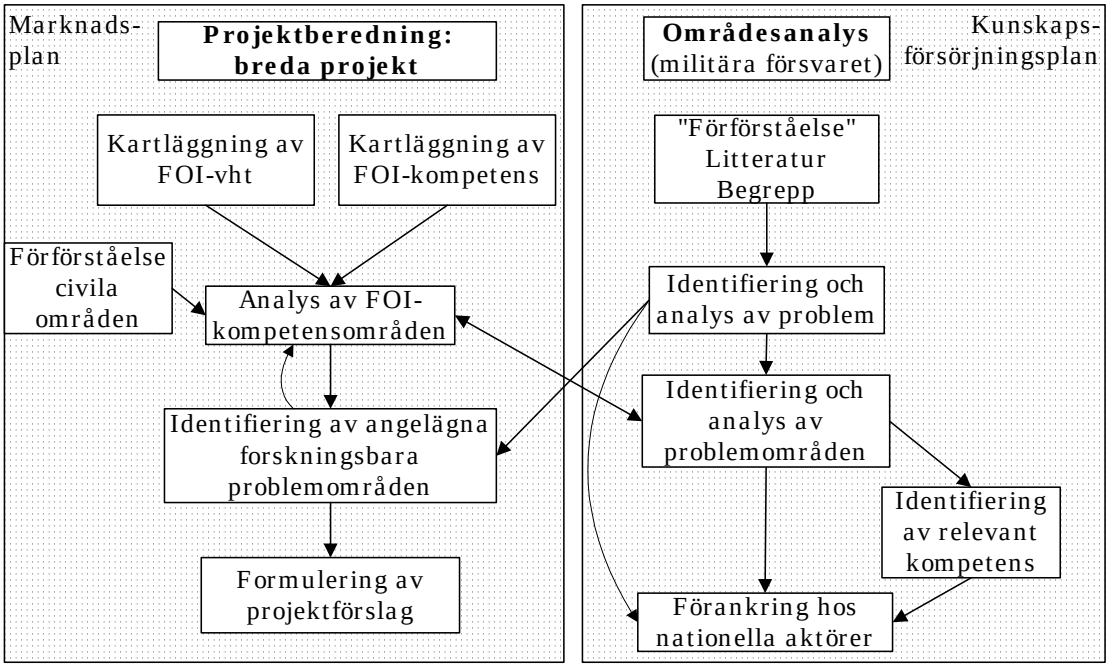
Arbetet har genomförts på FOI inom ramen för projektet IT-försvar. Detta projekt består av två huvuddelar:

- En områdesanalys, vilken har resulterat i denna rapport.
- En projektberedning för breda projekt, vilken genom att klargöra FOIs verksamhet och kompetens samt föreslå nya projekt ger förutsättningarna för en bred satsning inom området IT-försvar.

I arbetet med områdesanalysen har representanter från avdelningarna Försvarsanalys, Systemteknik och Ledningssystem deltagit. Ett arbetsinternat genomfördes 14 - 15 augusti 2001 i Nyköping med deltagare från FOI enligt följande: E Anders Eriksson, Viiveke Fåk, Jonas Hallberg, Amund Hunstad, Eva Mittermaier, Leif Månsson och Sören Palmgren. Ett uppföljningsmöte hölls i Linköping 25 september 2001 med deltagare från FOI enligt följande: E Anders Eriksson, Viiveke Fåk, Jonas Hallberg, Amund Hunstad, Eva Mittermaier och Sten-Åke Nilsson. Kommentarer på en preliminär version av promemorian har inkommit från Mats Ohlin, FMV; Ingvar Ståhl, FM; Erland Jonsson, Chalmers; och Simone Fischer-Hübner, Karlstads universitet.

Arbetsområden för områdesanalysen och relationen till projektberedningen illustreras av Figur 1 nedan. Figuren ger också en översiktlig struktur för denna rapport. Kapitel 2 *Begreppsdefinitioner* redogör för den terminologi som används i detta dokument. Terminologin relateras till allmän informationssäkerhets- och IT-säkerhetsterminologi, men även till övrig aktuell terminologi inom området. I kapitel 3 *Pro-*

blemområden redogörs för resultatet av identifieringen och analysen av problem och problemområden. Kapitel 4 *Nationell kompetens relativt problemområden* innehåller en redovisning av nationella aktörer inom respektive problemområde samt en kortfattad analys av samlad befintlig kompetens inom IT-försvarsområdet. Kapitel 5 *Underlag till program för området IT-försvar* innehåller slutsatser och rekommendationer för inriktningen på den forskning som ska ligga till grund för framtidens IT-försvar.



Figur 1: Arbetsområden för områdesanalysen gällande IT-försvar.

1.2 Problemområdet

Sårbarhets- och säkerhetsutredningen[1] fastslår att även om sannolikheten[2] för ett avancerat IT-angrepp mot Sverige är svår att uppskatta kan konsekvenserna bli så allvarliga att problemet i högsta grad måste beaktas. Detta är egentligen tillräckligt för att motivera behovet av ett effektivt IT-försvar. Liksom ett starkt konventionellt försvar kan verka krigsavhållande kan man tänka sig att ett svagt IT-försvar gör ett avancerat IT-angrepp betydligt mer troligt än ett väl utvecklat. De faktorer som behöver beaktas vid värdering av hot är:

- Den tekniska svårighetsgraden att genomföra ett visst angrepp.

[1] Sårbarhets- och säkerhetsutredningen, *Säkerhet i en ny tid*, SOU 2001:41, maj 2001.

[2] Begreppet *sannolikhet* används i denna rapports resonemang i en relativt vid och intuitiv mening. Detta kan anses begränsa den strikt vetenskapliga precisionen i begreppet, ty rörande intentionella hot, som till exempel ett avancerat IT-angrepp, har strikt sannolikhetsresonemang vissa svagheter. I sådana sammanhang kan man argumentera för att introducera begrepp som *trolighet* som alternativ till sannolikhet. Det bör då dock beaktas att Nationalencyklopedins ordbok i sin definition av sannolikhet (i matematiska sammanhang) beskriver sannolikhet som *”grad av trolighet”*. För att bibehålla argumentationsmässig enkelhet och för att undvika att införa likartade begrepp med förväxlingsrisk, används därmed sannolikhet som ett samlande begrepp.

- Sannolikheten att någon aktör, i besittning av tillräcklig förmåga att överkomma svårigheterna, skulle vara intresserad att genomföra angreppet.
- Konsekvenserna av angreppet ifråga.

Ovanstående diskussion kan i princip även tillämpas på företag som bedriver elektronisk handel på Internet. Några förhållanden gör ändå att marknadens incitament inte utan vidare räcker till för att få till stånd ett väl underbyggt IT-försvar snarare än ad hoc-mässiga säkerhetslösningar vartefter behoven uppstår:

- Det råder brist på jämförbarhet och transparens när det gäller kommersiella IT-lösningars säkerhetsnivå. Därigenom finns svårigheter att ta ut en premie för hög kvalitet i detta avseende.
- Användning av de facto-standarder gör att många av de hot och risker som kan drabba ett företag troligen också drabbar konkurrenterna. Hot och risker av detta slag kan vara mindre allvarliga för det enskilda företaget än för samhället i stort eftersom hotet mot den relativa konkurrenspositionen – och därmed företagets överlevnad – inte är så allvarligt.
- Ett aktiebolags förmåga att bära hot och risker begränsas av dess aktiekapital. Det blir därigenom indifferent mellan ett utfall som precis leder till att företaget går i konkurs efter att ha täckt alla uppkomna skador, och ett där mycket mer omfattande samhälleliga skador uppkommer.

Det är i princip dessa tre faktorer som utgör underlaget inför ett offentligt åtagande inom IT-säkerhet (utöver sådana åtaganden när det gäller rättsväsen, utbildning, forskning etc. som gäller för alla samhällssektorer). Härtill kommer de behov staten har som ägare av IT-system. Inte minst gäller detta försvaret, den sektor som står i fokus för föreliggande rapport.

Hittills har Försvarsmakten hanterat IT-relaterade hot och risker genom att kompensera de allvarliga konsekvenserna med separation av system och därmed minskad sannolikhet för IT-angrepp. För *Det nya försvaret* blir dock bilden annorlunda. Nämligen en organisation vars verksamhet är starkt beroende av distribuerade informationssystem, vilka exponeras för de risker det medför att vara ansluten till publika nät, och utgör ett attraktivt mål, speciellt i händelse av kris eller krig. Därmed uppstår risker med såväl hög sannolikhet som allvarliga konsekvenser, om inte ett effektivt aktivt IT-försvar byggs upp för att hantera dessa risker.

Det är mycket svårt att förutsäga de möjliga konsekvenserna av ett avancerat IT-angrepp, men följande scenarion måste anses vara realistiska vid avsaknad av ett aktivt IT-försvar.

- Belastningsattacker via kopplingar till externa nät, eller från i förväg preparerade datorer i det egna systemet, medför att tillgängligheten kan begränsas kraftigt under en längre tid innan åtgärder vidtagits. Detta skulle kunna medföra produktions- eller försäljningsbortfall för ett företag. För ett högteknologiskt militärt försvar involverat i skarpa operationer skulle det vara förödande.
- Infekterade datorer i ett ledningssystem blockerar, manipulerar eller förstör sensordata som överförs i systemet, vilket försämrar eller förvränger verklighetsbilden för systemets operatörer. Detta kan leda till felaktiga beslut i kritiska lägen.

- Underrättelseinhämtning genom dolda system- och programfunktioner, vilka vidarebefordrar känslig information.

Ett IT-försvar minskar, liksom ett konventionellt försvar, både sannolikheten för och konsekvenserna av ett angrepp. Detta kan delas upp i ett antal faktorer:

- Sannolikheten för ett angrepp minskar.
- Sannolikheten för att ett angripet system överhuvudtaget påverkas minskar.
- Tiden till upptäckt av angrepp minskar.
- Tiden innan motåtgärder sätts in minskar.
- Sannolikheten för att motåtgärderna får avsedd effekt ökar.

2. Begreppsdefinitioner

Detta kapitel redovisar allmän informationssäkerhets- och IT-säkerhetsterminologi, för att därefter i relation till detta och IT-hot diskutera begreppet IT-försvar. Slutligen relateras begreppet IT-försvar till övrig aktuell terminologi inom området, speciellt amerikansk sådan terminologi.

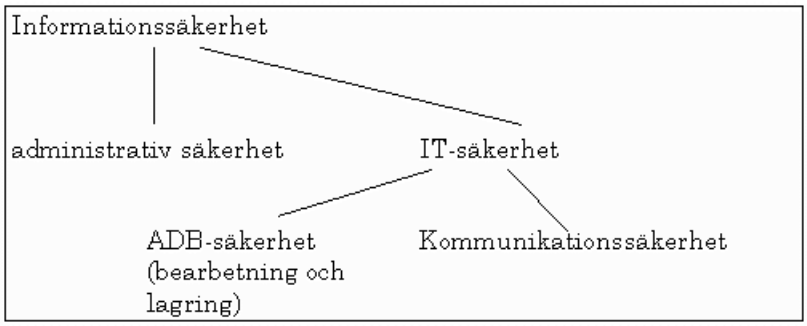
2.1 Informationssäkerhet och IT-säkerhet

Informationssäkerhet består i att bevara någon eller flera av egenskaperna sekretess, tillförlitlighet och tillgänglighet för information, vilken på något sätt är kritisk för en given verksamhet.

IT-säkerhet består i att bevara någon eller flera av egenskaperna sekretess, tillförlitlighet och tillgänglighet för information och tjänster som hanteras respektive tillhandahålls av distribuerade system.

Administrativ säkerhet rör rutiner och information vilken inte är en del av informationssystemet men påverkar dess säkerhet, såsom behörighetsadministration med mera.

Informationstekniska standardiseringen i Sverige, ITS, definierar informationssäkerhet som bestående av administrativ säkerhet och IT-säkerhet. IT-säkerhet, i sin tur, delas upp i ADB-säkerhet och kommunikationssäkerhet. Detta illustreras av Figur 2 från rapporten ITS 6[3], vilken innehåller definitioner av de olika begreppen. Det kan noteras att termen ADB-säkerhet är synonym med datasäkerhet. Denna uppdelning har anammats av Sårbarhets- och säkerhetsutredningen[4].



Figur 2: Uppdelning av informationssäkerhet (ITS, 1994).

Det finns ett starkt beroende mellan IT-säkerhet och administrativ säkerhet. Detta medför att båda dessa områden måste beaktas för att få en heltäckande bild av problematiken, dvs graden av säkerhet i distribuerade informationssystem. Däremot täck-

[3] ITS, Informationstekniska standardiseringen i Sverige, *Terminologi för Informationssäkerhet, Rapport ITS 6*, mars 1994.

[4] Sårbarhets- och säkerhetsutredningen, *Säkerhet i en ny tid*, SOU 2001:41, maj 2001.

er de inte aspekter gällande information som inte hanteras med eller berör distribuerade informationssystem, vilka dock torde vara en del av informationssäkerheten.

I fortsättningen av denna rapport kommer IT-säkerhet i en vidare bemärkelse, vilken inkluderar administrativ säkerhet, att behandlas. Denna vidare användning av begreppet IT-säkerhet exkluderar dock de delar av informationssäkerheten som inte berör distribuerade informationssystem.

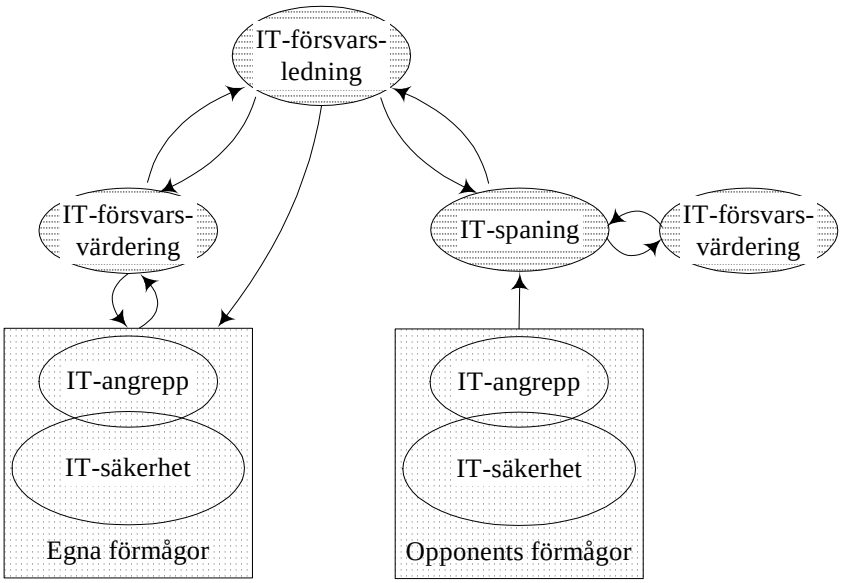
2.2 IT-försvar

Traditionellt har man tänkt sig IT-säkerhet som ett huvudsakligen passivt försvar. Särskilt i förhållande till kvalificerade angripare med möjlighet till omfattande förberedelser betraktas dock idag tanken på ett fullgott passivt försvar som allt mindre realistisk. Därför måste även aktiva komponenter beaktas. Ett aktivt IT-försvar brukar delas upp i förmågorna att skydda, upptäcka och reagera (SUR). En till SUR-tanken relaterad förändring är att medan man tidigare försökte eliminera risker, ser man det idag som oundvikligt att ta risker och strävar efter att göra detta på ett välavvägt sätt.

I föreliggande analys kommer vi inte att använda uppdelningen skydda, upptäcka och reagera, men väl en annan som kan relateras till denna nämligen förmågorna IT-angrepp, IT-säkerhet och IT-spaning. Syftet med denna indelning är att skilja på förmågor som gäller det egna systemet respektive riktas mot andra system. Förmågan IT-säkerhet innefattar de delar av förmågorna skydda, upptäcka och reagera som är begränsade till det egna systemet. De delar av förmågan upptäcka som baseras på kunskap om andra system ingår i IT-spaning och de delar av förmågan reagera som riktas mot andra system ingår i IT-angrepp. IT-spaning och IT-angrepp kan också användas för strategiska operationer vilka syftar till att i förväg kartlägga alternativt begränsa en opponents förmågor.

För att möjliggöra ett effektivt IT-försvar som dessutom är koordinerat med andra försvarskomponenter måste en ledningsförmåga finnas. Dessutom behövs en förmåga till värdering, IT-försvarsvärdering, vilket framträder som en väsentlig och komplex förmåga. Den inbegriper nivåer på IT-säkerhets-, IT-angrepps- och IT-spaningsförmågor, i såväl egna som andras nuvarande och framtida system, samt möjliga effekter på system och omgivning. Värderingsresultaten är av stor vikt för alla de andra IT-försvarsförmågorna.

De resulterande fem förmågorna IT-angrepp, IT-säkerhet, IT-spaning, IT-försvarsledning och IT-försvarsvärdering samt möjliga relationer mellan dem illustreras av Figur 3 nedan.



Figur 3: Förmågor och relationer mellan dessa.

Figur 3 illustrerar beroendet mellan förmågorna samt behovet av att behärska ett flertal för att kunna vara effektiv inom någon av dem. Exempelvis kräver effektiv IT-spaning stor kunskap om IT-angrepp och framförallt IT-säkerhet, samt förtroende med tillgängliga värderingsmetoder.

Utgående från Figur 3, beaktande både direkta och indirekta relationer mellan förmågorna samt en sammanföring av egna och andras förmågor, framträder överlapp och ömsesidiga beroenden mellan alla förmågorna. Dessutom måste ett IT-försvar vara en del av en övergripande informationsstrategi för den aktuella organisationen.

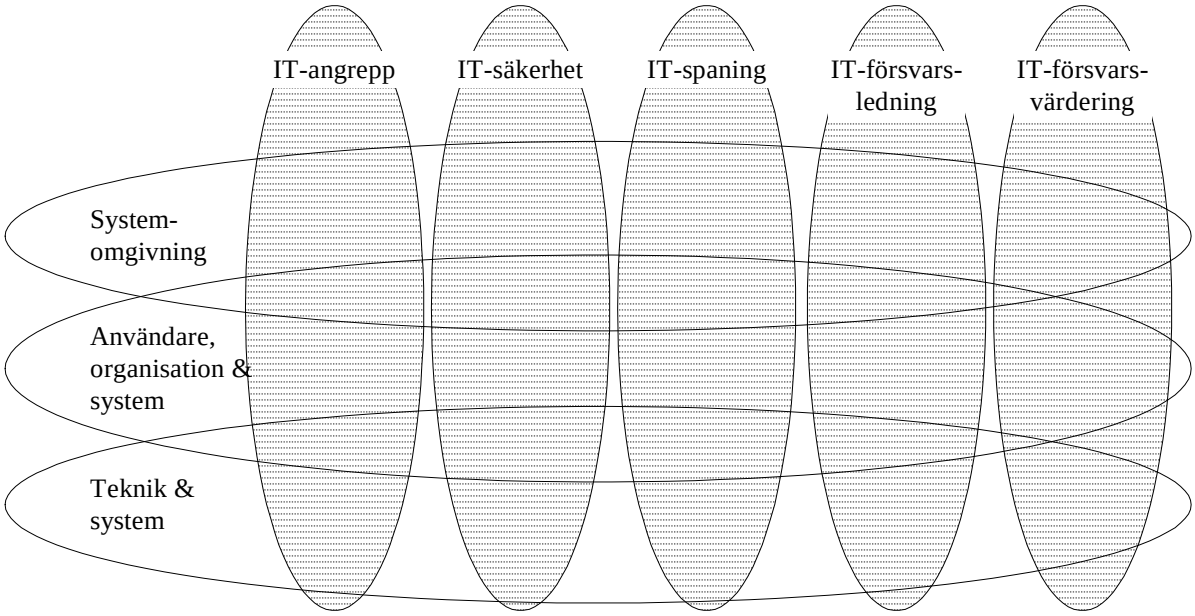
Det faller sig naturligt att prioriteringen och utformningen av de olika IT-försvarsförmågorna är organisationsberoende. En klar skiljelinje kan tyckas finnas mellan dem som har som ambition att utnyttja de offensiva förmågorna strategiskt och dem som endast är intresserade av att försvara sig mot IT-hot. Likt ett konventionellt militärt försvar kräver dock ett IT-försvar offensiva förmågor. Därmed finns det ett behov av kunskap inom detta område för alla organisationer.

Som vi ovan avgränsat begreppet IT-försvar bedrivs det med IT-baserade förmågor, vilket inkluderar administrativa rutiner rörande distribuerade informationssystem. Däremot exkluderas exempelvis fysiska medel och motmedel, påverkan med elektromagnetisk strålning samt registrering av röjande strålning.

Var och en av IT-försvarsförmågorna innehåller ett stort antal frågeställningar. Dessa frågeställningar är av starkt varierande karaktär, gällande till exempel teknik, organisation eller policy. Ett sätt att kategorisera frågeställningarna är att studera dem ur de tre aspekterna *Systemomgivning*, *Användare, organisation & system* samt *Teknik & system*. *Teknik & system* berör tekniska frågeställningar för det aktuella systemet. *Användare, organisation & system* inkorporerar frågor gällande samspelet mellan människor och det tekniska systemet. Då de distribuerade informationssystemen blir allt mer omfattande och behoven av att anpassa de tekniska systemen och organisationerna till varandra allt tydligare, kommer denna aspekt att beröra en stor del av den eller de organisationer som använder systemet. *Systemomgivning* innehåller frågor rörande

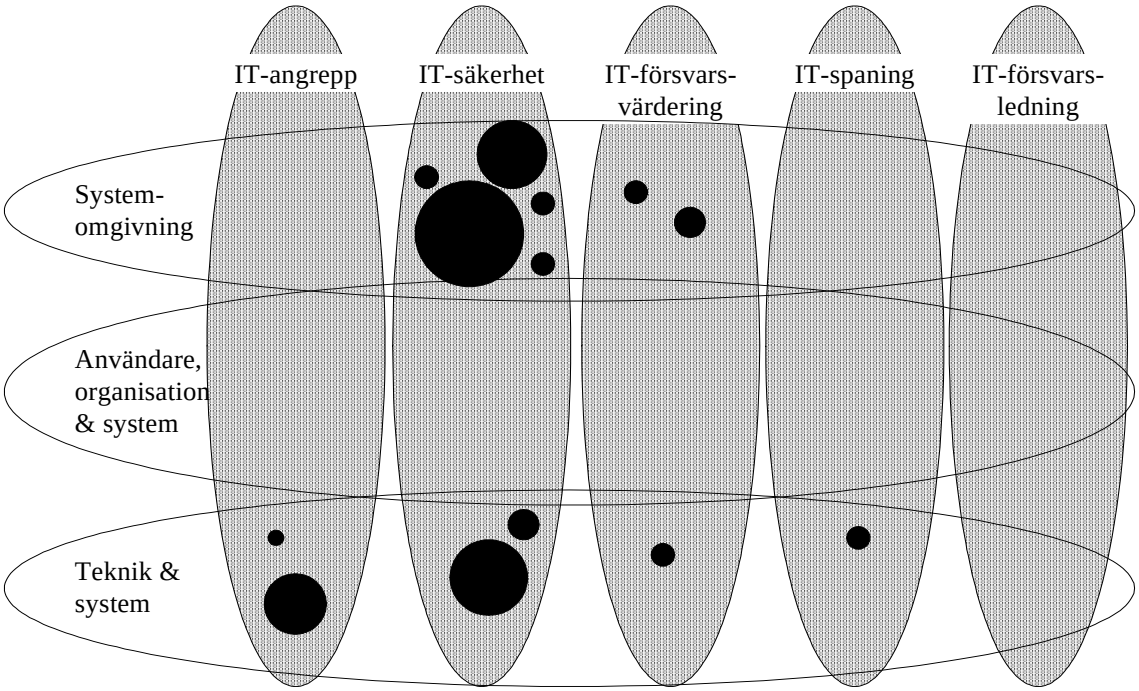
interaktionen mellan systemet i en vid bemärkelse, dvs inklusive användare och organisation, och det omgivande samhället. Exempelvis innehåller ett beaktande av användarautenticering frågor rörande teknik (användning av lösenord, aktiva kort eller biometri, lagring av verifieringsdata, etc.), användare och organisation (rimliga krav på och acceptans hos användare, administration av autenticeringssystemet, etc.) och omgivning (lagar och förordningar, allmän acceptans i samhället, etc.). En indelning av IT-försvarsfrågor i olika aspekter kan aldrig bli helt entydig utan resulterar i både överlapp och beroenden.

För att få med både förmågorna och aspekterna i en figur förenklas bilden genom att överlappen mellan förmågorna samt mellan aspekterna *Systemomgivning* och *Teknik & system* tas bort. Resultatet blir en matrisliknande bild, se Figur 4, vilken kan användas för att kategorisera verksamhet och kompetens.



Figur 4: Aspekter och förmågor gällande IT-försvar.

Figur 5 nedan innehåller en kategorisering av de FOI-projekt som bedrevs under 2001. Projekten representeras av en cirkel vars area är proportionell mot budgeten. Den totala omsättningen var ungefär 20 MSEK och största finansiär var ÖCB som stod för 8,7 MSEK. Figuren visar inom vilka förmågor och aspekter som projekten genererar ny kunskap. Om figuren istället skulle visa vilka förmågor och aspekter genomförandet av projekten kräver kunskap inom, skulle cirklarna täcka betydligt fler förmågor och aspekter.



Figur 5: FOI-projekt inom IT-försvarsområdet under 2001.

2.3 IT-hot

Som berörts ovan är förståelse för avancerade hot centralt för ett kompetent IT-försvar. Klassiska hot- och riskresonemang används dock i rapportens vidare resonemang i begränsad grad. Istället utgår rapportens vidare diskussion i huvudsak från terminologi i enlighet med avsnittet 2.2 IT-försvar. Nedan förs en kort argumentation för detta.

Hot kan utgöras av subjekt, men också bestå av händelser. Därmed blir de tätt förknippade med brister. Hotens vikt beror också på den potentiella skadan. I en riskanalys intar begreppet hot en central roll. I kapitel 1 diskuterades risker som en sammanvägning av sannolikheten för och konsekvensen av en händelse. Händelsen består då av kombinationen av ett eller flera hot och brister, vilket resulterar i ett antal kedjor av hot, brister och skador.

Ur ett operativt perspektiv ter det sig naturligt att analysera en situation utifrån relevanta risker. Därmed framträder aktiviteter såsom hot-, sårbarhets- och konsekvensanalys.

Inom forskning och utveckling blir dock perspektivet annorlunda. Forskning och utveckling syftar till kunskap, metoder och verktyg vilka förbättrar förutsättningarna för, förmågan till och resultaten från hot-, sårbarhets- och konsekvensanalyserna. Forskning och utveckling i sig beskrivs bättre med de förmågor och aspekter som introducerats tidigare i detta kapitel, istället för det operativa perspektiv som riskanalysen rör sig inom.

2.4 Avgränsning och relation till andra begrepp

IT-relaterade hot har på senare år fått stor uppmärksamhet i försvarsdebatten. Många begrepp har i detta sammanhang myntats såsom informationskrigföring (Information Warfare, IW), informationsoperationer (Information Operations, IO), informationssäkring (Information Assurance, IA) och Computer Network Attack, Defense och Operations (CNA, CND resp. CNO). Bilaga 1 redovisar ytterligare terminologidetaljer.

Informationsoperationer, IO, och informationskrigföring är vida begrepp vilka inkluderar allt som har med informationssäkerhet, både avseende skydd och strategiskt utnyttjande eller påverkan av, att göra. IT-försvar är däremot begränsat till information som lagras i, bearbetas med eller överförs med hjälp av distribuerade informationssystem. Informationssäkring (eng. information assurance, IA) är en beteckning för den defensiva delen av informationsoperationer och innefattar därmed andra områden än IT-försvar.

CNO betecknar den del av IO som bedrivs via nätverk, vilket i princip jämställer det med IT-försvar. Av de fem förmågorna som ingår i IT-försvar så inkluderar CNO IT-angrepp, IT-säkerhet, IT-spaning och IT-försvarsledning, förmågan IT-försvarsvärdering ingår dock inte. Därmed ligger begreppet CNO nära begreppet IT-försvar som det används i denna rapport. IT-försvar ska alltså ses som en verksamhet på taktisk nivå som operativt kan samverka med andra typer av stridskrafter för att uppnå olika typer av mål.

3. Problemområden

Ett antal för IT-försvar relevanta problemområden har identifierats. Varje problemområde spänner över flera aspekter och förmågor relaterade till IT-försvar. Därigenom indikeras möjligheter för tvärvetenskapliga studier inom respektive problemområde. Detta är en utmärkt utgångspunkt, ty för att uppnå tillfredsställande IT-säkerhet är kunskapsinhämtning på tvärs av vetenskapliga domäner nödvändig.

De identifierade problemområdena är de som bedöms vara av störst relevans för utvecklingen av ett IT-försvar. Andra identifierade områden kan tänkas existera, men de bedöms vara av mera begränsad relevans. Man kan även tänka sig att modellera IT-försvarsområdet utgående från en annan mängd problemområden, utan att det nödvändigtvis behöver vara någon sämre eller bättre modell. Det kan enkelt nog vara - en annan modell.

Problemområdena har identifierats inom ramen av ett arbetsseminarium, där först ett antal frågeställningar inom området detekterats. Dessa har samlats under de nedan listade problemområdena, som var för sig bedöms ha en forskningsmässig potential.

De flesta problemområden spänner, med avseende på kunskapsbehov, över alla IT-försvarsaspekter och ett antal IT-försvarsförmågor. Om inget annat framgår av kommentar för respektive problemområde, gäller att problemområdet kunskapsmässigt spänner över alla aspekter och alla förmågor. Om istället de kombinationer av aspekter och förmågor där forskning inom problemorådet kan producera ny kunskap beaktas, blir bilden en annan. Till exempel spänner problemområdet Offensiva metoder och tekniker över alla aspekter och alla förmågor. Producerad kunskap ligger dock inom förmågorna IT-angrepp och IT-spaning. I avsnitt 3.8 har problemområdena placerats in i aspekt-förmågestrukturen formulerad i kapitel 2 utgående från möjlig kunskapsproduktion.

3.1 Arkitektur

För distribuerade informationssystem är arkitekturen, eller strukturen, avgörande för vilken säkerhetsnivå som kan uppnås operativt. Ett systems arkitektur påverkar inte bara den defensiva säkerheten utan alla de fem IT-försvarsförmågorna. Ett systems arkitektur, eller åtminstone ramarna för arkitekturen, fastläggs relativt tidigt under designen av systemet. Därför är det av yttersta vikt att säkerheten beaktas från första stund genom design av en säkerhetsarkitektur. Området spänner över alla aspekter och förmågor. Fokus är på frågeställningar som:

- På vilket sätt man bygger upp ett IT-systems arkitektur för att bidra till en hög IT-säkerhet?
- Val mellan centraliserade hierarkiska system kontra decentraliserade och plattare arkitekturer.
- Att förstå komplexiteten i system av system.

Forskning inom området är i allmänhet fokuserad på delfrågor med relevans för arkitekturområdet som helhet. En medveten och bredare satsning på arkitektur vore av stort värde för vidare utveckling av IT-försvarsområdet.

3.2 Samhällsaspekter på IT-försvar

Ett tydligt exempel på yttre påverkan är de lagar vilka reglerar hur ett informationssystem kan utformas och med vilka medel dess säkerhet kan försvaras. Att utifrån gällande lagstiftning bestämma vad som är legalt för ett IT-försvar är en komplicerad process. Omvänt gäller att juridiken behöver influeras av IT-försvarsfrågor, då en viss eftersläpning relativt den tekniska utvecklingen kan observeras.

Utöver juridiska aspekter på IT-försvar är det även nödvändigt att beakta andra samhällsmässiga avvägningar, som till exempel vilket offentligt åtagande som kan vara aktuellt och relevant. Samarbetsformer mellan offentlig och privat sektor är också aktuellt att eftersträva och studera. Omvärldsbevakning, exempelvis med avseende på aktivistgrupper och IT-hot, är exempel där internationella studier och samarbete är värdefullt. I många sammanhang rörande samhällsaspekter och avvägningar inom IT-försvarsområdet, blir frågeställningar kring begrepp som förtroende centrala.

Området spänner över alla aspekter och förmågor. Förmågemässigt kan en tyngdpunkt till förmågorna IT-angrepp och IT-spaning noteras. Fokus är på frågeställningar som:

- Vilka medel kan tillgripas vid IT-angrepp och IT-spaning och hur påverkas detta av yttre omständigheter, såsom det säkerhetspolitiska läget?
- Hur kan lagstiftningen förändras för att förbättra förutsättningarna för ett IT-försvar?
- Internationellt samarbete: Med vem avser vi samarbeta och hur realiserar vi samarbetet?

3.3 IT-säkerhetspolicy

En adekvat IT-säkerhetspolicy är en grundförutsättning för ett fungerande IT-försvar. Den måste beakta frågor rörande omgivning, användare och organisation samt teknik. Tyngdpunkten inom detta område är förmågemässigt på IT-försvarsledning och IT-försvarsvärdering och aspektmässigt på Systemomgivning, men övriga förmågor och aspekter är av vikt att inkorporera i all analys av policyfrågor. Fokus är på frågeställningar som

- Hur påverkar en IT-säkerhetspolicy användarnas, organisationens och omgivningens tilltro till ett informationssystem?
- Informationsstrategi och IT-säkerhet
- Utbildning av användare, speciellt i syfte att göra dem medvetna om IT-säkerhetsavvägningar.
- Koalitioner: Hur realiserar man policysamverkan i koalitioner av olika aktörer och system så att de fungerar på ett adekvat sätt?

Det finns en betydande omfattning på verksamheten inom området, men den bedöms inte vara sammanhållen på ett sätt som till fullo gynnar utvecklingen av IT-försvarsområdet.

3.4 Defensiva metoder och tekniker

Defensiva metoder och tekniker utgör grundstenar inom IT-säkerhetsförmågan och byggstenar för en säkerhetsarkitektur. Området är på inget sätt begränsat till aspekten Teknik & system, men tyngdpunkten ligger där. Fokus är på frågeställningar som:

- Autenticering
- Delegering av rättigheter
- PKI (eng. Public Key Infrastructure)
- Intrångsdetektering
- Brandväggar
- Spårbarhet

Forskningen inom detta område har en relativt lång historia och har därigenom nått en betydande mognad.

3.5 Offensiva metoder och tekniker

Liksom defensiva metoder och tekniker utgör grundstenar inom IT-säkerhetsförmågan, utgör offensiva metoder och tekniker grundstenar inom förmågorna IT-angrepp och IT-spaning. Vidare ligger tyngdpunkten också inom detta område på aspekten Teknik & system. Fokus är på frågeställningar som

- IT-vapen
- IT-spaning
- Effekter på offensiva metoder och tekniker av doktrin och taktik

Forskning inom problemområdet är begränsad. Dock kan det observeras att en betydande del av defensiv forskning har en självklar relevans för offensiva metoder, och som redan noterats finns en tydlig forskningsmässig mognad för defensiva metoder och teknik.

3.6 Analys och värdering

Det finns ett fundamentalt behov av adekvata tekniker för analys och värdering av IT-försvarsförmågor, premisser givna av systemomgivningen och hotbild. Utan en IT-försvarsvärderingsförmåga går det inte att bedöma säkerhetsnivån i ett system, vinster med investeringar i säkerhetsförbättringar eller risker behäftade med systemmodifieringar. Fokus är på frågeställningar som:

- Hotagentanalys[5]
- Angriparidentifiering

[5] Analys av vilka aktörer som står bakom hoten.

- Val av reaktion
- Ledningsstöd
- Systemvärdering
- Taktisk och operativ värdering

De aktuella frågeställningarna är mycket komplexa och det finns ett stort behov av både grundläggande forskning och tillämpad metodutveckling inom detta problemområde.

3.7 Realtidshantering av angrepp

Problemområdet realtidshantering av angrepp är centralt då tidsfaktorn är av avgörande betydelse för ett IT-försvar. Detta medför att automatiserade stödfunktioner är väsentliga och därmed ett stort behov av forskning och utveckling. Det bör noteras att området är beroende av resultat från övriga problemområden. Implementerade lösningar är nödvändiga för försvaret i längden. Fokus är på frågeställningar som:

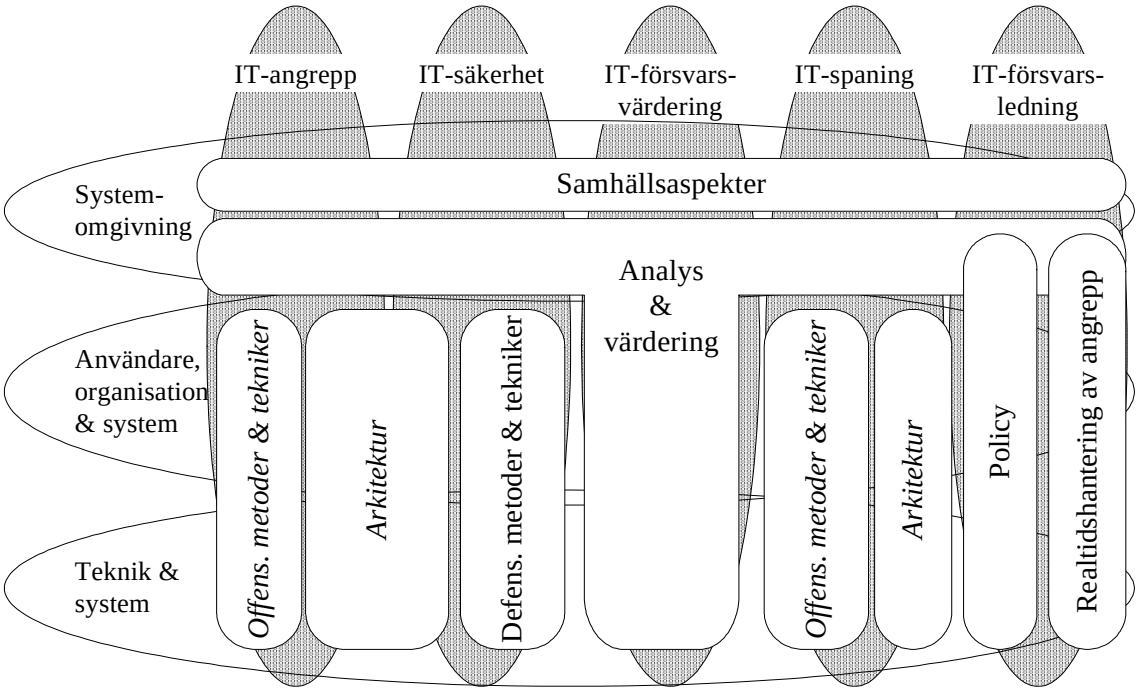
- Upptäckt och analys av angrepp
- Automatiskt beslutsfattande
- Lägesbild

Omfattande forskning på relaterade delproblem, som exempelvis beslutsfattande, inom andra områden gör att problemområdet har en åtminstone partiell forskningsmognad. Däremot är forskningsmognaden svagare inom andra delproblem, såsom upptäckt och analys av angrepp. Dessutom torde, på liknande sätt som för problemområdet arkitektur, en medveten och bredare satsning på realtidshantering av angrepp vara av stort värde för vidare utveckling på IT-försvarsområdet.

3.8 Problemområdena i aspekt-förmågestrukturen

I Figur 6 nedan har de identifierade problemområdena placerats in i aspekt-förmågestrukturen. Varje problemområde spänner över flera aspekter och förmågor relaterade till IT-försvar. Därigenom indikeras behovet av tvärvetenskapliga studier inom respektive problemområde.

Figur 6 visar inom vilka förmågor och aspekter som de olika problemområdena kan generera ny kunskap. Om figuren istället skulle visa vilka förmågor och aspekter de kräver kunskap inom, skulle i stort sett alla problemområdena täcka alla förmågor och aspekter.



Figur 6: Problemområdena infogade i aspekt-förmågestrukturen (kursiv stil används för namnen på de problemområden som har flera markeringar i figuren).

4. Nationell kompetens relativt problemområden

Givet de problemområden som specificerades i kapitel 3, innehåller detta kapitel en sammanställning av nationella aktörer inom respektive område. Sammanställningen har en forskningsmässig[6] tyngdpunkt och med nationella aktörer avses här organisationer. Där kompetens är mera bunden till individer är detta inte specificerat. Det ligger i sakens natur att en kompetenskartläggning är inexakt och att det inte går att fullt rättvisande infoga kompetenser i en sådan indelning som vi har försökt oss på.

FOI och FMV är de aktörer som enligt denna kartläggning är aktiva inom flest problemområden. Om man däremot bildar ett kluster av alla högskolor och universitet har även dessa en liknande bredd på sin kompetens, bortsett från inom offensiva metoder och tekniker. Med tanke på att ett nätverk redan existerar mellan högskolornas forskning inom IT-säkerhetsområdet, kan man observera att det här existerar en intressant potential att nyttja. Resterande aktörer har sin IT-försvarsrelevanta kompetens koncentrerad till ett eller några få problemområden.

Att aktörer inom totalförsvaret har bäst täckande kompetens inom IT-försvarsområdet, speglar i all huvudsak inget annat än att försvarsfrågor har en hemvist inom totalförsvaret. Vad som är av värde att notera är att det finns viktig kompetens inom alla områden, bortsett från inom offensiva metoder och tekniker, även hos aktörer utom totalförsvaret. Med sina vinklingar av de aktuella problemställningarna kan dessa på ett värdefullt sätt komplettera totalförsvarets IT-försvarskompetens.

Nedan kommenteras den nationella kompetensen inom vart och ett av problemområdena kort. Därefter sammanfattas i Tabell 1 olika aktörer och vilka av problemområdena de är aktiva inom.

Arkitektur: Omfattningen av den nationella kompetensen inom området råder det viss osäkerhet omkring. Det kan dock konstateras att ett tydligt behov av vidare utveckling existerar. Detta bottnar i att det hittills har varit en tydligare viktläggning på defensiva metoder och tekniker än på arkitektur, vilket resulterar i mer fokus på detaljer än på helhet.

Samhällsmässiga aspekter på IT-försvar: Ett tydligt intresse inom juridiken för IT-juridiska frågor kan observeras. Rörande övriga samhällsmässiga aspekter kan man observera att det finns en bred kunskapsbas hos många aktörer, men att verksamheten relevant för IT-försvar är liten och präglad av begränsad samverkan.

IT-säkerhetspolicy: Verksamheten och kompetensen inom detta område är delvis splittrad på en skala från tydligt tillämpningsnära kompetens till mera tekniskt orienterade detaljstudier.

Defensiva metoder och tekniker: Framför allt inom aspekten Teknik & system finns det betydande kompetens och verksamhet. Denna är dock inte heltäckande eller sammanhållen. Ett aktivt nätverk mellan forskare vid universitet och högskolor finns

[6] Med forskningsmässigt avses här verksamhet som genererar ny kunskap. Därmed ingår även en del ej akademiskt orienterad forskning.

dock. Ett nationellt program skulle mer effektivt kunna nyttja den spridda men betydande kompetensen inom området.

Offensiva metoder och tekniker: Den nationella kompetensen är koncentrerad till myndighetssidan. För närvarande är den varken heltäckande eller sammanhållen. De aktörer som tas med här är de vilka studerar, med forskningsmässig inriktning, offensiva metoder och tekniker för strategiskt utnyttjande av säkerhetsbrister.

Analys och värdering: Med avgränsning enligt avsnitt 3.6 är kompetens inom området i huvudsak koncentrerad till totalförsvaret.

Realtidshantering av angrepp: Den nationella kompetensen inom problemområdet är fördelad på flera instanser. Forskningen är begränsad och uppdelad på några av de delproblem som finns inom området.

Tabell 1: Nationella aktörer relaterade till problemområden. Använda förkortningar förklaras efter tabellen.

	Arkitektur	Samhälls-mässiga aspekter	IT-säkerhets-policy	Defensiva metoder och teknik	Offensiva metoder och teknik	Analys och värdering	Realtids-hantering av angrepp
FHS		√	√			√	
FMV	√		√	√	√	√	√
FOI	√	√		√	√	√	√
FRA				√	√	√	
FM [7]		√	√	√	√	√	√
ÖCB		√				√	
Chalmers	√			√		√	√
Karlstad universitet	√		√	√			
LiU		√	√	√			
LU				√			
SICS			√	√			
SU/KTH		√	√	√			
Uppsala Universitet		√					
Försvarsdepartementet		√	√			√	
Datainspektionen		√					
IT-kommissionen		√					
PTS		√					
Justitiedepartementet		√					
Polisen		√					√
Statskontoret			√				
Utrikesdepartementet		√					
Företag	√			√			√
Svenskt Näringsliv		√	√				

Förkortningar för olika aktörer

FHS: Försvarshögskolan

FMV: Försvarets materielverk

[7] Innefattar aktörerna FM, FM CERT, FM KRI LED och FM MUST.

FM: Försvarsmakten

KRI LED: Krigsförbandsledningen Ledningssystemavdelningen

MUST: Militära underrättelse- och säkerhetstjänsten

FOI: Totalförsvarets forskningsinstitut

FRA: Försvarets radioanstalt

Företag: Innefattar olika företag med kompetens inom IT-försvarsområdet, som till exempel SAAB, Ericsson, Kockums och Sectra

LiU: Linköpings universitet

LU: Lunds universitet

PTS: Post- och telestyrelsen

SICS: Swedish Institute of Computer Science

SU/KTH: Stockholms universitet/Kungliga tekniska högskolan

ÖCB: Överstyrelsen för civil beredskap

5. Underlag till program för området IT-försvar

Utifrån resonemanget i kapitel 1 framstår ett aktivt IT-försvar som en väsentlig del av alla distribuerade informationssystem, vilkas säkerhet är kritisk för en organisation eller samhället som helhet. För Försvarsmaktens fortsatta utveckling är det av yttersta vikt att verksamhetskritiska informationssystem har såväl proaktiva som reaktiva förmågor för att upprätthålla egenskaperna sekretess, tillförlitlighet och tillgänglighet. Detta eftersom sannolikheten för avancerade angrepp är påtaglig, speciellt i ett läge av kris eller krig, och de möjliga konsekvenserna mycket allvarliga.

I kapitel 2 föreslås användningen av tre aspekter[8] och fem förmågor[9] för att ge en struktur åt området. Denna struktur kan användas dels för att kategorisera frågeställningar, verksamhet och kompetens inom området och dels för att klargöra dess omfattning.

De problemområden som identifieras i kapitel 3 härstammar ur en process vilken identifierade problem som kräver forskningsinsatser. Genom att infoga problemområdena i strukturen erhålls en bild av deras omfång. En slutsats är att forskning inom området IT-försvar är av mycket stark tvärvetenskaplig natur. Detta illustreras av att samtliga problemområden identifierade i kapitel 3 spänner över samtliga aspekter. Då aspekterna interagerar med varandra och gränserna mellan dem är diffusa, står det klart att ett brett angreppssätt är nödvändigt för att kunna producera användbara resultat inom problemområdena. Samtidigt är dock fokusering av yttersta vikt för att kunna tillföra något nytt inom området. Därmed framstår behovet av forskningsprogram där fokusering och överblick harmoniserar. Krav på både bredd och djup (fokusering) medför att volymen blir stor, alltså måste rejäla satsningar göras för att uppnå resultat.

För att bygga upp ett effektivt IT-försvar krävs en bred och betydande satsning som involverar *alla* de problemområden som identifierades i kapitel 3. I Tabell 2 nedan kommenteras forskningsbehov, rörlighet (det vill säga hur områdets innehåll och betydelse förändras med tiden) och försvarsspecifikhet för vart och ett av problemområdena.

[8] Systemomgivning; Användare, organisation & system samt Teknik & system

[9] IT-angrepp, IT-säkerhet, IT-spaning, IT-försvarsledning och IT-försvarsvärdering

Tabell 2: Forskningsbehov, rörlighet (dvs hur områdets innehåll och betydelse förändras med tiden) och försvarsspecifikhet för problemområdena.

Problemområde	Forskningsbehov	Rörlighet	Försvarsspecifikhet
Samhällsaspekter på IT-försvar	Stort behov av forskning om hur samhället och tekniska system påverkar varandra	Stabilt. Forskningsbehovet ökar med användandet av IT.	Handlar för försvaret snarare om att beakta relevant kunskapsuppbyggnad än att initiera forskning.
IT-säkerhetspolicy	Kunskap om och metoder för framtagande, förhandlande och implementation av policy	Stabilt. Mycket stor vikt på sikt då evolutionära ledningssystem, och dynamiska koalitioner mellan sådana, ska realiseras	Innehåller specifika delar (t ex rörande koalitioner och mobilitet) annars goda förutsättningar för samverkan med andra aktörer.
Offensiva metoder och tekniker	Egen verksamhet behövs för att kunna förutse framtida utveckling.	Mycket dynamiskt. Ständigt behov av nya initiativ.	Utveckling av nya metoder är försvarsspecifik verksamhet (kunskap hos många, men inte aktiv nyutveckling).
Defensiva metoder och tekniker	Viktigt att ligga långt fram med nya metoder dels för att hantera aktuella hot och dels för att förhindra uppkomsten av nya hot.	Mycket dynamiskt. Ständigt behov av nya initiativ.	Innehåller specifika delar (t ex rörande mobilitet och krav på tillgänglighet) annars goda förutsättningar för samverkan med andra aktörer.
Realtidshantering av angrepp	Stort behov av många nya metoder för ett effektivt operativt IT-försvar.	Relativt dynamiskt. Kontinuerligt behov av nya förbättrade metoder.	De hårda tidskraven och antalet beslutsalternativ (avseende till exempel användande av offensiva metoder) är försvarsspecifika
Analys och värdering	Stort behov av många nya metoder. Kräver stor insats av grundforskning.	Dynamiskt (främst avseende värdering). Kontinuerligt behov av nya anpassade och förbättrade metoder.	Avseende tekniska komponenter finns ett allmänt intresse. Högre aggregationsnivåer är mer försvarsspecifika
Arkitektur	Nya metoder för att få med säkerhetsaspekter vid systemutveckling samt att ge förutsättningar för det operativa IT-försvaret. Kräver stor insats av grundforskning.	Relativt stabilt. Kontinuerligt behov av nya förbättrade metoder.	Specifika krav avseende offensiva och defensiva metoder samt realtidshantering av angrepp ger försvarsspecifika intressen. I övrigt finns allmänna intressen och möjligheter till samverkan.

Av intresse är naturligtvis inom vilka problemområden det är av strategisk vikt att FM finansierar forskningsverksamhet och i så fall i vilken utsträckning. Först kan det slås fast att alla områden (utom möjligen Samhällsaspekter på IT-försvar) kräver både försvarsspecifik *och* allmängiltig (dvs intressant för både FM och civila aktörer) forskning för att möjliggöra samverkan med andra forskningsproducenter. Därmed kan forskningssatsningar inte begränsas till enbart försvarsspecifika frågor. Det finns dock många forskningsproblem där samverkan med civila intressenter är möjlig, då endast området Offensiva metoder och tekniker kan anses vara helt försvarsspecifikt. Vidare krävs sammanhållna satsningar inom forskningsprogram för att skapa den vetenskap-

liga bredd som behövs för att få med de olika aspekterna på problemen. Därmed framstår det som gynnsamt för FM att verka för och medverka vid genomförandet av nationella forskningsprogram.

Problemområdena Defensiva respektive Offensiva metoder och tekniker intar en särställning på grund av sin dynamik. Det finns ett mycket starkt beroende mellan dessa två problemområden och verksamhet inom det ena åtföljs därför lämpligen av verksamhet inom det andra, varmed resurser kan styras mellan de två områdena alltefter aktuella behov. Den grundläggande betydelsen för annan verksamhet inom IT-försvarsområdet gör att det är viktigt att bygga vidare på den begränsade verksamhet som finns.

Problemområdet Analys och värdering måste byggas upp då nya metoder är absolut nödvändiga för att relaterade problem inom andra områden ska kunna lösas på ett strukturerat sätt. Behovet av grundforskning är stort och därmed ligger de färdiga metoderna en bit in i framtiden. Inom den kvalitativa delen av området kan dock medel snabbare omsättas i konkreta resultat.

Problemområdena IT-säkerhetspolicy, Arkitektur och Realtidshantering av angrepp är alla mycket viktiga för realiseringen av framtidens avancerade ledningssystem. Realtidshantering av angrepp är det mest dynamiska av dessa tre problemområden. Detta beror delvis på att det är avhängigt resultaten från de andra områdena och att förändringar där kan återspeglas i förutsättningarna för det operativa IT-försvaret. Effektiviteten hos metoderna för realtidshantering av angrepp har dock en mycket stor inverkan på den totala IT-försvarsförmågan. Därmed är behovet av tillämpad forskning inom området stort. Problemområdena IT-säkerhetspolicy och Arkitektur är mer stabila, dvs de aktuella metoderna är inte lika beroende av yttre faktorer. Däremot är de fundamentala för uppbyggnaden av stora distribuerade informationssystem. För dessa två områden är behovet av grundforskning stort och därmed ligger de färdiga metoderna en bit in i framtiden.

Utgående från ovanstående resonemang är det inte möjligt göra någon slags prioritering mellan problemområdena. Alla är viktiga. Ett första mål måste vara att få upp forskningsverksamheten till en rimlig grundnivå inom vart och ett av problemområdena. Därefter kan prioriteringar och omfördelningar göras alltefter behov och resultat.

BILAGA 1 – Urval av relevanta amerikanska begrepp och deras definitioner

Från sammanställning av Göran Kindvall, FOI Försvarsanalys.

Ur Joint Pub 1-02: Department of Defense Dictionary of Military and Associated Terms Includes US Acronyms and Abbreviations and NATO Terms (English Only), 23 March 1994 As Amended Through 1 September 2000

computer network attack--Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Electronic attack (EA) can be used against a computer, but it is not computer network attack (CNA). CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. An example of the two operations is the following: sending a code or instruction to a central processing unit that causes the computer to short out the power supply is CNA. Using an electromagnetic pulse device to destroy a computer's electronics and causing the same result is EA. Also called **CNA.** [..]

computer network defense--Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. Also called **CND.** [..]

defensive information operations--The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. [..]

information assurance--Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called **IA.** [..]

information operations--Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called **IO.** [..]

information security--Information security is the protection and defense of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called **INFOSEC.** [..]

information warfare--Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called **IW.** [..]

offensive information operations--The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decisionmakers to achieve or promote specific objectives. These capabilities and activities include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could include computer network attack. [..]

Ur Joint Pub 3-13: Joint Doctrine for Information Operations, 9 Oct 1998

Computer network attack (CNA)

Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves.

Information assurance

IO that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information operations

Actions taken to affect adversary information andinformation systems, while defending one's own information and information systems. IO require the close, continuous integration of offensive and defensive capabilities and activities, as well as effective design, integration, and interaction of C2 with intelligence support. IO are conducted through the integration of many capabilities and related activities. Major capabilities to conduct IO include, but are not limited to, OPSEC, PSYOP, military deception, EW, and physical attack/destruction, and could include CNA. IO-related activities include, but are not limited to, public affairs (PA) and civil affairs (CA) activities. There are **two major subdivisions within IO:** offensive IO and defensive IO.

Offensive IO involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers and achieve or promote specific objectives. These assigned and supporting capabilities and activities include, but are not limited to, OPSEC, military deception, PSYOP, EW, physical attack/destruction, and special information operations (SIO), and could include CNA.

Defensive IO integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive IO are conducted and assisted through information assurance (IA), OPSEC, physical security, counterdeception, counter-propaganda, counterintelligence (CI), EW, and SIO. Defensive IO ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. Offensive IO also can support defensive IO.

Information warfare

Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.