



Militärteknik i ett tjugoårigt perspektiv

Underlag till Försvarsmaktens Perspektivstudie 2017

GÖRAN KINDVALL, ÅKE WISS (RED.)

Göran Kindvall, Åke Wiss (red.)

Militärteknik i ett tjugoårigt perspektiv

Underlag till Försvarmaktens Perspektivstudie 2017

Titel	Militärteknik i ett tjugårigt perspektiv - Underlag till Försvarmaktens Perspektiv- studie 2017
Title	Military technologies with a 20 year horizon – Texts for the Swedish Defence Forces Long Term Study 2017
Rapportnr/Report no	FOI-R--4462--SE
Månad/Month	November
Utgivningsår/Year	2017
Antal sidor/Pages	89 p
ISSN	1650-1942
Kund/Customer	Försvarmakten
Forskningsområde	6. Metod- och utredningsstöd
Projektnr/Project no	E13590
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Föreliggande rapport har tagits fram inom ramen för FOI-projektet *Stöd till militärstrategisk inriktning (SMI)* och är en sammanställning av teknikområden med framtida militär relevans. Syftet med rapporten är att lämna underlag till Försvarmaktens perspektivstudie. Författarna är anställda på FOI och är antingen experter eller personer med lång erfarenhet inom respektive område.

Rapporten redovisar i kortform ett antal utvalda teknikområden som företrädare för perspektivstudien identifierade som intressanta och relevanta i ett 20-årigt tidsperspektiv. Grunden för urvalet var att tekniken *skulle kunna* vara förbandssatt inom en tjugoårsperiod.

Rapportunderlaget är framtaget främst för att kunna användas i spel och seminariediskussioner om militärteknik inom Försvarmaktens perspektivstudie under 2017.

Nyckelord: perspektivstudie, militär teknik, teknikutveckling

Summary

This report has been prepared by the FOI project Support for military strategic direction (SMI) and is a compilation of technology with future military relevance. The report aims to provide a basis for the Armed Forces long term study. The authors are employees of FOI and are either experts or has long experience in the respective field.

The report details in a short-form a number of selected technologies which has been identified as interesting and relevant in a 20-year time horizon. The basis for the selection of technologies was that it was deemed that they could be deployed within a period of twenty years.

The documentation is designed primarily to be used in games and seminars on military technology in the Armed Forces perspective study during 2017.

Keywords: long term planning, military technology, technology development

Innehållsförteckning

1	Inledning	8
1.1	Bakgrund	8
1.2	Metod	8
1.3	Läsanvisning	8
2	Om teknikutveckling	10
3	Additiv tillverkning	12
3.1	Beskrivning av området	12
3.2	Övergripande trender fram till 2035	13
3.3	Koppling till andra teknikområden och krav på dessa	15
3.4	Potentiella militära tillämpningar	15
3.5	Begränsande faktorer	17
3.6	Referenser	17
4	Cyber	19
4.1	Beskrivning av området	19
4.2	Övergripande trender fram till 2035	19
4.3	Utveckling av specifika delområden/teknologier	21
4.4	Potentiella militära tillämpningar	24
4.5	Begränsande faktorer	24
4.6	Referenser	25
5	HPM (High Power Microwave)	26
5.1	Beskrivning av området	26
5.2	Övergripande trender fram till 2035	26
5.3	Koppling till andra teknikområden och krav på dessa	28
5.4	Utveckling av specifika delområden/teknologier	28
5.5	Potentiella militära tillämpningar	29
5.6	Begränsande faktorer	30
5.7	Referenser	31
6	Hypersoniska system	33
6.1	Beskrivning av området	33
6.2	Övergripande trender fram till 2035	33
6.3	Koppling till andra teknikområden och krav på dessa	34
6.4	Utveckling av specifika delområden/teknologier	34
6.5	Potentiella militära tillämpningar	35
6.6	Begränsande faktorer	35

6.7	Referenser	36
7	Informationsteknologi	37
7.1	Beskrivning av området	37
7.2	Övergripande trender fram till 2035	37
7.3	Utveckling av specifika delområden/teknologier	39
7.4	Potentiella militära tillämpningar	41
7.5	Begränsande faktorer.....	42
7.6	Referenser	42
8	Laser	43
8.1	Beskrivning av området	43
8.2	Övergripande trender fram till 2035	43
8.3	Koppling till andra teknikområden och krav på dessa	44
8.4	Utveckling av specifika delområden/teknologier	45
8.5	Potentiella militära tillämpningar	45
8.6	Begränsande faktorer.....	45
8.7	Referenser	46
9	Obemannade/autonoma system	47
9.1	Beskrivning av området	47
9.2	Övergripande trender fram till 2035	48
9.3	Koppling till andra teknikområden och krav på dessa	50
9.4	Potentiella militära tillämpningar	50
9.5	Begränsande faktorer.....	51
9.6	Referenser	51
10	Plattformer	53
10.1	Inledning.....	53
10.2	Markplattformer	53
10.3	Sjöplattformer	55
10.4	Undervattensplattformer	59
10.5	Luftplattformer	63
11	Rymden	67
11.1	Beskrivning av området	67
11.2	Övergripande trender fram till 2035	67
11.3	Koppling till andra teknikområden och krav på dessa	69
11.4	Utveckling av specifika delområden/teknologier	70
11.5	Potentiella militära tillämpningar	72

11.6	Begränsande faktorer	73
11.7	Referenser	73
12	Signaturanpassningsteknik (SAT)	75
12.1	Beskrivning av området	75
12.2	Övergripande trender fram till 2035	75
12.3	Kopplingar till andra teknikområden.....	77
12.4	Utveckling inom specifika delområden	77
12.5	Potentiella militära tillämpningar	78
12.6	Begränsande faktorer	79
12.7	Referenser	79
13	Soldatsystemet	81
13.1	Beskrivning av området	81
13.2	Övergripande trender fram till 2035	81
13.3	Koppling till andra teknikområden och krav på dessa	82
13.4	Utveckling av specifika delområden/teknologier	82
13.5	Potentiella militära tillämpningar	85
13.6	Begränsande faktorer	85
13.7	Referenser	85
	Förkortningsordlista	86
	Bilaga 1	89

1 Inledning

1.1 Bakgrund

FOI-projektet *Stöd till militärstrategisk inriktning (SMI) 2017* har som en del av sitt uppdrag att lämna underlag till Försvarsmaktens perspektivstudie. Föreliggande rapport är en del av detta uppdrag.

Försvarsmaktens perspektivstudie studerar möjliga utvecklingar i ett tjugoårigt perspektiv. Som en del i detta arbete studeras teknikutveckling med relevans för militär förmåga.

Uppgiften från Försvarsmakten innebär att i skriftlig form redovisa en samlad och strukturerad övergripande sammanställning av utvecklingen inom ett antal teknikområden i tjugoårsperspektivet. Rapporten ger inte en heltäckande presentation av alla tänkbara tekniker eller teknikområden, utan ska ses som ett axplock.

Rapportunderlaget är framtaget främst för att kunna användas i spel och seminariediskussioner om militärteknik inom Försvarsmaktens perspektivstudie. Det användes som bakgrundsmaterial till de teknikspel som bedrevs av Perspektivstudien under februari 2017.

Författarna är anställda på FOI och är antingen experter eller personer med lång erfarenhet inom respektive område.

Rapporten redovisar i kortform ett antal utvalda teknikområden som företrädare för perspektivstudien identifierade som intressanta och relevanta i ett 20-årigt tidsperspektiv. Grunden för urvalet var att tekniken *skulle kunna* vara förbands-satt inom en tjugoårsperiod.

1.2 Metod

För att samla in underlaget identifierade redaktörerna, i några fall med hjälp av linjechefer, lämpliga författare inom respektive område på FOI.

Författarna förväntades följa en mall vid textframtagningen (se bilaga 1). De framtagna texterna redigerades. Rapporten sändes därefter ut i sin helhet till samtliga författare för kommentar. Efter att kommentarerna beaktats vidtog rapportgranskning enligt befintliga rutiner på FOI Försvarsanalys.

Ingen klustring av områden har skett. Som läsaren kommer att upptäcka finns det kopplingar mellan områdena. Dessa kopplingar har inte analyserats vidare i denna rapport.

1.3 Läsanvisning

I kapitel 2 presenteras ett övergripande resonemang om teknikutveckling. Därefter presenteras de olika teknikområdena. Vi har valt att presentera dem i bokstavsordning. I tabellen nedan framgår författare till respektive område.

Ämnesområde	Författare
Additiv tillverkning	Steven Savage
Cyber	Joel Brynielsson, Hannes Holm, Fredrik Johansson, Magnus Sparf
HPM (High Power Micro-wave)	Tomas Hurtig, Sten E Nyholm
Hypersoniska system	Erik Berglund, Martin Hagström
Informationsteknologi	Joel Brynielsson, Linus Gisslén, Tove Gustavi
Laser	Lars Sjöqvist, Göran Kindvall
Obemannat/Autonoma system	Göran Kindvall, Martin Hagström
Plattformer (mark, sjö, luft)	Tomas Mårtensson (luft), Linus Fast (yt sjö), Mats Nordin (undervatten sjö), Martin Hagström (mark)
Rymden	Daniel Faria, Sandra Lindström
Signaturanpassningsteknik (SAT)	Lars Bohman, Hans Kariis
Soldatsystemet	Göran Kindvall, Sofia Hedenstierna, John Ottosson, Thomas Eriksson

Efter genomgången av teknik följer en förkortningsordlista. Rapporten avslutas med den mall som författarna förväntades följa vid författandet av respektive kapitel.

2 Om teknikutveckling

Förmågan att förutsäga var nästa betydelsefulla tekniksteg kommer att tas bedöms som så viktig att stater och organisationer är beredda att lägga omfattande resurser på att tidigt försöka identifiera och förstå betydelsen av dessa. Detta sker exempelvis via bred avskanning och horisontspaning (*horizon scanning*) samt detaljerad värdering av identifierade områden som bedöms ha potential att utvecklas.

I USA talar man om den tredje offsetstrategin¹ för det koncept på vilket det amerikanska försvaret ska vila under de närmaste åren.² Detta bygger mycket på den snabba utveckling – tack vare kommersiella drivkrafter – som sker inom bland annat artificiell intelligens och autonoma system. Fem komponenter som lyfts fram i den tredje offsetstrategin är autonoma inlärningssystem (*deep learning*), samverkan mellan människa och maskin i beslutsfattande, förbättring av den mänskliga prestationsförmågan, avancerad samverkan mellan människa och maskin i strid (exempelvis samverkan mellan människor och obemannade system) samt semi-autonoma nätverksbaserade vapensystem hårdgjorda för att klara intensiv tele- och cyberkrigföring. Fokus är både på kort- och långsiktiga resultat och på att kombinera det nya med befintliga system.

Ett annat sätt att karakterisera teknikutvecklingen utgår från att små, smarta och billiga vapen blir allt mer tillgängliga för både stater och irreguljära aktörer.³ De teknikområden som lyfts fram är robotik, artificiell intelligens (bland annat för navigering och måligenkänning), additiv tillverkning och nanoteknologi (material och explosivämnen). Dessa områden, var för sig eller kombinerat, skapar nya hot och möjligheter.

Kombinationer av teknikutveckling inom flera områden kan komma att innebära verkligt nya omvälvande tillämpningar, genom att förstärka effekten av utvecklingen inom enskilda teknikområden eller genom att skapa helt nya effekter. Att genomföra analyser för att identifiera och förstå potentialen hos sådana kombinationer är därför viktigt. Detta ställer krav på systemförståelse, bred samverkan över teknikområdesgränserna och relevanta metoder.

Duellen mellan medel och motmedel pågår hela tiden och sker stegvis även om tidsförloppet varierar mycket mellan olika områden. Just nu går utvecklingen relativt snabbt inom exempelvis cyberområdet till skillnad från exempelvis fasta drivämnen där den sker med inkrementella steg.

Många av de idag intressanta teknikområdena drivs till stor del av civila intressen, men kan komma att ha stor påverkan på militära tillämpningar. Det gäller exempelvis autonomi, robotik, IT och bioteknik. Civil teknik behöver dock ofta anpassas avseende tillförlitlighet, robusthet och säkerhet för att uppfylla militära krav.

¹ Offset betyder här att det är en strategi för att 'ta tillbaka initiativet', d.v.s. att åter bli övermäktig en motståndare som har anpassat sig till dagens vapen och taktik. Nu handlar det om att kunna hantera s.k. A2/AD (Anti-access, area denial).

² USA:s vice försvarsminister Bob Work, "CNAS Defense Forum," (JW Marriott, Washington, December 14, 2015), <http://www.defense.gov/News/Speeches/Speech-View/Article/634214/cnas-defense-forum> (Besökt 2017-06-13).

³ Se till exempel T.X. Hammes, Technology Converge and Power Diffuses – The Evolution of Small, Smart and Cheap Weapons, Policy Analysis, CATO Institute, no 786, 27 January 2016.

Teknikutvecklingen påverkar alla Försvarsmaktens arenor och plattformar – den framtida soldaten, mark, sjö, luft, ledning, logistik, rymd och cyber. Det är därför viktigt att upprätthålla både bred och djup kompetens inom områden med särskild försvarsmaktsrelevans så att man över tiden både kan förstå värdet av ny teknik och värdera denna på en systemövergripande nivå.

3 Additiv tillverkning

3.1 Beskrivning av området

Additiv tillverkning (eng. *additive manufacturing*, även *3D printing*) är en tillverkningssteknik där man lager för lager bygger upp en tredimensionell komponent med hjälp av små partiklar eller tråd utifrån en 3D-modell i en digital datafil. Additiv tillverkning lämpar sig särskilt väl för tillverkning av komponenter gjorda av polymerer, polymerkompositer eller metaller. Keramer är också möjliga men är idag mindre vanliga.

Teknologin lämpar sig för automatisering och mångfaldigande av identiska produkter men även för tillverkning av små serier och enstaka komponenter. Teknologin möjliggör tillverkning av strukturer som är svåra eller opraktiska att tillverka genom konventionella bearbetningstekniker, till exempel komponenter med interna hålrum.

Additiv tillverkning som produktionsteknik har funnits sedan 1980-talet men fram till ca år 2000 användes den huvudsakligen för tillverkning av enstaka exemplar (s.k. *rapid prototyping*) från polymerer där måttliga krav på dimensionsriktighet och mekanisk hållfasthet ställdes. Sedan dess har stora framsteg gjorts inom produktion av metalliska komponenter för bland annat flygsystem, gasturbiner och medicinska implantat. Investeringar (100-tals miljoner USD årligen) görs i FoU-miljöer i USA, Europa och Asien och tekniken är en viktig del av den fjärde industriella revolutionen, s.k. *Industry 4.0*.⁴

Utrustning för additiv tillverkning av metaller finns i olika utföranden där värmekällan kan vara en laser, elektronstråle eller ljusbåge. Styrning och kontroll av värmekällan är kritisk då den påverkar smält- och stelningsstegen och därmed materialets mikrostruktur och dess mekaniska, magnetiska, kemiska (korrosions) och utmattningssegenskaper. En additiv tillverkningsutrustning anpassad för ett visst material, till exempel en titanlegering, kan användas för tillverkning av många olika produkter. Det enda som i princip krävs är att en ny datafil laddas. Dock bör det påpekas att om man exempelvis byter pulvertyp (annan kornstorlek) så krävs normalt en justering eller större förändring av tillverkningsprocessen.

Typiskt för komponenter som tillverkas idag är att de är relativt små men komplexa, svåra att tillverka med konventionell teknik, kräver många bearbetnings- eller fogningsoperationer och görs av dyra och/eller svårbearbetade metaller/legeringar.

Inom försvarstillämpningar förutspås additiv tillverkning leda till kortare ledtider, billigare produktion, billigare underhåll, komponenter med lägre vikt och högre prestanda, mindre inventarier, livstidsförlängning och även kortare logistikkedjor i fält. Flertalet stora leverantörer av försvarsmateriel i USA och

⁴ Industry 4.0 eller den fjärde industriella revolutionen är en samlande term för en rad teknologier och koncept inom automation, processindustriell IT och tillverknings teknologier. Konceptet har koppling till *Internet of Things* och innebär att varje produkt i produktionskedjan bär med sig information om vart den ska och hur, för att fabriken ska kunna organisera sig själv. Målet är produktion med kortare omställnings- och ledtider, färre fel, mer flexibilitet och ingen tidskrävande programmering.

Europa investerar i miljöer för additiv tillverkning och i kompetensuppbyggnadsprojekt. Några som kan nämnas är MTU, Airbus, BAE Systems, MBDA, GKN Aerospace, Boeing och Dassault. Minst två länder (Norge och USA) har satt ihop mobila, containerbaserade additiva tillverkningsenheter som har fälttestats (även vintertid) med lovande resultat. USA har additiv tillverkning som en permanent resurs inom TRADOC.⁵ Under 2017 planerar EDA (Europeiska försvarsbyrån) att, under en multinationell fältövning, demonstrera en containerbaserad additiv tillverkningsenhet följt av en utställning, detta i syfte att informera försvarsorganisationer om teknikens möjligheter.

Det är inte ovanligt att det vid anskaffning av större materielsystem samtidigt köps in reservdelar för systemets beräknade livslängd, detta för att säkerställa tillgänglighet över kanske 30-40 år. Detta innebär stora inventariestkostnader i lager och logistiksystem. Det är möjligt att additiv tillverkning kan komma att användas för ”just in time”-tillverkning utifrån aktuella behov förutsatt att det finns en kvalificerad leverantör med kapacitet, lämplig utrustning och material till hands. I så fall minskar inventariestkostnaderna till det som behövs för att spara datafiler för respektive komponent. Det skulle även innebära att krav ställs på systemleverantören att vid behov kunna leverera reservdelar under en mycket längre tid än idag.

För att certifiera komponenter för högpresterande tillämpningar krävs bättre kunskap inom processkontroll, icke-förstörande provning, efterbearbetning och designoptimering. Vidare krävs bättre förståelse av teknikens möjligheter och begränsningar hos beslutsfattare och systemleverantörer.

Jämfört med teknologins potential används additiv tillverkning för närvarande i blygsam skala. För att kunna utnyttja den additiva tillverkningens alla fördelar krävs ett flertal tekniska studier, nya regelverk kring certifiering, nya designverktyg, utbildning, utveckling av nya affärsmodeller och sätt att hantera de informationssäkerhetsrisker som tekniken kan medföra.

3.2 Övergripande trender fram till 2035

Additiv tillverkning utvecklas mycket snabbt och betraktas som både nödvändig och drivande för *Industry 4.0*. Som med alla nya tekniker bör man dock behålla ett rimligt förhållningssätt och inte förvänta sig mirakler. Det är inte troligt att additiv tillverkning kommer att ersätta befintliga tillverkningstekniker, men den kan utan tvekan fungera som ett värdefullt komplement till dessa. Allteftersom kunskap om teknikens möjligheter och begränsningar sprids kan man förvänta sig att flera tillämpningar implementeras. Nuvarande tekniska och ekonomiska trender beskrivs närmare nedan.

Additiv tillverkning används redan för serietillverkning av kritiska komponenter till flygmotorer och för komponenter som används i krävande tillämpningar förknippade med stora ekonomiska risker om oväntade fel skulle inträffa.

Det finns ett flertal leverantörer av utrustning för additiv tillverkning i Europa och USA. Det finns även tecken på växande samverkan mellan företag som utvecklar utrustning och de som säljer pulver optimerade för additiv tillverkning,

⁵ US Army Training and Doctrine Command.

och det förekommer även samgående och uppköp. Man kan skönja strategier där samma företag levererar båda utrustning och pulver, och att bådadera är optimerade för varandra. Man kan även förvänta sig att företag inriktar sig mot tillämpningsområden med liknande krav när det gäller produktstorlek, produktionsvolym, krav på certifiering och provning, till exempel i flygsektorn.

Det är möjligt att nya affärsmodeller kommer att utvecklas, där legotillverkning sker i större skala, eller att företag säljer överskottskapacitet. Sådana signaler finns redan inom försvarssektorn.

Att optimera produkter för additiv tillverkning kräver nya verktyg och nya kompetenser. Idag använder man befintliga designer med bara smärre justeringar. Bristen på verktyg och kompetens för design kan fördröja implementering, men så länge man inte designar helt nya produkter finns ingen större risk för detta.

Storleken på komponenter som kan tillverkas genom additiv tillverkning begränsas av utrustningen till volymer som idag oftast är mindre än 50x50x50 cm. Dock finns det intresse för att kunna tillverka större komponenter, och vissa speciella maskiner kan tillverka meterstora komponenter. Det finns inget tekniskt hinder att skala upp då smältzonen i additiv tillverkning bara är av mm-storlek. Det är mer en fråga om marknaden vill köpa större komponenter i tillräckliga volymer. NASA har tillverkat en demonstrator som väger 100-tals kg och är meterstor. Tillverkning av ännu större komponenter rapporteras ske i Kina.

De metallpulver som idag finns att köpa är sällan optimerade för additiv tillverkning. Vissa legeringar kan användas utan problem och för vissa pågår utvecklingsarbete som inte nödvändigtvis kräver stora modifieringar. Det pågår även studier av samband mellan den additiva tillverkningsprocessen och hur denna påverkar materialets mikrostruktur och följaktligen materialets mekaniska egenskaper, korrosionsbeständighet, utmattningssegenskaper etc.

Additiv tillverkning kommer på sikt att möjliggöra mer komplexa, sammansatta komponenter med ökad funktionalitet. Det är en fördel då volymen för samma funktionalitet förväntas krympa, men det ställer högre krav på design, och med en högre grad av integration kommer det bli svårare att reparera en skadad eller obrukbar komponent.

Det är en fördel att drivkrafterna som motiverar industrins stora investeringar i additiv tillverkning för civila produkter speglar behov som köpare och brukare av försvarsmateriel också prioriterar. I grova drag är dessa drivkrafter kostnads-effektiv tillverkning och system med låga drifts- och underhållskostnader.

Då försvarsmateriel inte alltid utnyttjas på samma sätt som motsvarande civila produkter kan det finnas olika fördelar och nackdelar med additiv tillverkning. Till exempel flygs militära flygplan mindre men förväntas hållas i drift längre, och militära fartyg måste kunna repareras och underhållas långt ifrån en hemmabas. Därför kan additiv tillverkning erbjuda större möjligheter för försvarets bruk än för motsvarande civila tillämpningar, men det krävs förstås att personal med lämplig kunskap samt tillverkningsutrustning finns tillgänglig.

Ett redan implementerat sätt att använda additiv tillverkning är att med hjälp av teknologin producera verktyg och formar för konventionell tillverkning.

Genom att sänka verktygets kostnad möjliggörs kostnadseffektiv tillverkning i serier som är mindre än vad som annars hade varit möjligt.

Genom att kunna tillverka specialverktyg vid behov minskas behovet av att alltid ta med sig en hel uppsättning verktyg ”i fall att” någon del skulle behövas. Detsamma gäller även för viss medicinsk utrustning. Därmed reduceras de logistiska behoven. Samtidigt krävs istället att utrustning och material för additiv tillverkning tas med.

Idag tillämpas additiv tillverkning på ett konservativt sätt där de tekniska riskerna är små och drivkrafterna huvudsakligen är ekonomiska. Detta gäller särskilt flygsektorn. Man tillverkar befintliga komponenter i samma legering efter samma design, eventuellt med smärre modifieringar. De stora vinsterna när det gäller ökad funktionalitet och sänkta kostnader förväntas nå dagens ljus om några år, och är beroende av hur fort tekniken kan implementeras och hur hård konkurrensen är från befintlig teknik.

3.3 Koppling till andra teknikområden och krav på dessa

All försvarsmateriel bör helst tillverkas på ett sätt som är så kostnadseffektivt, tillförlitligt och miljövänligt som möjligt. Materiel för alla domäner (luft, mark, sjö och rymd) påverkas. Även materiel som inte är krigsmateriel påverkas, till exempel hygien- och sjukvårdsutrustning.

Additiv tillverkning kopplas direkt till materialteknik och tillverkningsteknik, samt till multifunktionella material. I och med additiv tillverkning krävs ett förändrat tankesätt för att teknikens möjligheter ska kunna tas tillvara på bästa sätt.

3.4 Potentiella militära tillämpningar

Eftersom i princip alla existerande komponenter kan tillverkas genom additiv tillverkning krävs en systematisk process för att identifiera och prioritera där det är mest lämpligt att påbörja studier av teknologins möjligheter och begränsningar. Andela & Knofius (2016) beskriver en sådan process och hur teknologin skulle kunna bidra till militär logistikförmåga.

Culverwell (2016) sammanfattar additiv tillverknings potential att bidra till en militär förmåga, indelat i följande avsnitt:

- *In the Defence Supply Chain*
- *As a Deployed Capability*
- *Barriers to Procurement*
- *Route to Exploitation*

I en färsk rapport ger Haseltine (2016) en mycket läsvärd översikt över hur teknologin kan bidra i fält.

Exempel på förvarstillämpningar och tänkbara motiveringar ges nedan. Listan är inte uttömmande.

<i>Exempel på tillämpning</i>	<i>Motivering</i>	<i>Status</i>
Kopiering av obrukbara komponenter som ej längre tillverkas eller lagerförs	Livstidsförlängning av arvet	Implementerat sedan länge
Viktbesparing genom bättre design	Högre systemprestanda	Implementerat (Kool, 2016)
Reservdelstillverkning i fält	Högre systemtillgänglighet och enklare logistik	Implementerat av US Army
Tillverkning på plats i svåra miljöer	”Bra att ha nu”-komponenter för att lösa pågående uppdrag	Implementerat i test (Norberg et al, 2016)
Reservdelar just-in-time	Lägre kapitalinvestering i reservdelar och logistik	Förslag som studeras
Individualisering av personlig utrustning, t.ex. pistolgrepp	Bättre komfort för soldaten	Implementerat i test-miljöer
Omdesign av befintliga komponenter	Lägre vikt, färre fogar, lägre kostnad	Serietillverkning, t.ex. bränslemunstycke till flygmotor (GE, 2015)
Omdesign av befintliga komponenter	Mer komplexa geometrier, bättre kylning	Implementerat i flygplan (US GAO, 2015)
Tillverkning av små serier	Lägre kostnad	Förslag
Reparation av slitna flyg- och vapensystemkomponenter	Underhåll och livstidsförlängning	Implementerat (Liu et al, 2016)

Det kan noteras att svenska militära styrkor även tilldelas fredsbevarande uppdrag i miljöer med dåliga kommunikationsmöjligheter. Där är logistikkedjan svår att upprätthålla. I en studie diskuterar Waleij et al (2015) hur additiv tillverkning kan bidra till humanitära insatser.

3.5 Begränsande faktorer

De faktorer som idag begränsar snabbare och bredare implementering av additiv tillverkning är desamma för militära och civila tillämpningar:

- Det saknas erfarenhet i många led, från design för additiv tillverkning till leverantörer och beslutsfattare som inte har kunskap om vad som är möjligt och omöjligt med teknologin.
- Ofullständiga kunskaper vad gäller exempelvis utmattning eller korrosionsegenskaper hos additivt tillverkade komponenter.
- Relevanta standarder för kvalitetssäkring saknas.
- Det finns en del legeringar tillgängliga i pulverform som kan användas för additiv tillverkning, men vissa legeringar måste modifieras och det finns utvecklingspotential för nya legeringar.
- Det saknas icke-förstörande provningsmetoder anpassade för additiv tillverkning.
- Det saknas kunskap om och metoder för efterbearbetning av additivt tillverkade komponenter.
- Det är oklart vilka regler som gäller angående *Intellectual Property Rights* (IPR) och ansvar om man använder additiv tillverkning för att kopiera eller modifiera komponenter.
- Det saknas processer för återbruk av överskottspulver som garanterar bibehållen pulverkvalitet.
- Additiv tillverkning öppnar för möjligheten att nya underleverantörer tillverkar på beställning utifrån en digital datafil, men det medför även risker avseende informationssäkerhet, manipulering, otillåten modifiering och förfalskning.
- Tekniken kan brukas av nya organisationer och små aktörer som i små lokaler och med begränsade resurser kan tillverka krigsmateriel.

3.6 Referenser

Andela, C. & Knofius, N., *Promising Enhancements of the Defence Logistics Footprint Using Additive Manufacturing*. NATO-AVT-258-03, 2016.

Culverwell, R.A., *Common Approach for NATO: The Exploitation of Additive Manufacture in Defence*. NATO-AVT-258-01, 2016.

General Electric. <http://www.gereports.com/post/119370423770/jet-engines-with-3d-printed-parts-power-next-gen/> (Besökt 2016-07-29).

Haseltine, S.J., *Exploiting Additive Manufacturing from a Deployed Military Perspective*. NATO-AVT-258-KN, 2016.

Kool, G., *Testing and Certification of a Redesigned Helicopter Part Made with Additive Manufacturing*. NATO-AVT-258-15, 2016.

Liu, Q., Walker, K.F., Djugum, R., Sharp, P.K., *Repair of Australian Military Aircraft Components by Additive Manufacturing Technology*. NATO-AVT-258-04, 2016.

Norberg, C.D., Flathagen, J., Østereng, T. *Small Nation Perspective on Deployed Military Additive Manufacturing*. NATO-AVT-258-02, 2016.

US GAO-15-505SP June 2015. *3D Printing: Opportunities, Challenges, and Policy Implications of Additive Manufacturing*. <http://gao.gov/assets/680/670960.pdf> (Besökt 2016-08-01).

Waleij, A., Tjäder, Z., Liljedahl, L., Brännström, N., *Can additive manufacturing revamp supply chains for humanitarian aid or peace operations?* FOI Memo 5569, 2015.

4 Cyber

4.1 Beskrivning av området

Cyberområdet spelar i dagens uppkopplade samhälle en viktig roll för både enskilda individer och samhället i stort. Oavsett om vi vill kontrollera saldot på vårt bankkonto, ringa ett telefonsamtal eller genomföra ett kortköp så är vi beroende av välfungerande och säkra kommunikationer. På samma sätt är centrala samhällsfunktioner som energi- och transportsektorn starkt beroende av fungerande och säkra informationssystem. Detsamma gäller i stor utsträckning också annan offentlig samhällsservice så som sjukvård och polisiär verksamhet.

Samtidigt tenderar allt fler samhällskritiska system att kopplas samman som ”system av system” på en global nivå, vilket leder till komplexa och svåranalyserade säkerhetsberoenden mellan många olika aktörer och intressenter. Detta innebär att vi samtidigt som vi blir alltmer beroende av informationsteknologi (IT) också blir mer och mer sårbara för störningar i IT-infrastruktur, helt oavsett om denna orsakas av den mänskliga faktorn, elavbrott eller cyberattacker från främmande makt.

Cyberförmågan är ett verkanssystem som existerar parallellt med de traditionella försvarsförmågorna och ger tillgång till alternativa sätt att uppnå ett visst mål. Inom den militära kontexten likställs inte sällan begreppet ”cyber” med samlingsnamnet *computer network operations* (CNO), vilket kan delas in i underkategorierna *computer network defence* (CND), *computer network attack* (CNA) och *computer network exploitation* (CNE). Lite grovt kan CND definieras som handlingar för att skydda, övervaka, analysera, detektera och svara på nätverksattacker, intrångsförsök och andra typer av handlingar riktade mot IT-system, medan CNA är den andra sidan av myntet. Vidare rymmer CNE-begreppet olika typer av attacker mot informationssystem för att möjliggöra spionage eller underrättelseinhämtning.

Även om dator- och nätverksoperationer är centrala för cyberområdet är det viktigt att inse att cybersäkerhet inte enbart har att göra med brandväggar, virus, hackerattacker och trojaner. I den senaste tidens omvärldsutveckling har det blivit alltmer tydligt hur olika typer av påverkansoperationer kan spela en allt viktigare roll i såväl krigstid, skymningsläge som fredstid, innefattande allt från att piska upp en hätsk stämning i sociala medier mot olika grupper till att fysiskt sabotera IT-relaterad infrastruktur. Cyberförmågan kan ingå som en komponent i sådana påverkansoperationer.

4.2 Övergripande trender fram till 2035

Dagens data- och nätverksteknologier bygger på nästan samma plattform som den som fanns på 1980-talet. Exempelvis var det då processorarkitekturen x86 slog igenom och programvaruspråket C++ släpptes. Idag, mer än 30 år senare, är x86 fortfarande bland de vanligaste arkitekturerna, och C++ är ett av de flitigast nyttjade programvaruspråken. I korthet innebär detta att samma typer av

mjukvarusårbarheter (exempelvis buffertöverskridningsbrister⁶) funnits i mer än trettio år. Inte heller distribuerade överbelastningsattacker (DDoS) är något nytt och trots att det idag finns en arsenal av olika tekniker för att försvara sig är det fortfarande i stort sett en fråga om att ha mer bandbredd än trafiken hotaktören kan producera. I och med att den teknologiska utvecklingen idag inte är lika explosiv som på 1980-talet är det rimligt att anta att dessa typer av sårbarheter kommer att bestå även om 20 år.

En stor skillnad kan dock spåras tillbaka till 1980-talet. Under denna tid var komplexiteten för IT-system så begränsad att en duktig programmerare kunde ha insyn i allt ifrån kablar till applikationsnivån. Detta har med tiden förändrats, och idag är en vanlig mjukvara så komplicerad att ingen enskild individ har komplett förståelse för hur allt hänger ihop. Bruk av ramverk och bibliotek som låter utvecklaren skapa applikationer utan att egentligen förstå vad som händer ”under huven” är idag praxis. Det finns dock oerhört många ramverk och bibliotek som fyller samma syfte. Det är sannolikt att det i framtiden kommer att bli färre överlappande ramverk och bibliotek, och istället större kommersiella drivkrafter bakom de som består. Sårbarhetsmässigt betyder en mer homogen applikationsflora att antalet brister per rad kod kommer att minska, men att de brister som dyker upp får större genomslag (då de är vanligare i praktiken).

Standardisering i form av ramverk, appbutiker och liknande kommer sannolikt även att påverka vilka typer av sårbarheter som förekommer. Det finns idag enkelt implementerade och relativt effektiva skydd mot till exempel buffertöverskridningsbrister. Problemet är dock att dessa inte alltid implementeras på ett korrekt sätt i operativsystem och att applikationer oftast inte måste inkorporera dem. Standardiseringen kommer att forcera utvecklingen av skydd, och därmed minska antalet exploaterbara minnessårbarheter, men den kan samtidigt öka antalet brister som rör felaktiga antaganden från utvecklare som inte helt förstår ramverket de nyttjar. Dessa brister inkluderar exempelvis *command injection*, *file inclusion*, *SQL-injection*⁷ och *cross-site scripting* (XSS).⁸

Det bör även tilläggas att ett ökat krav på funktioner gör att antal rader kod inte kommer att bli färre, utan fler, vilket i sin tur kan betyda fler sårbarheter. Vi måste också alltjämt leva med mycket av den *legacy*-kod som skapades i en tid då cyberattacker i stort sett var obefintliga.

Att injicera skadlig kod i hårdvara är mycket attraktivt eftersom hotaktören då kringgår de allra flesta moderna IT-skyddsmekanismer. Idag är det dock väldigt få skadliga koder som sprider sig till hårdvarukomponenter (till exempel BIOS/UEFI⁹ eller *firmware*¹⁰ för en hårddisk). Anledningen till detta är att den skadliga koden måste vara specialskriven för varje hårdvara, vilket i kombination med den stora variationen på hårdvara helt enkelt gör att det inte är särskilt lukrativt utom kanske för motiverade aktörer med stora resurser. Vi ser dock redan idag att de hårdvaror som nyttjas blir mer och mer lika, och att vissa leveran-

⁶ En sårbarhet som möjliggör omskrivning av en applikations inre, t.ex. tillägg av en bakdörr.

⁷ *Structured Query Language* (SQL) injection handlar om införande av skadliga anrop till en SQL-databas.

⁸ *Cross Site Scripting* (XSS) handlar om införande av skadlig javascript-kod genom en part som mottagaren litar på.

⁹ BIOS/UEFI är ett grundläggande program som startas på en dator innan dess fullskaliga operativsystem körs.

¹⁰ Ett *firmware* är en enklare typ av operativsystem som oftast nyttjas av IT-system med specialiserade tillämpningsområden, såsom tv-kontroller, hårddiskar och routrar.

törer (exempelvis Intel) blir allt mer dominerande på marknaden. Samtidigt får drivrutiner och *firmware* som styr hårdvaror allt fler egenskaper. Homogeniseringen och produktutvecklingen av hårdvara visar inga tecken på att avta, och kommer i kombination att göra det mer lukrativt att utföra cyberattacker mot hårdvara.

En trend som väntas hålla i sig är det så kallade *Internet of Things* (IoT, svenska: "sakernas internet"). I takt med att kostnaden för att förse olika föremål med nätverksuppkoppling blir allt lägre så ser vi redan idag hur allt fler klockor, övervakningskameror, personvågar, TV-apparater och kylskåp börjar kopplas upp trådlöst. Enligt olika prognoser kommer inom kort tid miljontals nya saker eller enheter kopplas upp på daglig basis, för att 2020 ha nått mer än 50 miljarder uppkopplade enheter. Dagens och än mer de framtida militära plattformarna, vapen- och sensorsystemen kommer även de sannolikt att innehålla IT-komponenter (sensorer, styrenheter, ställdon etc.) som är mer eller mindre uppkopplade i nätverk.

Även om IoT erbjuder en rad spännande möjligheter så kan det också förväntas skapa enorma säkerhetsutmaningar. Exempelvis kan enheter med nätverksuppkopplingar för några få kronor komma att stå vidöppna för välkända sårbarheter i årtal, eftersom säkerhetsuppdateringar omöjligen kan prioriteras med sådana affärsmodeller. Således kommer det att finnas gränssytor, via till exempel cyberrymden, insiders och leverantörskedjor, som ger möjlighet att påverka fysiska system. Även om informationen som finns på enheterna i sig själv inte är högt intressant för en motståndare, så kan den attackerade enheten eller informationen på grund av den alltmer uppkopplade naturen hos olika enheter utgöra grunden för en attack mot mer skyddsvärd information.

En annan trend som förväntas fortgå är att utveckling och exekvering av skadlig kod blir allt mer användarvänlig; affärsmodellen och användarkraven blir helt enkelt allt mer lika de som finns för allmän mjukvara. I korthet innebär detta att det i framtiden kommer att vara enklare för mindre kompetenta hotaktörer att identifiera nya brister, samt att exploatera existerande brister.

Slutligen prognostiseras det kring två mer svårförutsägbara trender, nämligen artificiell intelligens och kvantdatorer. Artificiell intelligens är idag ett omoget område, men har redan visat sig kunna vara till hjälp för att behandla diverse problem. Det är inte omöjligt att det om 20 år är en basfunktion inom de allra flesta tekniska produkter. Om detta blir fallet öppnar sig nya möjligheter att utföra cyberattacker genom att träna om algoritmerna som den artificiella intelligensen är baserad på.

Kvantdatorer är än mer omoget än artificiell intelligens men kan om stora framsteg görs komma att förändra IT i grunden. Exempelvis kan en kvantdator i teorin knäcka gruppen av asymmetriska krypton som idag hjälper till att skydda data (till exempel vid webbsurfning).

4.3 Utveckling av specifika delområden/teknologier

För att hinna med i den snabba utvecklingen inom cyberområdet krävs investeringar. Eftersom vi människor är delaktiga i konstruktion, installation, drift och

användning av teknologier bör framtida arbeten beakta människa och maskin i kombination, snarare än isolerat.

4.3.1 Standardiserade tester och empiri

Det råder idag ingen brist på lösningsförslag och verktyg inom IT-säkerhetsområdet. IT-säkerhetslösningar spänner över allt från träning av personal mot nätfiskeförsök till kryptokakor som upptäcker om kontrollflödet i en mjukvara har riktats om från det förväntade. Faktum är att det finns oräkneliga verktyg och metoder som är tänkta att hantera samma problem, men som fungerar på helt olika sätt.

En av de största anledningarna till den stora mängden säkerhetslösningar är att det idag är oerhört svårt att avgöra vad som fungerar bra och vad som fungerar dåligt. Det finns ingen tillförlitlig eller valid empiri som rör angrepp, eller någon standard för hur utvärderingar av olika verktyg och metoder bör utföras.

För att cybersäkerhet ska uppnå samma mognadsgrad som till exempel det medicinska området, där det inte är accepterat att föreslå en produkt utan att produkten i fråga genomgått omfattande tester, krävs det en stor kulturförändring kring utförande av produkttester.

4.3.2 Detektion av sårbarheter

Det behövs omfattande utveckling av metoder för att identifiera och behandla sårbarheter för att uppnå framtida säkra IT-system.

I och med att IT-system blir allt mer komplicerade, och därmed allt svårare för utvecklare att förstå, finns det en risk att även kritiska sårbarheter blir fler till antalet, samt att det tar längre tid att identifiera dem.

Utgående från antagandet att det alltid kommer att finnas sårbarheter blir följaktligen frågan hur de bäst detekteras och behandlas i efterhand. Idag tillämpas huvudsakligen två typer av verktyg för att automatisera denna tidskrävande process. Den ena kategorin är så kallade *fuzzers*, verktyg som kommunicerar med mjukvaror på sätt som är tänkta att få dem att krascha och därigenom exponera sårbarheter. Den andra kategorin är statisk kodanalys, som involverar att automatiskt granska källkod för att identifiera användning av sårbara funktioner och dylikt.

Ingen av dessa metoder är för närvarande särskilt effektiv. En *fuzzer* är otillräcklig eftersom det finns många sätt att interagera med en mjukvara, och testfall på grund av tidsbegränsningar enbart kan skapas för en liten delmängd av alla dessa interaktioner. Statisk kodgranskning är otillräckligt eftersom det inte är möjligt för verktyget att effektivt spåra komplexa flöden i en applikation. Exempelvis är det svårt för ett kodgranskningsverktyg att förstå hur en förfrågan från en klient kopplas till ett svar från en server, då källkoden för dessa metoder inte är ihopkopplad.

4.3.3 Intrångsdetektionssystem och hotmodeller

Att bygga ett system som identifierar och förhindrar alla angrepp som utförs är något av en "helig graal" då det skulle möjliggöra säker exekvering av sårbara

system. Forskningen inom intrångsdetektion är omfattande och innefattar allt från placering av sensorer till val av algoritmer som är tänkta att larma för angrepp.

All sensordata som produceras i och med IoT är ett viktigt forskningsområde, både idag och i framtiden. Olika sensorer fångar in data som var och en för sig kanske är irrelevanta, men som i kombination ger tydliga indikationer på cyberangrepp. Att skapa algoritmer som på ett effektivt sätt korrelerar olika typer av data för att identifiera angrepp, samt metoder för att spara och söka i dessa stora datamängder på ett effektivt sätt, är därmed viktigt både idag och om tjugo år.

Tyvärr bygger dagens intrångsdetektionssystem på förenklade hotmodeller, såväl gällande vilka cyberattacker som är rimliga som hur en hotaktör kan förväntas uppträda. Anledningen till detta är den begränsade forskningen kring hotmodellering, exempelvis vad som kan ses som rimliga beteenden hos en hotaktör under olika förutsättningar. Utöver standardiserade empiriska tester krävs omfattande teoriutveckling kring hotmodellering för att uppnå effektiva intrångsdetektionssystem.

4.3.4 Cyber situational awareness och träning inom cyberförsvar

Att kunna bygga upp och vidmakthålla en god lägesförståelse med avseende på cyberrymden är kritiskt för att kunna bedöma cyberattackers roll i en större kontext. Många exempel på sådana typer av mer komplexa och domänöverskridande attacker har utförts under de senaste åren, och de kan förväntas öka i omfattning. *Cyber situational awareness* (CSA) är det övergripande område som handlar om människans förmåga att förstå cyberrymden tillsammans med situationsuppfattningen kring de fysiska arenorna. En god CSA är till exempel en förutsättning för att kunna upptäcka om en cyberattack i själva verket syftar till att avleda uppmärksamheten från ett långt värre datorintrång, eller huruvida ett datorintrång syftar till att åstadkomma en effekt i den fysiska miljön.

För att uppnå en god förmåga inom CSA krävs övning. På grund av begränsad tillgång till realistiska träningsmiljöer är det idag ovanligt att relevant personal har övats. Det är än ovanligare att någon empirisk forskning faktiskt bedrivits baserad på sådan träning. Omfattande träning, samt forskning kring sådan träning, krävs för att öka förmågan inom CNO.

På samma sätt krävs det träning kring utförande av offensiva operationer för att öka motståndskraften mot sådana operationer.

4.3.5 Kaskadeffekter i cyberberoende infrastruktur

Samhället är beroende av att kritiska infrastrukturer såsom elnät, vattenförsörjning och transporter fungerar som de ska. Numera utgör även informationsinfrastrukturen en sådan alltmär central infrastruktur, och denna påverkar och påverkas i hög grad av andra infrastrukturer.

Förmåga behövs därför avseende att kunna bedöma den ömsesidiga påverkan mellan cyberrymden och övriga miljöer. För att åstadkomma detta behöver representativa modeller av cyberrymden tas fram och relateras till befintliga modeller av andra kritiska infrastrukturer. Med sådana modeller kan man genom

simulering försöka bedöma effekten av hur olika attacker kan tänkas drabba samhället, och effektiviteten av olika skyddsåtgärder.

4.3.6 Beteende i cyberrymden

Att kunna verka dolt i cyberrymden och att i en cyberoperation kunna upptäcka, klassificera och identifiera aktörer kräver förutom en anonym nätverksanslutning också att man kan dölja sitt beteende i form av hur man uttrycker sig, skriver skadlig kod samt vilka användningsmönster som utnyttjas då man genomför inhämtning och intrång. Detta gör det nödvändigt att för framgångsrikt utförande av eller försvar mot cyberattacker tillägna sig kunskap avseende att kunna dölja och/eller känna igen relevant beteende i cyberrymden och i de spår en motståndare lämnar efter sig.

Att analysera beteende i cyberrymden och cyberoperationer handlar forskningsmässigt om att ta tillvara på det som görs i forskningsfronten avseende inhämtning och analys av stora mängder data (i olika utsträckning strukturerade texter, metainformation, bilder, filmklipp m.m.) som underlag för utveckling av processer och verktyg anpassade för cyberdomänen. Området är tillämpat och kräver kompetenser inom exempelvis maskininlärning, datorlingvistik, antropologi, bildanalys, informationsvisualisering och etik.

4.4 Potentiella militära tillämpningar

Vad gäller cyberområdet är det svårt att dra en definitiv och skarp gräns mellan militära och icke-militära tillämpningar. Många av de IT-attacker som har ägt rum och som kan misstänkas ha en statsaktör som utförare eller i varje fall sponsor av attackerna har inte skett i krigstid och mot militära mål, utan som ett medel i en politisk konfliktsituation. På samma sätt utförs påverkansoperationer inte bara i krig utan också som ett rent politiskt maktmedel i fredstid. Sammantaget gör detta att cyberområdet inte kan betraktas från ett rent militärt perspektiv, utan att Försvarsmakten och andra aktörer måste samarbeta och dela information om dessa frågor – såväl nationellt som internationellt.

Givet detta finns det möjliga militära tillämpningar från kartläggning av specifika individer i försvarsunderrättelsesyfte till att slå ut energitillförseln i en hel stad eller att slå mot högvärdiga militära plattformar. Genom att rikta cyberattacker mot fiendens nätverk eller IT-sensorer kan även möjligheterna till effektiv kommunikation eller situationsbedömning till stora delar slås ut.

4.5 Begränsande faktorer

Begränsande faktorer för användning av eller försvar mot cyberangrepp är i första hand inte tekniska utan snarare etiska eller juridiska. Att slå ut fiendens energikapacitet som en kaskadeffekt av ett lyckat cyberangrepp kan innebära stora taktiska fördelar på slagfältet, men kan på samma gång innebära stort lidande hos civilbefolkningen. På samma sätt är det etiskt och juridiskt tveksamt huruvida det är lämpligt att försöka påverka opinionen hos en meningsmotståndare genom att på olika sätt sprida desinformation från falska avsändare på sociala medier.

Ovanstående kan tyckas självklart, men faktum är att juridiken inte heller är tydlig vad gäller försvar mot vissa cyberrelaterade angrepp. Detta gäller också för andra typer av angrepp, där det enda riktigt effektiva sättet att försvara sig mot en motståndare är att rikta motattacker mot dennes system, vilket snabbt skulle kunna leda till en accelererande konflikt.

4.6 Referenser

Brynielsson, J., Franke, U., Tariq, M., Varga, S., *Using cyber defense exercises to obtain additional data for attacker profiling*. I Proceedings of the 14th IEEE International Conference on Intelligence and Security Informatics (ISI 2016), Tucson, Arizona, September 2016.

Brynielsson, J., Franke, U., Varga, S., *Cyber situational awareness testing*. I Akhgar, B. & Brewster, B. (eds.), *Combating Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*, chapter 12, pages 209–233. Springer International Publishing, 2016. doi:10.1007/978-3-319-38930-1_12.

Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Mårtenson, C., Svenson, P., *Harvesting and analysis of weak signals for detecting lone wolf terrorists*. *Security Informatics*, 2(1), 2013. doi:10.1186/2190-8532-2-11.

Brynielsson, J. & Sharma, R., *Detectability of low-rate HTTP server DoS attacks using spectral analysis*. I Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2015), pages 954–961, Paris, France, August 2015. doi:10.1145/2808797.2808810.

Franke, U. & Brynielsson, J., *Cyber situational awareness – A systematic review of the literature*. *Computers & Security*, 46:18–31, October 2014. doi:10.1016/j.cose.2014.06.008.

Holm, H., *A large-scale study of the time required to compromise a computer system*, *IEEE Transactions on Dependable and Secure Computing*, 2013.

Holm, H., *Signature based intrusion detection of zero-day attacks: (not) a closed chapter?*, 47th Hawaii International Conference on Systems Sciences (HICSS), 2014.

Holm, H. & Afridi, K., *An Expert-Based Investigation of the Common Vulnerability Scoring System*, *Computers and Security*, 2015.

Holm, H., Buschle, M., Shahzad, K., Ekstedt, M., Korman, M., *P²CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language*, *IEEE Transactions on Dependable and Secure Computing*, 2014.

Holm, H., Ekstedt, M., Andersson, D., *Empirical analysis of system-level vulnerability metrics through actual attacks*, *IEEE Transactions on Dependable and Secure Computing*, 2012.

Holm, H. & Sommestad, T., *SVED: Scanning, Vulnerabilities, Exploits and Detection*, MILCOM: Premier Military Communications Event, 2016.

5 HPM (High Power Microwave)

5.1 Beskrivning av området

Telekrigsföringsoperationer förväntas få en allt större roll i framtida konflikter. Den offensiva delen, Elektronisk Attack (EA), innefattar aktiva åtgärder som olika typer av störning, vilseledning och generering av elektromagnetiska pulser med hög toppeffekt. Delområdet HPM (eng. *High Power Microwave*) behandlar teknologier för att generera elektromagnetiska pulser med hög toppeffekt som temporärt eller permanent kan försätta målelektroniken ur funktion. Inom området studeras hur HPM-strålning verkar mot olika typer av elektroniska komponenter och utrustningar samt hur man provar och skyddar utrustning och samhällssystem mot denna typ av elektromagnetisk påverkan.

Det som skiljer HPM från andra typer av EA är möjligheten till permanent fysisk förstörelse av elektronisk utrustning samt möjligheten att störa/förstöra även icke kommunicerande elektroniska system genom inkoppling av energi via kablage och/eller direkt in på kretskort, så kallad bakvägskoppling. Så kallad framvägskoppling är endast aktuell för kommunicerande målobjekt och innebär att den skadliga energin kopplas in via systemets antenn. Framvägskoppling kan i sin tur delas upp i inombands- och utombandskoppling för att skilja på om HPM-pulsens frekvens överensstämmer med målsystemets kommunikationsfrekvens (inomband) eller inte (utomband).

Det faktum att HPM-tekniken blivit fältmässig innebär att man börjar kravställa militär materiel med avseende på HPM-hotet.¹¹ Detta innebär i sin tur att det pågår ett intensivt arbete på flera håll i världen (inklusive Sverige) för att ta fram metoder för att prova materiels tålighet mot HPM-bestrålning.

5.2 Övergripande trender fram till 2035

Då militär elektronik ofta är väl skärmad och då HPM-tålighet börjar bli en del av kravställningen vid anskaffning av ny materiel är det knappast troligt att HPM-vapen kommer att användas för att på bred front slå ut motståndarens elektronik på slagfältet. HPM-tekniken kan dock användas för att generera mycket kraftig störning som försvårar motståndarens kommunikation, i huvudsak genom framvägskoppling, d.v.s. där mikrovågorna tränger in till exempel via antenner eller sensorer.

Bredbandiga HPM-källor kan ge signaler med mycket hög toppeffekt som sprider energin över ett brett frekvensområde. Själva pulsen är kortvarig, någon eller några nanosekunder, men då den kan genereras med hög repetitionsfrekvens, som dessutom kan varieras, blir det svårt för motståndaren att hitta luckorna som tillåter kommunikation. HPM-operatören vet däremot när pulserna kommer och kan utnyttja luckorna för egen kommunikation. Då energin i strålningen är spridd över ett brett frekvensband är det inte troligt att den ger förstörande verkan.

¹¹ MIL-STD-464C, "Department of Defence Interface Standard, Electromagnetic Environmental Effects Requirements for Systems", Dec 2010 (med hemlig definition av HPM-hot och plattformar i MIL-HDBK-235-8).

De HPM-källor som kan generera en extremt hög toppeffekt är smalbandiga, dvs. strålningens frekvensinnehåll är mycket begränsat. Dessa källor kan åstadkomma förstörande verkan i såväl kommunicerande som icke-kommunicerande elektronisk utrustning.

En trend verkar vara att använda HPM på ett mer förtäckt sätt i en tidig fas av en konflikt och då i syfte att slå ut/störa det civila samhällets infrastruktur och kommunikationer. Mycket tyder på att Ryssland använde avancerad telekrigföring och HPM för att störa både civilsamhället och den primitiva militära kommunikationen i Ukrainakonflikten.¹²

Då verkansavstånd för förstörande verkan är av storleksordningen enstaka kilometer behöver man komma nära målet för att åstadkomma denna typ av verkan.

Den tidigare nämnda utvecklingen av provningsmetodik och användning av metodiken på olika typer av elektroniska system ger också mycket god insikt i hur HPM-vapen bör specificeras för att slå mot specifika mål. Denna utveckling innebär i sin tur att vi kan förvänta oss HPM-vapen som är anpassningsbara för att kunna slå ut flera olika typer av mål, så kallad ”smart HPM”. Utvecklingen av *Active Electronically Scanned Array* (AESA)-tekniken¹³ för radarapplikationer möjliggör en mycket koncentrerad antennlob som dessutom kan styras för att följa ett mål eller svepa av ett område.

Genom att utnyttja en större yta som antenn blir det möjligt att skapa stora effektiva antenner med hög antennförstärkning på till exempel flygplanskroppar/-vingar.

5.2.1 Exempel på försök och användning

I USA bygger Boeing en demonstrator i form av en HPM-kryssningsrobot som ska kunna ta sig fram till och bestråla målet på relativt nära håll. I det öppet tillgängliga materialet verkar det som att tanken är att den ska verka mot civil elektronik.¹⁴

Flera länder undersöker HPM-teknik för att stoppa bilar och båtar genom att störa/förstöra motorns elektroniska tändsystem. De närmaste åren kommer vi säkert att se en hel del utvecklingsarbete för att använda HPM-teknik mot drönare och speciellt svärmar av drönare.¹⁵

I USA har man utvecklat HPM-liknande strålkällor i syfte att störa/förstöra IED-elektronik. Ett problem i detta sammanhang är att avgöra om en IED verkligen oskadliggjorts vid bestrålning.

¹² Blank, S., “A Military Assessment of the Russian War in Ukraine”, American Foreign Policy Council, <http://russialist.org/transcript-a-military-assessment-of-the-russian-war-in-ukraine/>, 2015. (Besökt 2017-06-12).

¹³ “Active electronically scanned array”, Wikipedia, https://en.wikipedia.org/wiki/Active_electronically_scanned_array (Besökt 2017-03-02).

¹⁴ Counter-electronics High-powered Microwave Advanced Missile Project (CHAMP), <http://www.boeing.com/features/2012/10/bds-champ-10-22-12.page>, 2012. (Besökt 2017-06-12).

¹⁵ Counter-electronics High-powered Microwave Advanced Missile Project (CHAMP), <http://www.boeing.com/features/2012/10/bds-champ-10-22-12.page>, 2012. (Besökt 2017-06-12).

5.3 Koppling till andra teknikområden och krav på dessa

Av naturliga skäl ställer användandet av HPM vissa krav på egen utrustning då den behöver vara väl skärmd för att inte skadas av 'egen eld'.

Även om strålningsloben har en viss bredd och alltså inte behöver riktas in lika noga som en laserstråle eller kinetiska projektiler från eldrörsvapen behövs någon form av inriktningsverktyg. I de fall objekten är små och har låg radarsignatur (exempelvis UAV:er eller svärmar av dessa) kan detta bli en utmaning.

Då en HPM-attack inte följs av explosioner eller annan direkt bekräftelse på verkan i målet kan man tänka sig en koppling till andra telekrigföringstekniker där det är möjligt att lyssna av motståndarens radiotrafik och eventuellt andra elektroniska system för att erhålla verkansbekräftelse. Sådana tekniker undersöks redan i samband med användandet av HPM mot IED:er.

Energiinnehållet i varje individuell HPM-puls varierar stort mellan olika typer av HPM-källor men överstiger i de flesta fall inte 1 kJ/puls, men då effekten är mycket hög och man vill kunna utnyttja en hög repetitionsfrekvens behövs en plattform som (åtminstone kortvarigt) kan leverera höga elektriska effekter.

5.4 Utveckling av specifika delområden/teknologier

Den pågående utvecklingen av nya metamaterial¹⁶ är intressant för tillämpningar i HPM-källor, exempelvis för att modulera genereringen av mikrovågspulser inuti strålkällan eller för att ändra dielektriska egenskaper hos vågledarfönster.

AESA är en intressant teknik för att skapa smala lobformer, vilket innebär längre verkansavstånd. Om uteffekten från varje antennelement kan ökas någon eller några storleksordningar bör AESA-antennerna kunna åstadkomma störande såväl som förstörande verkan.

För att med HPM-verkan kunna angripa många olika typer av mål är det nödvändigt att HPM-källor konstrueras för att kunna generera flera pulser med olika karaktär. Eftersom känsligheten hos elektronisk utrustning varierar med den infallande strålningens frekvens, polarisation, pulsform (främst stigtid) och varaktighet behöver en HPM-källa kunna generera en lång serie av pulser med olika värden på dessa parametrar. Främst är det en ökad frekvensavstämbarhet och möjligheter till pulsmodulering som är aktuella.

En ökad energiverkningsgrad hos HPM-genererande system skulle innebära vinster i form av minskad vikt, volym och energibehov samt möjligheter att generera mycket långa serier av pulser. Minskad vikt och volym liksom ett mindre energibehov skulle innebära ökade möjligheter till plattformintegrering för fler plattformar och situationer. Långa pulsserier ökar möjligheterna att täcka ett brett frekvensområde med fler pulser.

¹⁶ Artificiella material med egenskaper som inte finns i naturliga material, t.ex. negativa brytningsindex eller omvänd Dopplereffekt. Se t.ex. Kshetrimayum, R.S. "A brief intro to metamaterials", IEEE Potentials Vol. 23, No. 5, December 2004.

Generering av HPM-pulser med olika karaktär kräver att strålkällans fysiska konstruktion kan ändras snabbt under fältmässiga förhållanden. Detta betyder möjligheter att ändra någon eller några geometriska dimensioner mellan pulser eller pulsskurar. För att åstadkomma detta, liksom en ökning av energiverkningsgraden, behövs, för varje typ av HPM-källa, ett omfattande utvecklingsarbete inkluderande såväl simuleringar som experiment.

Med större kännedom om olika måltypers känslighet kan man anpassa frekvens och pulsform för att maximera verkan i den aktuella måltypen. Detta innebär ett steg i utvecklingen av 'smart HPM'. Ett annat steg i denna riktning vore utveckling av möjligheterna att på avstånd detektera funktionen hos målelektronik, det vill säga att mäta upp målelektronikens arbetsfrekvenser, dataflöden m.m. för att anpassa HPM-pulsgenereringen samt sedan efter bestrålning detektera målelektronikens funktion för att kunna konstatera skillnader och därigenom avgöra om avsedd verkan har uppnåtts.

En förutsättning för att kunna göra en sådan taktisk anpassning av genererade HPM-pulser är att man har tillgång till ett stort referensbibliotek innefattande många olika typer av elektronikobjekt. Detta förutsätter en väl utvecklad provningsmetodik och utrustning för att prova elektronik och kompletta systems känslighet över en stor parameterrymd. Omvänt kan den kunskapen användas för att identifiera svagheter i egna elektroniska system och för att utveckla skyddsmetoder.

För att kunna genomföra provning vid hotnivåer, inklusive förstörande verkan, behövs relativt kraftiga provningskällor som kan avstämmas i exempelvis frekvens, uteffekt och pulslängd. Provning kan genomföras i flera steg, först för att finna känsliga frekvenser m.m. hos provobjektet, sedan för att identifiera från vilka riktningar och vid vilka polarisationer som objektet är känsligast, och slutligen för verifiering av verkan under fältmässiga förhållanden.

5.5 Potentiella militära tillämpningar

HPM kan ur telekrigföringsperspektiv ses som en mycket kraftig elektromagnetisk störning för att förhindra fiendens kommunikation, men med potential till förstörande verkan mot all elektronisk utrustning, såväl kommunicerande som icke-kommunicerande.

Användning av telekrigföring och HPM kan skapa förvirring och osäkerhet i ett tidigt skede av en konflikt genom att slå ut civila elektroniska system som kommunikationssystem och distributionsnoder för elförsörjning, vilka ofta är dåligt eller inte alls skyddade mot HPM. Trenden med ökad användning av elektronisk kommunikation, till exempel *Internet of Things* (IoT), gör civilsamhället mycket sårbart för HPM-attacker. Möjligheterna att slå ut civil elektronisk infrastruktur begränsar kraftigt möjligheterna för det civila samhället att stödja Försvarmakten vid en militär konflikt. Enligt vissa uppgifter skedde

detta i Ukraina vid Rysslands intervention 2014.¹⁷ En sådan ‘*electronic knock-down*’ syftar till att passivisera fiendens statsapparat och militära styrkor.¹⁸

HPM är en tyst verkansform, vilket innebär att det kan ta en stund innan den som blir utsatt för HPM förstår att det handlar om en HPM-attack. Detta medför bl.a. att HPM lämpar sig för användning i inledningsskedet av en operation, före insats av andra medel. Det är i få militära operationer som HPM-användning skulle vara det enda angreppsmedlet; oftast ger HPM störst effekt tillsammans med andra verkansformer. Däremot kan sabotageverksamhet, terrorism, m.fl. subversiva användningsområden med fördel nyttja enbart HPM, eftersom detta ger användaren möjligheter att försvinna innan HPM-verkan konstaterats.

Soldatsystem för information, kommunikation och navigering kommer sannolikt att i någon mån vara härdade (skärmade) men kravet på portabilitet och användarvänlighet begränsar möjligheterna att skydda dem. De begränsade möjligheterna till HPM-skydd av elektronisk utrustning i denna tillämpning och i andra installationer med snäva vikt- och volymkrav gör dessa till potentiella mål för HPM-vapen.

HPM har fördelen av en relativt bred strålningslob, vilket gör att man inte behöver rikta strålningen exakt mot en punkt för att kunna träffa ett mål. Detta är intressant för att kunna verka mot svärmar av små luftmål, till exempel UAV:er som genomför en koordinerad attack men med distribuerade uppgifter, det vill säga vissa UAV:er navigerar, andra bär en verkanslast, andra har som uppgift att störa och förvilla. Dessa är svåra att komma åt med konventionella verkansformer. I Ryssland finns planer på att montera en HPM-kanon på Buk-systemets bandgående chassi för luftvärnsapplikation.¹⁹

HPM kan även användas mot elektroniska triggersystem i sprängladdningar, exempelvis IED:er, i såväl militär som civil kontext. Det tyska företaget Diehl studerar bredbandiga HPM-källor för denna tillämpning²⁰.

5.6 Begränsande faktorer

Den fysikaliska begränsningen vad gäller den energi som i en kort puls kan riktas mot målet är luftens genomslagshållfasthet. Genererar man elektriska fält som överstiger denna joniseras luften och strålningen reflekteras. Enda sättet att undvika denna grundläggande fysikaliska begränsning är att använda en stor antennarea eller flera antenner och mikrovågsgeneratorer som arbetar i fas så att strålningen från flera separata enheter kan samverka i målet.

Det faktum att strålningseffekten avtar kvadratiskt med avståndet gör att räckvidden alltid kommer att vara begränsad och ”att hålla ett stort avstånd” mellan

¹⁷ Johnson, R. F. “Update: Russia’s hybrid war in Ukraine is working” IHS Jane’s Defence Weekly, 26 February 2015 & R.D. Thiele, “Crisis in Ukraine – The Emergence of Hybrid Warfare”, ISPSW Strategy Series: Focus on Defense and International Security, Issue No. 347, May 2015, s. 2.

¹⁸ Rácz, A., “Russia’s Hybrid War in Ukraine, Breaking the Enemy’s Ability to Resist”, The Finnish Institute of International Affairs, FIIA report 43, July 2015, s. 39.

¹⁹ Rogulin, D., “Russia’s new ‘microwave cannon’ to disable enemy drones within 10 km radius”, ITAR-TASS, June 15, 2015, <http://tass.ru/en/russia/800636>

²⁰ <http://www.diehl.com/en/diehl-defence/products/sensor-and-security-systems/protection-systems/convoy-protection.html>. (Besökt 2017-06-12).

HPM-källa och det man vill skydda (avspärning med utökat perimeterskydd) kommer alltid att vara ett bra skydd mot HPM.

En begränsande faktor på små plattformar är tillgången till anpassad elektrisk energiförsörjning. HPM-källor behöver matas med korta högspänningspulser med tillräckligt hög toppeffekt, vilket kräver särskild utrustning som upptar viss vikt och volym. För att erhålla en smal strålningslob och därigenom ett långt verkansavstånd behövs det en antenn med stor diameter; ju större desto längre verkansavstånd. Detta begränsar möjligheterna att använda HPM effektivt monterade på mindre robotar.

Det finns inga indikationer på att HPM-pulser avsedda för bekämpning av elektroniska system skulle ha negativ inverkan på människor eller biologiska material, däremot kan HPM-bestrålning av civilbefolkning leda till oro för effekter.

Bristande skydd av egna system kan vara en begränsande faktor vid HPM-användning. Elektronisk utrustning i närheten av HPM-källan kan utsättas för sidolober, så därför måste denna utrustning HPM-skyddas eller sidoloberna begränsas med hänsyn till den taktiska användningen.

5.7 Referenser

“Active electronically scanned array”, Wikipedia,
https://en.wikipedia.org/wiki/Active_electronically_scanned_array (Besökt 2017-03-02).

Blank, S., *A Military Assessment of the Russian War in Ukraine*, American Foreign Policy Council, <http://russialist.org/transcript-a-military-assessment-of-the-russian-war-in-ukraine/>, 2015. (Besökt 2017-06-12).

Counter-electronics High-powered Microwave Advanced Missile Project (CHAMP), <http://www.boeing.com/features/2012/10/bds-champ-10-22-12.page>, 2012. (Besökt 2017-06-12).

Johnson, R. F., *Update: Russia's hybrid war in Ukraine is working*. IHS Jane's Defence Weekly, 26 February 2015.

Kshetrimayum, R.S., “A brief intro to metamaterials”, IEEE Potentials Vol. 23, No. 5, December 2004.

MIL-HDBK-235-8, Hemlig.

MIL-STD-464C, *Department of Defence Interface Standard, Electromagnetic Environmental Effects Requirements for Systems*, Dec 2010.

Protection Systems Convoy Protection, <http://www.diehl.com/en/diehl-defence/products/sensor-and-security-systems/protection-systems/convoy-protection.html> (Besökt 2017-06-12).

Rácz, A., *Russia's Hybrid War in Ukraine, Breaking the Enemy's Ability to Resist*, The Finnish Institute of International Affairs, FIIA report 43, July 2015

Rogulin, D., *Russia's new 'microwave cannon' to disable enemy drones within 10 km radius*, ITAR-TASS, June 15, 2015, <http://tass.ru/en/russia/800636>. (Besökt 2017-06-12).

Thiele, R.D., *Crisis in Ukraine – The Emergence of Hybrid Warfare*, ISPSW Strategy Series: Focus on Defense and International Security, Issue No. 347, May 2015.

6 Hypersoniska system

6.1 Beskrivning av området

Med hypersonisk hastighet avses hastigheter kring eller över fem gånger ljudhastigheten (Mach 5).

Hypersoniska farkoster har förekommit sedan rymdålderns inledning på 1940-talet. Den första hypersoniska farkosten var den tyska V-2-raketen från mitten av 1940-talet. Ett annat tidigt exempel är det amerikanska X-15, som var ett raketdrivet flygplan som flögs på 1960-talet och nådde farter om Mach 6,7 och höjder om 100 km.

Den vanligaste formen av framdrivning för höga hastigheter har varit raketmotorn. För X-15-flygplanet gav raketmotorn en hastighet om 2000 m/s och för Apollofärdena och andra rymdfarkoster har det handlat om hastigheter upp till 11000 m/s. I militära sammanhang är ballistiska robotar de enda egentliga exemplen på hypersoniska farkoster – samtliga drivna av raketmotorer.

Förhållandena vid flygning beror mycket starkt på farten som den aktuella farkosten flyger med. Vid överljudshastigheter bildas stötvågor som gör att aerodynamiken ändrar karaktär och vid hastigheter omkring fem gånger ljudhastigheten, det vill säga Mach 5 eller ungefär 1700 m/s, inträffar ett antal fenomen som gör att själva luften ändrar egenskaper.

De två största problemområdena vid flygning med hypersonisk hastighet är framdrivning och uppvärmning. Vid hypersoniska hastigheter upphör dagens luftförbrukande motorer (ramjet) att fungera och alla hypersoniska farkoster fram till för några år sedan har därför varit utrustade med raketmotorer.

6.2 Övergripande trender fram till 2035

Intresset för flygfarkoster med höga hastigheter har länge varit stort, men det har inte varit möjligt att helt lösa problemen med framdrivning och uppvärmning. Det finns åtminstone två drivkrafter bakom utvecklingen av hypersoniska farkoster. En uppenbar anledning är att minska tiden från start till mål, vilket är intressant både för militära ändamål och för passagerarflyg. En annan anledning för militära ändamål är att minska möjligheterna för motståndarens luftförsvar att ingripa mot farkosten.

Den senaste tidens tekniska framsteg, som huvudsakligen baseras på komplexa datorsimuleringar av hypersonisk strömning och tillhörande förbränningsförlopp, har lett till att hypersoniska vapen och andra farkoster har kommit närmare en realisering. Hypersoniska kryssningsrobotar kommer sannolikt att introduceras omkring 2025 och såväl bemannade som obemannade flygplan strax efter 2030. Exempelvis är ett nytt hypersoniskt strategiskt spaningsflygplan, SR-72, under utveckling vid Lockheed Martin och beräknas tas i tjänst efter 2030.

6.3 Koppling till andra teknikområden och krav på dessa

Viktiga forskningsområden för framdrivning för hypersoniska hastigheter är framförallt beräkningsfysik i kombination med experiment, men även materialteknik och sensorteknik för höga temperaturer är viktiga områden.

6.4 Utveckling av specifika delområden/teknologier

Framdrivning är det viktigaste teknikområdet för att uppnå hypersoniska hastigheter. Det finns flera möjliga motortekniker för att åstadkomma detta.

Raketmotorer använder inte syret i luften för förbränningen, vilket innebär att de har hög dragkraft oberoende av omgivande luft, men också att de måste bära med sig både bränsle och oxidator.

En effektivare form av motor är ramjet, som använder luftens syre till förbränningen. I en ramjet bromsas luften upp så att förbränningen sker i underljudshastighet inne i brännkammaren. Uppbromsningen av luften ger dock förluster, vilket begränsar den maximala hastigheten till omkring Mach 4. Ramjet används bland annat i jaktroboten Meteor, som nyligen introducerats till JAS 39.

För att nå högre hastigheter kan scramjet (*supersonic ramjet*) användas. I scramjet bromsas luften inte upp lika mycket och förbränningen sker i en gasblandning som strömmar i överljudsfart. Idéer om scramjet har funnits i många år, men har varit svåra att realisera.

Förbränningsförloppen i överljudsströmning är ytterligt komplicerade och instabila, varför utvecklingen inom avancerad beräkningsfysik kopplad till experiment har varit helt nödvändig för att ge tillräcklig insikt i problematiken.

Under det senaste decenniet har ett antal experimentfarkoster med scramjet flugits. Den första lyckade flygningen gjordes 2002 i Australien av en grupp ledd av University of Queensland. Deras *HyShot* flög under 6 sekunder i en hastighet om Mach 7,6.

X-43 var ett litet obemannat amerikanskt flygplan med scramjet med vätgas som bränsle. X-43 flög 2004 och satte då ett nytt hastighetsrekord för flygfarkoster om Mach 9,6 eller 11000 km/h. Nästa amerikanska experimentflygplan använde scramjet med vanligt flygbränsle. X-51 gjorde sin första lyckade flygning 2013 och nådde då Mach 5 under 210 sekunder.

Scrammotortekniken anses nu vara tillräckligt utvecklad för att utnyttjas i serieproducerade robotar. Idag bedrivs utveckling av hypersoniska attackrobotar i åtminstone USA, Ryssland och Indien samt troligen i Kina.

Den amerikanska *High Speed Strike Weapon* (HSSW) bygger på X-51 och bedöms tas i tjänst under den senare halvan av 2020-talet. HSSW ska kunna bäras internt av F-35 och B-2 och ha en hastighet som överstiger Mach 5.

I Ryssland utvecklas sjömålsroboten *Zirkon* som det finns mycket begränsad information om. Den rysk-indiska *BrahMos II* anses dock vara en exportversion av *Zirkon* med kortare räckvidd. *BrahMos II* är planerad att flyga under 2017 och ska ha en toppfart om Mach 7 och en räckvidd om 290 km.

Hittills har alla scramjetdrivna farkoster använt raketmotor för att nå tillräcklig starthastighet, det vill säga omkring Mach 5. För en robot är detta fullkomligt acceptabelt, men för bemannade eller obemannade flygplan vore det önskvärt med en motor som kunde ändra sin funktion för att möjliggöra såväl start och landning som hög marschhastighet på hög höjd.

Forskningen kring scramjet är idag inriktad mot att dels öka tillförlitlighet och prestanda, dels ta fram motorer som kan möjliggöra en hel flygning med start och landning.

Ett alternativ till scramjet är detonationsmotorer. I alla befintliga förbränningsmotorer sker förbränningen relativt långsamt i form av deflagration²¹, men i en detonationsmotor sker förbränningen mycket snabbt i form av en detonation. Under detonationen hinner gaserna inte expandera, vilket gör att förbränningen sker under högt tryck och hög termodynamisk effektivitet. Att gå från effektiv förbränning till en effektiv motor har visat sig vara svårt.

Pulsdetonationsmotorn (PDE) delar grundläggande idé med den enkla pulsjetmotorn som fanns på V-1, den första jetdrivna kryssningsroboten. En första flygning med ett obemannat flygplan med PDE gjordes 2008.

En annan typ av detonationsmotor använder roterande eller kontinuerlig detonation. Den tekniken finns idag bara i simuleringar och laboratorier, men den skulle kunna ge motorer med hög effektivitet över stora hastighetsområden.

6.5 Potentiella militära tillämpningar

Den militära effekten av hypersoniska system kan vara mycket stor. Hypersoniska farkoster med lång räckvidd skulle kunna nå alla punkter på jorden inom någon eller några timmar. Hypersoniska attackrobotar skulle vara mycket svåra att motverka med luftförsvarssystem och hypersoniska luftmålsrobotar skulle vara en mycket stor fördel i luftstrid eftersom de skulle vara svåra att fly undan ifrån.

6.6 Begränsande faktorer

Uppvärmning är ett centralt problemområde för hypersoniska farkoster. Vid all flygning ger luftmotståndet upphov till uppvärmning, men vid hypersoniska hastigheter blir uppvärmningen mycket kraftig. Apollokapslarna hanterade uppvärmningen med en värmesköld som förgasades och därigenom tog upp och förde bort värmen. Rymdskytteln hade isolerande keramikplattor för att skydda mot värmen. Spaningsplanet SR-71 som utvecklades på 1960-talet flög i det här sammanhanget bara i drygt Mach 3, men cirkulerade bränsle för att kyla ner cockpit och andra utsatta ytor.

Hypersoniska farkoster måste byggas i värmeståliga material för att klara den strukturella hållfastheten. Därtill kommer problematiken med att de olika systemen ombord måste kunna hantera värmen. Detta gäller inte minst olika sensorer som till exempel robotmålsökare.

²¹ Deflagration sker när reaktionszonen i ett explosivämne (till exempel krut) breder ut sig i ämnet med mindre än ljudets hastighet. (Wikipedia)

6.7 Referenser

Critical Technologies for Hypersonic Vehicle Development, NATO RTO-EN-AVT-116, December 2006.

Musielak, D.E. & Saracoglu, B.H., *Soaring at Hypersonic Speeds – 2015 Status of High Speed Air Breathing Propulsion*, AIAA HSABP, December 2015.

Panday, K.M. & Debnath, P., *Review on Recent Advances in Pulse Detonation Engines*, Journal of Combustion Volume 2016, 2016.

“Lockheed Martin Wins Hypersonic Plane Research Contract worth \$147 Million”, International Business Times, 2016-09-20.

“Tactical Boost Glide (TBG)”, DARPA, <http://www.darpa.mil/program/tactical-boost-glide>. (Besökt 2017-06-12).

7 Informationsteknologi

7.1 Beskrivning av området

Informationsteknologi (IT) är ett samlingsbegrepp för teknologi som är avsedd att hantera och bearbeta information.²² Särskilt åsyftas den informationshantering och -bearbetning som åstadkoms med datorer, datornätverk och datorprogramvara, där datorer utöver konventionella persondatorer även inbegriper styrsystem, databasservrar, övervakningssystem, mobiltelefoner m.m. Mycket av den informationsbehandling som avses sker idag ”online”, vilket behandlas särskilt i kapitlet om cyber. För att undvika överlapp kommer därför vissa aspekter av internetanslutna system och de möjligheter och problem dessa medför att behandlas förhållandevis kortfattat nedan.

En stor mängd av de produkter (exempelvis fordon, telefoner och kameror) som kommer ut på marknaden idag innehåller någon typ av IT-system. Utvecklingen av *Internet-of-things* innebär dessutom att informationsteknologi implementeras i kylskåp, kaffeautomater, dörrlås, klimatanläggningar och allt annat som kan tänkas behöva beräkningskraft och lagringsförmåga för att tillhandahålla bättre funktionalitet. Datorers förmåga att spara, hantera och analysera data ligger till grund för en stor del av vår teknologiska utveckling de senaste 50 åren. Det finns anledning att anta att IT kommer att spela en än större roll i framtiden eftersom IT påverkar hela samhället.

7.2 Övergripande trender fram till 2035

Utvecklingen inom IT har de senaste decennierna varit extremt snabb och har i stor utsträckning styrts av enskilda tekniska genombrott, både på hårdvaru- och mjukvarusidan. Att förutse trender på lång sikt är av det skälet svårt, men i detta avsnitt listas några mer övergripande trender som kan ses i samhället redan idag.

7.2.1 Ökad sammankoppling av IT-system

En tydlig trend i samhället är att mängden tillgänglig information ständigt ökar och att olika informationssystem i allt större utsträckning kopplas ihop med varandra – direkt eller indirekt. Sammankoppling av olika informationssystem ger enorma möjligheter för både privatpersoner och företag att optimera och planera. Den uppenbara nackdelen är att samhällets sårbarhet för haverier, systemfel och IT-attacker ökar drastiskt.

7.2.2 Analysprogram ersätter människor

En trend inom IT är att överlåta mer och mer databehandling och analys till datorer, ungefär som att man i den fysiska världen har överlåtit mycket av arbetet till maskiner och robotar. Några av de främsta anledningarna är att datorer är snabba, har perfekt minne och enorm beräkningskraft som ökar för varje år. Den

²² Andersson, J., Astell, M., Axberg, S., Brehmer, B., Brynielsson, J., Hagstedt, D. S., Nylander, M., Reberg, M., Sivertun, Å., *Teknik till stöd för ledning*, band 3 av *Lärobok i Militärteknik*, kapitel 7 ”Informationsteknik”, ss 117–143. Försvarshögskolan, Stockholm, 2009.

förmåga som fram till nu i mångt och mycket har saknats hos datorer är förmågan att kunna fusionera olika typer av information och analysera betydelsen av den på en hög abstraktionsnivå. På senare år har stora framsteg gjorts inom just analysförmågan hos datorer. Idag kan datorer användas för att transkribera tal till text och översätta mellan olika språk i realtid, men också för att analysera text, sammanfatta rapporter, skapa rapporter etc. Datorers förmåga att kunna utföra typiskt mänskliga aktiviteter – ”tänka” – brukar benämnas artificiell intelligens (AI).²³

AI är ett mycket aktivt forskningsområde och det finns redan idag exempel på mycket avancerade analyssystem som inom vissa områden klarar att prestera bättre än en människa. Ett exempel är IBM:s AI-system Watson.²⁴ Generellt är den här typen av system (ofta refererade till som expertsystem) ännu inte tillräckligt pålitliga för att kunna ersätta en mänsklig expert, utan används främst som stöd och komplement. Man kan emellertid förvänta sig att de förmågor som nämnts ovan successivt kommer att förfinas och förbättras till en nivå där datorprogram helt kan ta över vissa förhållandevis avancerade analysuppgifter som idag måste utföras manuellt.

7.2.3 Robotar och autonoma system blir en del av vardagen

En utveckling som kan förväntas de kommande 20 åren är att datorer och maskiner i större utsträckning kommer att interagera med människor i den fysiska världen. Datorer används allt mer för att kontrollera olika typer av fordon (med autopiloter i flygplan och självkörande bilar som kända exempel), och enkla hushållsrobotar har redan idag gjort sitt intåg i våra hem i form av dammsugare och gräsklippare.

En stor anledning till att robotar och autonoma system ännu inte förekommer i samhället i större utsträckning är att de inte kan hantera kontext och situationer lika bra som människor, och att de därför inte klarar att anpassa sig till en föränderlig omvärld tillräckligt bra. Rent tekniskt handlar det både om att förmågan att tolka sensordata, framförallt bilder, behöver förbättras och att förmågan till en mer generell situationsförståelse måste utvecklas. Det finns också juridiska och etiska aspekter som begränsar de möjliga användningsområdena. På de tekniska områdena görs idag stora framsteg.

7.2.4 Människan som en del av nätverket

En möjlig – om än spekulativ – utveckling av IT på längre sikt är att människan kopplas samman med ett IT-system och blir en del av ett nätverk. Idén att sätta in mikrochips i kroppen, som till exempel möjliggör lättare identifiering, har funnits i många år och det finns redan idag proteser som är sammankopplade med det mänskliga nervsystemet. I förlängningen kan man tänka sig en utveckling där gränsen mellan dator och människa blir allt mer diffus, och där till exempel tekniska hjälpmedel används för att förstärka de mänskliga

²³ Gisslén, L., *Artificiell intelligens: Teknisk prognos*. Teknisk rapport FOI-R--3919--SE, 2014.

²⁴ <http://www.nyteknik.se/digitalisering/hajpade-superdatorn-lar-sig-svensk-ward-6780133>. (Besökt 2016-09-07).

sinnesintrycken. En sådan utveckling kan till del vara etiskt kontroversiell, men ur teknisk synvinkel fullt möjlig.²⁵

7.3 Utveckling av specifika delområden/teknologier

I detta avsnitt beskrivs ett antal områden som kan komma att få särskild betydelse för forskning och utveckling med avseende på försvarstillämpningar under de kommande två decennierna.

7.3.1 Automatisk textanalys och artificiellt resonerande

I och med datorernas intåg i samhället kunde stora mängder text göras sökbar på ett sätt som tidigare inte var möjligt. Datorernas användningsområden begränsade sig länge till enklare informationshantering såsom att sortera bland stora mängder data och matcha sökord med data som fanns i systemet. Utvecklingen på senare år har gått mot att bearbeta informationen ytterligare så att den blir mer relevant för användaren. Stora framsteg har gjorts inom textanalys och automatiserat resonerande. Ett bra exempel är den sökfunktion som Google tillhandahåller. När användaren skriver in ett ord eller en fras i sökfältet försöker de underliggande algoritmerna förstå vilken information användaren är intresserad av genom att titta på såväl de enskilda orden som kontexten. Informationen som sökmotorn hittar rangordnas utifrån bedömd relevans, där relevansen avgörs av olika kriterier, till exempel hur viktig informationen är för andra användare. Även om det i slutändan är användaren som avgör vilken information som är mest relevant förenklas sökprocessen avsevärt av den avancerade sökfunktionen.

Exemplet ovan illustrerar väl hur datorprogram kan fungera som beslutsstöd åt en mänsklig användare. Programmet assisterar användaren genom att sortera, filtrera och visualisera information, men i slutändan ligger det på den mänskliga användaren att fatta ett beslut och agera på informationen.

7.3.2 Automatisk bildanalys

Att få datorer att tolka information som tillhandahålls i form av bilder har länge varit en utmaning. Ett stort steg framåt kom med introduktionen av *deep learning*, en teknik inom området maskininlärning/AI. I dagsläget kan man få datorer att med viss säkerhet klassificera vissa typer av objekt i en bild. Vissa system klarar till och med att beskriva innehållet i en bild med en enkel mening.²⁶ Osäkerheten i denna typ av klassificeringar är dock fortfarande stor och tekniken är ännu så länge framförallt användbar inom begränsade domäner, där datorn kan lära sig känna igen ofta återkommande situationer. Datorer kan med liknande teknik även lära sig känna igen ansikten, tal och röster. Det är inte otänkbart att en dator inom en snar framtid kan skapa sig en situationsförståelse som i vissa avseenden liknar en människas genom att betrakta omvärlden med en kamera, eventuellt i kombination med andra sensorer.

²⁵ Att bara ge personer som hör eller ser dåligt syn och hörsel tillbaka är knappast särskilt kontroversiellt, men andra möjligheter som teknikutvecklingen medger kan vara det.

²⁶ Karpathy, A., Fei-Fei, L., *Deep visual-semantic alignments for generating image descriptions*.

7.3.3 Kryptering

Att kryptering fungerar är en grundförutsättning för vårt ständigt uppkopplade samhälle. Skulle dagens kryptering knäckas skulle exempelvis banksystemet omedelbart kollapsa. Samma öde skulle drabba alla andra teknologier som är beroende av kryptering såsom e-post, telefontrafik, webbsidor, databaser.

RSA-kryptering och liknande varianter av de så kallade asymmetriska kryptosystemen används idag i stor utsträckning för säker dataöverföring, datalagring m.m. Liksom många krypteringsmetoder förlitar sig RSA på asymmetri med avseende på svårighetsgraden att utföra en beräkning jämfört med att reversera den. RSA-kryptering använder sig av asymmetrin i multiplikation där det är lätt att multiplicera ihop två primtal (med dagens teknik görs det på bråkdelen av en sekund), men svårt att efteråt dela upp det sammansatta talet i dess två primtalsfaktorer (inversen av multiplikation utgörs således av att finna den unika faktoriseringen bestående av de två primtalen som använts för multiplikationen).

Tekniken använder en publik nyckel (produkten av de två stora primtalen) för att kryptera ett datapaket. För att dekryptera krävs det kännedom om vilka de två individuella primtalen (den privata nyckeln) är. Det är bara den som har den privata nyckeln som kan dekryptera ett meddelande. Med dagens teknik är det i princip omöjligt att efteråt beräkna (faktorisera) de två primtalen som använts vid multiplikationen, vilket innebär att bara den som redan vet de två primtalen kan dekryptera datapaketet. Eftersom svårigheten att faktorisera växer med storleken på de ingående primtalen så går det att välja primtal så att faktorisering inte blir möjlig inom överskådlig framtid.

De algoritmer som faktorerar primtal idag ser inte ut att kunna bytas ut mot väsentligt snabbare motsvarigheter, utan man förlitar sig på att det inte kommer att uppfinnas en överlägsen algoritm före 2035. Ett forskningsgenombrott som gör det möjligt att konstruera en tillräckligt generell så kallad kvantdator skulle helt förändra detta. Med en sådan massivt parallell dator skulle faktoriseringar kunna åstadkommas lika smärtfritt som själva krypteringen och därmed skulle redan färdigutvecklade algoritmer för kvantberäkningar kunna användas för att knäcka många av dagens asymmetriska krypteringssystem.²⁷

7.3.4 Skadlig mjukvara

Det är ett väl känt faktum att IT-system är sårbara för attacker från fientlig mjukvara. Sådan mjukvara går under benämningar som virus, trojanska hästar och maskar, beroende på dess uppbyggnad. Trenden är att skadlig mjukvara blir mer och mer avancerad. Stuxnet är troligtvis den mest kända sofistikerade skadliga koden i dagsläget. Stuxnet ger en indikation om att framtida attacker kommer att använda sig av tekniker som konventionell krigföring använder sig av idag med avseende exempelvis på kamouflage, vilseledning och riktade attacker.

Skadlig mjukvara kan med dagens ihop- och uppkopplade system orsaka stor skada på kort tid. Det är därför av största vikt att såväl företag som myndigheter

²⁷ Amselem, E., Svenson, P., Gisslén, L., *Kvantinformatik*. Teknisk rapport FOI-R--3920--SE, 2014.

får resurser att både följa utvecklingen på detta område och möjlighet att utveckla motåtgärder i samma takt.

7.4 Potentiella militära tillämpningar

De delområden/teknologier som beskrivs i föregående avsnitt är alla intressanta ur militär synvinkel eftersom de kan ingå som komponenter i mer omfattande system med specifika tillämpningsområden. Några exempel ges nedan.

7.4.1 Beslutsstödsystem

Eftersom information används som underlag för beslut i såväl civila som militära operationer är det nödvändigt att kunna hantera och analysera informationen löpande. Då datamängderna kan vara stora är det nödvändigt med tekniska hjälpmedel i form av analys-/beslutsstödsprogram. Olika typer av analysprogram kan användas inom exempelvis logistikplanering, sårbarhetsanalys, uppgiftsfördelning/optimering under strid, hotanalys och resursplanering.

Analysprogram kan också användas för att utföra mindre sofistikerade analysuppgifter så att mänskliga resurser kan utnyttjas till annat. Ett exempel är övervakning, där det är till stor hjälp att automatiskt kunna känna igen situationer och händelser utifrån bilder, videoströmmar och andra media.

7.4.2 Autonoma fordon

I militär kontext kan autonoma eller semi-autonoma fordon användas för spaning, transporter och i strid. Obemannade fordon som opererar över större avstånd behöver ha ett visst mått av autonomi inbyggt för den händelse att kommunikationen med basen bryts. Vidare är det resurseffektivt att kunna förflytta exempelvis en kolonn med transportfordon genom att aktivt navigera ett fordon och låta de övriga följa efter med hjälp av lokal självstyrning. När det gäller användande av autonoma fordon i strid återstår många etiska frågor att ta ställning till.

7.4.3 Övning och träning

Spel och simuleringar används i allt större omfattning som hjälpmedel vid träning av bland annat brandmän, poliser och militär personal. I en virtuell verklighet kan man träna scenarier som av praktiska eller ekonomiska skäl inte är möjliga att öva i verkligheten. Det kan till exempel handla om strid i främmande miljöer eller krissituationer där skaderisken är för hög för att man ska kunna träna säkert i verkligheten.

För att övningar i en virtuell verklighet ska upplevas som realistiska krävs inte bara att den simulerade världen ser verklig ut, utan också att aktörerna, agenterna som befolkar den, uppvisar ett lagom intelligent beteende. Ett alternativ är att låta alla personer i den simulerade världen styras av verkliga människor, ett annat alternativ är att datorgenerera beteenden för åtminstone de personer i den simulerade världen som är mindre centrala. För att kunna återskapa ett trovärdigt mänskligt beteende hos de automatgenererade aktörerna är utvecklingen inom AI central.

Även autonoma system som ska användas i verkligheten kan tränas med hjälp av simuleringar.

7.4.4 IT-attacker

Att kunna skydda sig mot IT-attacker är nödvändigt inom i princip all militär verksamhet. Skyddet innefattar säker kryptering såväl som möjligheter att detektera och motverka skadlig kod.

7.5 Begränsande faktorer

Utvecklingen inom IT har de senaste åren gett upphov till ett stort antal etiska och juridiska utmaningar. Det handlar bland annat om integritetsproblem som uppstår vid hantering av personrelaterade data, och frågan om vem som har det juridiska ansvaret för eventuella (materiella eller immateriella) skador som uppstår vid användningen av autonoma IT-system. De uppkomna problemen bromsar den tekniska utvecklingen, dels genom att forskning inom vissa områden försvåras, dels genom att användandet av vissa teknologier begränsas av lagar och överenskommelser. Att det behövs ett juridiskt regelverk som styr användandet av viss teknik är de flesta instanser överens om. Exakt hur regelverket ska se ut är däremot betydligt svårare att enas om.

Många av de områden som nämns i detta kapitel är fortfarande förhållandevis outvecklade. Som inom all forskning gäller att oväntade problem kan uppstå och att resultaten inte alltid blir de förväntade.

7.6 Referenser

Amselem, E., Svenson, P., Gisslén, L., *Kvantinformatik*. Teknisk rapport FOI-R--3920--SE, 2014.

Andersson, J., Astell, M., Axberg, S., Brehmer, B., Brynielsson, J., Hagstedt, D. S., Nylander, M., Reberg, M., Sivertun, Å., *Teknik till stöd för ledning*, band 3 av *Lärobok i Militärteknik*, kapitel 7 "Informationsteknik", ss 117–143. Försvarshögskolan, Stockholm, 2009.

Gisslén, L., *Artificiell intelligens: Teknisk prognos*. Teknisk rapport FOI-R--3919--SE, 2014. <http://www.nyteknik.se/digitalisering/hajpade-superdatorn-lar-sig-svensk-var-d-6780133>. (Besökt 2016-09-07).

Karpathy, A., Fei-Fei, L., *Deep visual-semantic alignments for generating image descriptions*. i: Proceedings of the 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2015), ss. 3128–3137, Piscataway, New Jersey, june 2015. IEEE.

8 Laser

8.1 Beskrivning av området

Laserbaserade system kan användas för många olika tillämpningar, exempelvis för att upptäcka optiska och elektrooptiska sensorer, för att blända, störa, eller förstöra dessa sensorer, för avståndsmätning, för högupplöst 3D-avbildning och som vapen för att bekämpa mål.

Laservapen har under lång tid tillmätts stort intresse för försvarstillämpningar. Omfattande studier av såväl verkans- som skyddsprinciper har bedrivits i den svenska försvarssektorn i flera decennier. Under 1990-talet bedrevs omfattande studieverksamhet om laservapensystem och skydd mot laserstrålning.

De framtida tillämpningar som då bedömdes finnas har inte realiserats i den takt som ansågs trolig. Detta beror i huvudsak på en för positiv bedömning av teknologiutvecklingen, särskilt avseende högeffektlasrar. Under senare tid har industritillämpningar med den snabba utvecklingen av diodpumpade fastatillstånds- och fiberlasrar påskyndat utvecklingen av taktiska laservapen. Andra faktorer som påverkat utvecklingen är de krav som ställs på stödjande teknikområden, till exempel kraftförsörjning av systemen, och ett identifierat behov av analyser av etisk, medicinsk och legal natur. Bland annat har konventionen om särskilt inhumana vapen en särskild del som förbjuder laservapen med uttalat syfte att skada ögon.

Laservapen brukar räknas till kategorin icke dödande vapen, det vill säga vapen som kan bekämpa ett mål med graderad verkan utan att permanent slå ut det. Exempel på detta är laservapensystemens möjlighet att utöver strukturförstörande verkan även kunna blända sikten och målsökare.

8.2 Övergripande trender fram till 2035

Utvecklingen av laservapen har dominerats av USA, där ett antal avancerade system utvecklats och demonstrerats under de senaste decennierna. Ett exempel på ett sådant är *Airborne laser* (ABL), där en avancerad kemisk laser placerades i en Boeing 747 med syfte att bekämpa ballistiska robotar redan i ”boost”-fasen. Svårigheterna att uppnå nödvändiga verkansavstånd och de höga kostnaderna ledde till att projektet avbröts för några år sedan. Även ett antal andra amerikanska laserprogram baserade på kemiska lasrar har avbrutits.

På senare år har tekniskt fokus för taktiska laservapentillämpningar skiftat från kemiska lasrar till fasta tillståndslasrar. Sådana kan göras mycket mer kompakta och ändå leverera höga effekter, dock ännu inte i nivå med de effekter som kan uppnås med kemiska lasrar.

Många av de demonstratorer som har tagits fram på senare tid bygger på kommersiellt tillgängliga fiberlasrar, som är kompakta, har hög effektivitet och stor yta per volymsenhet. Ett exempel är den markbaserade demonstrator som tagits fram av det tyska företaget Rheinmetall. I detta fall har man utnyttjat ett befintligt vapenstativ och ersatt kanonen med fiberlasrar.

Samtidigt har tillämpningsfokus för laservapen skiftat från strategiska (exempelvis ABL) till mer taktiska tillämpningar, till exempel som mark- eller fartygsbaserat luftförsvar.

Ett antal utvecklingsprogram pågår, med syfte att integrera laservapen på plattformar. Bland dessa kan nämnas *High Energy Laser Demonstrator* (för markfordon) och *Maritime Laser Demonstrator* (för fartyg).

En alternativ laserteknologi är frielektronlasern (FEL), där elektroner accelereras i en elektronaccelerator. Frielektronlasern har högre effektförbrukning än fasta tillståndslasrar, men kan ge högre stråleffekt, varierbar frekvens (våglängd) och även möjliggöra kontinuerlig strålning. Effektbehov och storlek kan begränsa system baserade på frielektronlasrar till användning på stora plattformar (främst fartyg).

Laservapens kostnadsbild skiljer sig från andra vapensystem genom att utveckling och anskaffning av själva vapnet är den stora kostnaden medan kostnaden per insats sedan är låg jämfört med andra system.²⁸ Ett krav är dock att plattformen kan energiförsörja laservapnet. Så länge det är möjligt är ammunitionsmängden för laservapnet ”obegränsad”.

Högenergilasrar är inte en mogen teknologi ännu. Bland annat energiförsörjning och termiska effekter kräver mer arbete, men de första systemen börjar bli preoperativa på den marina arenan.

Inom 5-10 år bedöms system som kan utnyttjas för att försvara baser mot attacker från RAM-hot, det vill säga granater och raketer, samt marina plattformar mot små snabbgående ytfarkoster och mindre lufthot som UAV:er, kunna vara operativa. Fasta tillståndslasrar är här sannolikt den mest lovande tekniken.

På längre sikt (10-20 år) bedöms volym och vikt hos system baserade på fasta tillståndslasrar komma att reduceras liksom behovet av kylning. Detta skulle kunna möjliggöra implementering i markfordon och små flygplan. I detta tidsperspektiv kan det också vara möjligt att implementera frielektronlasrar på fartyg, vilket skulle kunna ge effekt mot hårdare mål än vad som är möjligt med fasta tillståndslasrar.

Om laservapen blir talrika kommer de potentiella målen för dessa med stor sannolikhet att vidta motåtgärder. Sådana kan handla både om hur de manövrerar (genom att rotera kan målet tvinga lasern att belysa det en längre tid), att använda reflekterande ytor eller att använda ytbeläggningar som skapar ett skyddande plasma när de belyses med laserstrålning.

8.3 Koppling till andra teknikområden och krav på dessa

Lasersystem ställer stora krav på energiförsörjning. Utvecklingen inom områden som energigenerering och energilagring är därför av betydelse för utvecklingen av högenergilasrar. Detta är en särskilt stor utmaning för system avsedda att placeras på markfordon eller flygplan. I dessa fall kan batterier som i sin tur laddas av små generatorer vara en möjlighet.

²⁸ Enligt uppgift mindre än en dollar (USD) för systemet LaWS, som bygger på en 30 kW laser.

Andra viktiga teknikområden är de som kan bidra till att forma strålen (exempelvis adaptiv optik), upptäcka och följa mål samt kyla lasersystemen.

8.4 Utveckling av specifika delområden/teknologier

Som nämnts ovan kommer utvecklingen av diodpumpade fasta tillståndslasrar och fiberlasrar troligtvis att medge mindre kompaktare enheter (moduluppbyggda) med högre verkningsgrad. En annan typ av laser av intresse för laser-vapentillämpningar är en vätskelaser som utvecklas av DARPA i USA. I dagsläget utnyttjas enbart inkoherent kombinerings²⁹ av laserstrålar. I framtida system bedöms strålar kunna adderas koherent vilket medför högre intensiteter och längre räckvidder. Även utveckling av teknologier för att kompensera för atmosfärsstörningar, som idag reducerar prestanda, kommer successivt att utvecklas.

8.5 Potentiella militära tillämpningar

De mest relevanta tillämpningarna av laser som vapen är skydd av fasta installationer och olika plattformar (mark-, sjö- och luftplattformar).

Den huvudsakliga användningen för en högenergilaser för fartygsbaserad är rimligen som kort- och medelräckviddigt luftvärnssystem. Atmosfäriska effekter på strålutbredningen minskar effekten på längre avstånd. Möjliga mål för lasern kan vara sensorer, små flygplan och obemannade flygande plattformar (UAV:er), snabba patrullbåtar, robotar, minor och granater. Lasern kan även skada infrastruktur längs kuster, till exempel kraftledningar. Ett laserluftvärn kan vara särskilt effektivt, relativt andra luftvärnssystem, när hoten kommer i svärmar. Några styrkor hos lasersystem är en strålstyrka som kan varieras efter behov, vilket möjliggör graderad effekt, kort reaktionstid samt förmåga att engagera flera mål samtidigt. Ett laserbaserat luftvärn kan därför vara svårare för motståndaren att mäta.

8.6 Begränsande faktorer

Lasersystem kräver en klar siktlinje till målet. Atmosfäreffekter (absorption, spridning, turbulens) och väder påverkar också effekten. Att sikta är också en utmaning då strålningen måste koncentreras på målet för att kunna bekämpa detta. Detta kräver precis följning och inriktning.

Motåtgärder för att begränsa verkan från ett laservapen kan vara att utnyttja reflekterande ytor, förgasande skikt eller målrörelse. Här ska givetvis motåtgärden ställas i relation till bland annat laserintensiteten och vid en ökning av intensiteten kan effekten reduceras. Området är dock viktigt och här behöver kunskap byggas upp för att verkanseffektivitet ska kunna bedömas på ett realistiskt sätt. Erfarenheter kring dessa frågor har oftast en hög sekretessnivå.

Enligt ovan förbjuds lasersystem med avsedd effekt mot ögon av en särskild internationell konvention. Denna förbjuder dock inte skador på ögon när lasrar

²⁹ Vid inkoherent strålkombinering tar man inte hänsyn till fasskillnader mellan strålarna utan adderar intensiteter. Vid koherent strålkombinering kan faser optimeras mellan strålarna och man kan kontrollera fasskillnader.

används för andra syften. Sådana risker torde också finnas när laserstrålning med mycket hög effekt sänds ut från högenergilasrar och reflekteras.

8.7 Referenser

Emerging Technology Concepts and Defence Planning in the Nordic Countries, FFI Externnotat 16/00336, February 2016.

Henrikson, M. och Sjöqvist, L., *Laserteknologier för telekrigstillämpningar - En översikt av teknikutvecklingen*, FOI-R--4089--SE, Juni 2015.

High-Energy Solid-State Laser Weapons, 11FMV2150-22, 2011-08-31, underlag från Fraunhofer INT till Teknisk Prognos.

Larsson, A., Akyuz, M., Nyholm, S. E. och Sjöqvist, L., *Elektriska vapen på stridsfältet – Litteraturöversikt rörande elektrifiering av plattformar, elektromagnetisk utskjutning och taktiska laservapen*, FOI-R--3962--SE, December 2014.

9 Obemannade/autonoma system

9.1 Beskrivning av området

Obemannade system har länge varit en realitet och förekommer i luft, på mark och till sjöss. De kan vara direkt fjärrstyrda eller kontrollerade med automatiska funktioner som tillåter olika nivåer av högnivåstyrning. Utvecklingen har gått fort de senaste decennierna och tekniken är idag inte längre förbehållen högteknologiska statliga aktörer.

Idag ökar också möjligheterna att snabbt göra plattformar fullt autonoma, det vill säga att de potentiellt kan verka helt utan att bli styrda av en operatör och med förmåga att anpassa sig till förändringar i omvärlden. Till exempel förs det diskussioner om framtida fordon på våra vägar ska vara helt autonoma och fordonstillverkare testar fordon med viss grad av autonomt uppträdande. Den civila marknaden bedöms komma att vara drivande för efterfrågan av teknik för autonoma system, men militära behov kommer att ställa särskilda krav avseende bland annat tillförlitlighet, robusthet och säkerhet. Dessutom kommer vissa militära tillämpningar att sakna direkta civila motsvarigheter, vilket visar på behovet av försvarsegen forskning och utveckling.

Ett exempel på ett existerande civilt fordon är de två självkörande bussar som testats under ca en månad (augusti-september 2016) på allmänna vägar i Helsingfors, ett annat att Ubers försök med självkörande taxibilar³⁰. Liknande tester har genomförts, pågår eller planeras även på andra håll. För att kunna navigera används kombinationer av kameror, radar, lidar³¹ och GPS. Oftast finns en person (hjälpförare) ombord som vid behov kan stoppa fordonet manuellt.

Även för försvarstillämpningar genomförs tester av mer eller mindre autonomt uppträdande fordon. Exempelvis har tester genomförts med logistikkolonner där det första fordonet är bemannat och styr de övriga fordonen i kolonnen.

Obemannade system används redan idag av (alla) tänkbara motståndare och är därför ett hot mot våra förband var vi än uppträder. Kvalificerade system är dyra, men det finns system som kan vara billiga och tillgängliga för till exempel irreguljära aktörer. Obemannade system ställer också nya krav på organisationen och existerande system.

Obemannade flygande plattformar, numera ofta benämnda drönare, har använts bland annat under de militära insatserna i Irak och Afghanistan. Dessa drönare är i huvudsak fjärrstyrda av mänskliga operatörer som befinner sig långt från det område där drönarna uppträder. Detta har lett till diskussioner om hur människor påverkas av att ha ett 9-till-5-jobb som i realiteten innebär att sitta vid en dator

³⁰ Se Ny Teknik, 21 september 2016. Som förberedelse för Ubers försök med taxibilar i Pittsburgh hade laserkartor för Pittsburghs gator, med centimeterprecision, tagits fram. Initialt kan bilarna ta två passagerare i baksätet medan det i framsätet sitter en person som kan ta över förarrollen vid behov och en tekniker som samlar information om funktion m.m. Senare utvidgning av försöken till San Francisco stoppades (av *California Department of Motor Vehicles*) och bilarna omlokaliserades till Arizona, se <http://www.telegraph.co.uk/technology/2016/12/23/uber-relocating-self-driving-cars-arizona-legal-battles-california/> (Besökt 2017-06-12).

³¹ LIDAR (Light Detection and Ranging) är en teknik som använder laser för att bestämma avståndet till ett föremål eller yta. Det används i en mängd olika branscher, bland annat atmosfärfysik, geologi, skogsbruk och oceanografi.

och styra vapeninsatser mot människor och anläggningar i andra länder, en sorts verklighetens TV-spel.

Teknikutvecklingen kommer dock snart att medge att uppdragen kan lösas utan en människa som operatör under själva uppdraget. På vägen till realiserandet av full autonomi kan man också tänka sig svärmar av drönare som kontrolleras av en enda operatör.

I militära sammanhang erbjuder plattformar utan personal en möjlighet att spara liv vid till exempel spaning, vapenleverans och logistiktransporter. Utvecklingen inom ett flertal områden håller för närvarande på att möjliggöra full autonomi för allt från stora till mycket små plattformar och på alla arenor – i luften, på marken, på och under vattenytan. En nyckelteknologi för att uppnå full autonomi är *kinodynamic motion planning*, det vill säga att kunna ta full hänsyn till ett fordons omvärld och planera färdväg och hastighet efter denna.

9.2 Övergripande trender fram till 2035

De viktigaste trenderna inom området obemannade/autonoma system är:

- En ökande grad av potentiell autonomi hos plattformar
- Användning av autonoma plattformar på allt fler arenor.

När det gäller den första punkten finns det som tidigare nämnts starka drivkrafter på den civila marknaden, särskilt hos fordonsindustrin. Autonomi möjliggörs av utvecklingen inom områden som navigation, sensorer och informationsbearbetning, det vill säga möjligheterna att mycket noggrant bestämma positioner, att kombinera sensorer av olika typer till kvalificerade multisensorsystem som kan ge information om omgivningen, samt att använda högpresterande datorer och informationssystem för att bearbeta all erhållen information i realtid och generera styrdata till plattformen.

Trots de möjligheter som detta skapar kommer det att dröja innan förarlösa fordon förekommer i den reguljära trafiken mer än i testsammanhang. Innan en större användning av autonoma fordon är möjlig krävs diskussion av eventuella regelverk som ska gälla för dessa och de risker som finns. En risk är att fordonen blir hackade och styrda av externa aktörer för deras syften. Analyser kommer sannolikt också att vara nödvändiga inför användning av autonoma plattformar för militära tillämpningar.

Samverkande plattformar, såväl bemannade som obemannade, i intelligenta ”svärmar” erbjuder intressanta tillämpningar i framtiden. Autonoma svärmar kan vara möjliga i tidsperspektivet 2035.

När det gäller den andra punkten ovan kommer med stor sannolikhet obemannade, och senare helt autonoma, plattformar uppträda på allt fler arenor. Förutom de mer traditionella flygande systemen (UAV:er), vilka har visat potential både som sensor- och vapenplattformar, innefattar detta även:

- Markplattformar, UGV:er (*Unmanned Ground Vehicles*). Den vanligaste uppgiften för sådana plattformar idag är röjning av minor, oexploderad ammunition (OXA) och sprängämnen. I framtiden kommer vi även att se tillämpningar som underrättelseinhämtning, övervakning

och logistiktransporter. I det senare fallet kan man tänka sig en semi-autonom lösning där det första fordonet körs av en chaufför medan övriga fordon i en logistikkolonn är obemannade och bara följer det första fordonet. På längre sikt kan man tänka sig en fullt autonom lösning.

- Sjöplattformar, USV:er (*Unmanned Surface Vehicles*). De vanligaste uppgifterna för USV:er är i dagsläget verkan mot sjöminor och som övningsmål. Dagens system är fjärrstyrda, men utveckling av halv-autonoma system pågår. I framtiden bedöms USV:er kunna utnyttjas för allt från spaning och kommunikation till att utgöra mobila baser eller utföra offensiva uppdrag. De flesta aktuella koncept är båtar som är 2-12 meter långa som kan levereras från fartyg eller fällas från transportflygplan. Samverkande svärmar av USV:er kan vara en intressant framtida utveckling. En USV kan också vara basplattform (och tillhandahålla kommunikation och energi) för UUV:er.
- Undervattensplattformar, UUV:er (*Unmanned Underwater Vehicles*). UUV:er kan användas för exempelvis hamnskydd (exempelvis för verkan mot minor), övervakningsuppdrag, underrättelseinhämtning. Autonomi och lång uthållighet är önskvärda egenskaper för dessa system. En intressant variant är så kallade bioniska AUV:er (*Autonomous Underwater Vehicle*), det vill säga autonoma system som efterliknar biologiska system – exempelvis fiskar – både avseende utseende och rörelser. Sådana koncept är under utveckling. AUV:er och UUV:er behöver i allmänhet en basplattform på eller ovanför havsytan, som kan användas som kommunikationslänk.

Som framgår finns det många potentiella användningsområden för obemannade system och dessa kommer sannolikt att bli ännu fler när semi-autonoma eller autonoma system blir verklighet i framtiden. Förutom de så kallade 3D-uppdragen (*Dirty, Dull and Dangerous*) som minröjning är bland annat övervakning, underrättelseinhämtning, kommunikation och logistik möjliga uppdrag. Rena offensiva uppdrag genomförs redan idag av UAV:er och med utvecklingen av renodlat stridande system som UCAV:er (*Unmanned Combat Air Vehicles*), som potentiellt kan ersätta och/eller komplettera jakt- och attackflygplan, tillförs ännu en offensiv dimension.

Utvecklingen av obemannade plattformar i olika storlekar och varianter i alla domäner kommer att innebära att de kommer att vara tillgängliga för många olika aktörer, både statliga och icke-statliga sådana. Additiv tillverkning (se kapitel 3) kan göra det möjligt att tillverka delar till obemannade plattformar efter de specifika behov som uppkommer i varje situation. Allt detta sammantaget innebär att vi kommer att behöva utveckla metoder för att motverka obemannade system, vare sig dessa uppträder i luften, på marken, på eller under havsytan. Tekniska lösningar som bygger på mikrovågs- och laserteknik kan här vara värdefulla komplement till mer traditionella bekämpningssystem.

9.3 Koppling till andra teknikområden och krav på dessa

Eftersom autonomi är knutet till olika plattformskoncept kommer utvecklingen av andra för plattformsutvecklingen relevanta områden att vara av betydelse. Detta kan handla om material- och energiteknik, som kan skapa förutsättningar för miniatyrisering och längre uthållighet.

Andra teknikområden som berörs är sensorteknik, signalbehandling, automation och styrning av farkoster, informationsteknologi samt navigeringstekniker.

9.4 Potentiella militära tillämpningar

Obemannade/autonoma plattformar kommer att vara oundgängliga system för Försvarsmakten i framtiden. Lösningar för många olika typer av uppgifter studeras, men kräver försvarsinriktad forskning som komplement till den kommersiellt drivna forskningen. Användningen ställer särskilda krav på militära system och dessutom finns det alltid en motpart som försöker utnyttja de svagheter som finns i systemen.

Den främsta militära tillämpningen är idag framförallt flygande plattformar för spaning och olika former av markfarkoster för olika röjningsuppgifter (till exempel minor och OXA). Idag är obemannade farkoster väsentligen fjärrstyrda men operatörens uppgifter underlättas allt mer i den takt som funktioner kan automatiseras.

För Försvarsmakten är området obemannade farkoster/system av stor vikt för den framtida operativa och strategiska verksamheten. Internationellt används små och medelstora obemannade system i allt större grad för underrättelseinhämtning, fastställande av lägesbild, leverans av last samt för operationer i svårtillgänglig eller farlig miljö. I aktuella konfliktområden som Ukraina och Syrien har användningen av obemannade farkoster ökat kraftigt.

Som redan framgått, men som sammanfattas här, kan obemannade och autonoma system utnyttjas för många olika typer av uppdrag i alla fysiska domäner. Några exempel är:

- ISTAR (*Intelligence, Surveillance, Target Attack, Reconnaissance*), till exempel som bärare av sensorer eller kommunikationslänkar. Dessa uppdrag kan även genomföras inomhus, med hjälp av små flygande eller kravlande system, för att exempelvis identifiera eventuella hot inne i en byggnad.
- Som vapenbärare, antingen som en av flera typer av uppdrag eller genom att utnyttja specifika plattformar avsedda för väpnad strid (exempelvis UCAV:er, som kan bekämpa flygplan och markmål).
- För telekrigföring, till exempel för att störa motståndarens kommunikationssystem och sensorer.
- För underhåll och logistik. Denna typ av uppdrag kan genomföras av både autonoma och semi-autonoma system. Ett semiautonomt logistikuppdrag kan exempelvis bestå av en bemannad lastbil som följs av (och leder) ett antal obemannade lastbilar.

- För röjning av minor och improviserade sprängämnen, på land (UGV:er) eller i havsmiljö (USV:er eller UUV:er/AUV:er).
- För att störa eller bekämpa motståndarens luftförsvar, s.k. SEAD (*Suppress Enemy Air Defence*) eller DEAD (*Defeat Enemy Air Defence*). Dessa uppdrag kan exempelvis utföras av UAV-svärmar eller UCAV:er.

Därutöver kommer motståndarens användning av obemannade farkoster påverka både beteende, skydd och rörelse hos egna förband. Egna system för upptäckt och verkan är väsentliga. Tidigare territoriella förmågor som skydd, maskering och vilseledning är även fortsättningsvis viktiga.

Ökad automation inom Försvarsmakten kan också påverka organisation, materielkostnader, beslutsprocesser och doktrin.

9.5 Begränsande faktorer

Idag tillåts inte fjärrstyrda flygplan (*remotely piloted aircraft systems*, RPAS) att flyga tillsammans med annan lufttrafik av säkerhetsskäl. Det kommer att dröja innan helt autonoma farkoster tillåts i samma område som annan trafik. I militära konflikter kommer sannolikt systemen att användas i större omfattning då civil trafik inte är närvarande.

Andra frågor är om och när obemannade fordon kommer att tillåtas på våra vägar om det finns risk att de kan fungera fel eller hackas och styras av personer som vill skapa kaos? Eller kommer det att krävas att det finns en människa någonstans i loopen. Även integritetsfrågor som kan uppstå vid övervakning av områden behöver analyseras. Om utnyttjandet av de möjligheter teknikutvecklingen medför begränsas på den civila marknaden kan detta också komma att få återverkningar på den militära marknaden.

I Hagström (2016) diskuteras bland annat folkrättsliga frågeställningar som kan uppkomma vid användning av autonoma plattformar för vapeninsatser. Vad innebär det att en ”maskin” självständigt kan ta ett beslut om vapeninsats och hur långt kan detta drivas och tillåtas. Det konstateras att det med ökande komplexitet i systemen krävs mer av användarna för att kunna förstå och förutse konsekvenserna av användning och att det är ansvaret för användningen av tekniken som borde ligga i fokus.

9.6 Referenser

Berglund, E. & Hagström, M., *Teknisk prognos obemannade system*, FOI Memo 4558, augusti 2013 (Teknisk Prognos 2013).

Biomimetic UUV, Fraunhofer INT, 11FMV2150-23, september 2011 (Teknisk Prognos 2012).

Bull, P., Persson, B., Löfgren, L., *Obemannade farkoster*, FHS MTI, juni 2013 (Teknisk Prognos 2013).

Emerging Technology Concepts and Defence Planning in the Nordic Countries, FFI Externnotat 16/00336. Denna rapport analyserar potentialen för

ett antal nya systemkoncept av vilka flera är olika typer av obemannade plattformar.

Evolutionary Robotics, Fraunhofer INT, 11FMV2150-26, november 2011 (Teknisk Prognos 2012).

Hagström, M. (red.), *Autonom våldsutövning – hot eller möjligheter. För en strukturerad debatt*, FOI Memo 5676, 2016.

Kinodynamic Motion Planning – Path Planning for Highly Agile Unmanned Systems, Fraunhofer INT, december 2013 (Teknisk Prognos 2014).

Nano Air Vehicles, Fraunhofer INT, 11FMV2150-27, november 2011 (Teknisk Prognos 2012).

”Så fungerar Ubers självkörande bilar”, Ny Teknik, 21 september 2016

Technology Forecast 2013 for A/UUV, Bruhnspace, oktober 2013 (Teknisk Prognos 2013).

The Multinational Capability Development Campaign (MCDCC) arbetar med att analysera motverkan mot obemannade autonoma system, s.k. CUAXS (*Counter Unmanned Autonomous Systems*) i alla domäner.

Unmanned Combat Aerial Vehicles (UCAV), Fraunhofer INT, mars 2014 (Teknisk Prognos 2014).

Unmanned Surface Vehicles, Fraunhofer INT, januari 2015 (Teknisk Prognos 2015).

10 Plattformer

10.1 Inledning

Teknikutvecklingen påverkar plattformarna inom mark-, sjö- och luftarenorna. Nya material möjliggör minskad vikt, ökad skyddsnivå och förbättrad signaturanpassning hos plattformarna. Nya sensor- och vapentechniker gör det lättare att upptäcka och bekämpa plattformarna. Dessutom kommer utvecklingen inom energiområdet att påverka plattformsutvecklingen.

Införandet av allt fler obemannade, eller på sikt helt autonoma, plattformar på alla arenor kommer också att ha stor påverkan. Dessa kan komma att ersätta eller komplettera traditionella plattformar för vissa uppgifter (se kapitel 9).

Kapitlet är uppdelat i:

- Markplattformar
- Sjöplattformar
- Undervattensplattformar
- Luftplattformar

Obemannade/autonoma plattformar och signaturanpassningsteknik beskrivs i egna kapitel, men kommenteras för respektive plattformstyp nedan.

10.2 Markplattformar

10.2.1 Beskrivning av området

Markplattformar i något utförande används av i stort sett alla enheter inom Försvarsmakten. Några utvecklingstrender kommer att vara gemensamma för många, som automation av olika funktioner, medan andra är förbehållet specialiserade plattformar, som avancerade skyddslösningar mot kvalificerade hot. De militärt mest intressanta trenderna och teknikutvecklingsområdena är de som riktas mot stridsfordon och stridsvagnar. Teknik som är tillämplig för andra plattformstillämpningar kommer naturligt användas där de utgör kostnadseffektiva lösningar på liknande problem, till exempel vikeffektiva skyddslösningar i logistik- eller ledningsfordon.

10.2.2 Övergripande trender fram till 2035

En tydlig trend är aktiva skyddssystem, vilka ökar skyddet mot vissa hot utan att öka vikten dramatiskt. Likaså har kvalificerade skyddsmaterial som keramer, för att dämpa den allt ökande massan hos pansarvagnar, åter fått uppmärksamhet. Elektriskt pansar kan komma att utnyttjas i framtiden, teorin är känd och flera länder har sannolikt utvecklingsprogram. En annan tydlig trend är införandet av, i fordonssammanhang avancerad, elektronik för stöd till omvärldsuppfattning, förar-, skytt- och operatörsstöd. Tekniken ger också möjlighet till högre automation av många funktioner, från styrning av fordon till automatisk avfyring. Redan idag görs experiment med obemannade markfarkoster men i vilka taktiska

situationer sådana är bättre lämpade än bemannade är en fråga som återstår att besvara. Några potentiella tillämpningar nämns i kapitel 9.

Samverkan mellan olika plattformar, sensor- och vapensystem förväntas öka inom alla vapenslag. Detta innebär att även markplattformarna ska kunna agera i samverkan med andra plattformar. I vilken utsträckning sådana systemlösningar kommer att ge önskad effekt till rimliga kostnader är ännu för tidigt att avgöra. Både material, aktiva skyddssystem och avancerade operatörsstödsystem förväntas utvecklas modulärt, ungefär som i den moderna fordons- och lastbilsindustrin, för att hålla nere livscykelkostnaden. Flera länder står inför vägval vad gäller framtida tunga markplattformar. Hur de vägvalen kommer att göras (exempelvis flera mindre lättare eller färre tyngre) är idag för tidigt att säga.

10.2.3 Koppling till andra teknikområden och krav på dessa

Många andra deltekniker som sensorer, elektronik och UAV:er (för lokal spaning och lägesbild), är i sammanhanget väl utvecklade men när dessa ska integreras i en markplattform uppstår nya krav. Telekrigsutrustning utvecklad för marint bruk upptar ofta större volymer än vad som kan tillåtas i markplattformar. Utrustning som utvecklats för flygtillämpningar har utformats med krav på låg vikt och extrem tillförlitlighet, men utan stor tålighet mot de påfrestningar som uppstår i en markplattform. Integrationen av ”nya” tekniker på markplattformarna kommer att ställa krav på andra teknikområden vilket initialt kan vara kostnadsdrivande.

10.2.4 Utveckling av specifika delområden/teknologier

Sedan länge har ”*all electrical vehicles*” funnits som målbild hos markplattformsutvecklarna. Med tillgång till stora energimängder och effekter kan både framdrivning och skyddssystem, och kanske även vapensystem, drivas av samma källa med flera fördelar. För att realisera detta krävs utveckling av effektiva högeffekttekniker för lagring, uppladdning och urladdning som kan rymmas inom volymen av ett fordon. Detta är, liksom avancerade skyddslösningar, integritetskritisk kunskap omgärdad av stor sekretess.

10.2.5 Referenser

Gouré, D., Lexington Institute, *Why the US military can't forget about ground combat vehicles*, Business Insider, Military & Defence, 2016-04-21, <http://www.businessinsider.com/why-the-us-military-cant-forget-about-ground-combat-vehicles-2016-4?r=US&IR=T&IR=T> (Besökt 2017-06-12).

Judson, J., *Combat Vehicle Modernization Strategy: One Year Later*, Defence News, 2015-10-15. <http://www.defensenews.com/articles/combat-vehicle-modernization-strategy-one-year-later>, (Besökt 2017-06-12).

Judson, J., *New Army Strategy Sees Future Combat Vehicles As Highly Mobile, Highly Lethal*, Defence News, 2015-10-15, <http://www.defensenews.com/story/defense/show-daily/ausa/2015/10/15/new-army-strategy-sees-future-combat-vehicles-as-highly-mobile-highly-lethal/73651700/> (Besökt 2017-06-12).

The future of armoured fighting vehicles, Army MoD UK, 2016-03-07,
<http://www.army.mod.uk/news/28476.aspx> (Besökt 2017-06-12).

The Ground Combat Vehicle (GCV) programme, Army Technology,
<http://www.army-technology.com/projects/ground-combat-vehicle-gcv/>
 (Besökt 2017-06-12).

US Army, *The US Army Combat Vehicle Modernization Strategy*
http://www.arcic.army.mil/app_Documents/CVMS_SEP_Master.pdf (Besökt
 2017-06-12).

10.3 Sjöplattformar

10.3.1 Beskrivning av området

I detta avsnitt hanteras ytgående plattformar – främst ytstridsfartyg men även plattformar för sjöminröjning och sjörörlig logistik. Plattformarna utgör element för att kontinuerligt över tid, inom ramen för hela konfliktskalan, möta skilda behov avseende territoriell integritet (TI) och väpnat angrepp (VA). I korthet handlar det om marina plattformar avsedda för sjöövervakning, sjöfartsskydd och kustförsvarsoperationer.

Generellt sett är fartygsmateriel mycket investeringstung avseende såväl anskaffning, tekniskt vidmakthållande som bemanning över tid. Detta gör att många länder har hamnat eller riskerar att hamna i ett otillfredsställande läge av kombinerad fåtalighetsproblematik och gradvis markant föråldring och förslitning av materielen med allt mer utdragna omsättningstakter.

Utvecklingen av marina stridskrafter i vårt närområde är beroende av den ekonomiska utvecklingen. Marinstridskrafternas övergripande roll i flera länder kan förenklat beskrivas som defensiv och stabiliserande. Utvecklingen förutsätter förmåga till strid med system i samverkan och det finns ett fokus på nya sensorer, vapensystem och bredbandig informationsöverföring. Parallellt sker en utveckling av obemannade och autonoma system som komplement till fartyg och helikoptrar eller som mer självständiga plattformar.

10.3.2 Övergripande trender fram till 2035

Oaktat svårigheterna att över tid vidmakthålla och utveckla grundplattan av fartygsmateriel sker kontinuerligt militärteknisk utveckling inom områden som påverkar plattformarnas potentiella systemeffekt kopplat mot höga konflikt-nivåer och marin väpnad strid.

”Ytstrid”

En övergripande trend torde vara en tydligare framväxt av två skilda kategorier av fartygsmateriel – ”arbetshästar” och ”fullblod”. Detta blir till del ett paradigmskifte utifrån ett svenskt perspektiv där vi under en längre tid har haft mycket fokus på ”multifunktionsfartyg” – plattformar som ska klara ut ett flertal olika funktioner och förmågor av skild karaktär för olika konflikt-nivåer och operationstyper.

Med begreppet ”arbetshäst” avses stabila sjösäkra fartyg som verksamhetsmässigt, driftprofilmässigt och ekonomiskt är optimerade för höga gångtidsuttag i låg konfliktnivå, för mötande av behov inom främst sjöövervakning men till del även sjöfartsskydd. Denna kategori utgörs av patrullfartyg, vedettbåtar eller motsvarande. Ur ett ekonomiskt perspektiv kan man förvänta sig att fartygsmaterielen blir standardiserad/samutnyttjad av olika aktörer såsom Marinen och Kustbevakningen.

Med ”fullblod” avses kvalificerade ytstrids- och luftförsvarsfartyg som, utefter ekonomi, tilldelas kvalificerade systemförmågor som medger kapacitet att fullt ut delta i den framtida integrerade luftsjöstriden – särskilt i kustnära områden (hela Östersjöns framtida operationsdjup). Utvecklings-, anskaffnings- och vidmakthållandekostnader bedöms bli så pass höga att antalet kvalificerade enheter blir ”lågt”, kanske singulärt – antingen har man denna marina förmåga eller så har man den inte. Denna typ av fartygsmateriel bedöms, särskilt jämfört med ”arbetshästarna”, ha ett begränsat gångtidsuttag i fredstid. Värdet ligger i trovärdig tröskeleffekt och ”fleet-in-being” i lägre konfliktnivåer och reell väpnad förmåga mot en kvalificerad motståndare i de högre konfliktnivåerna.

En annan övergripande trend, kopplad till ”fullbloden”, är kraftigt utvecklad samverkan eller t.o.m. hård integration mellan luft- och sjöstridskrafter. Drivkrafter för detta är bland annat fåtalighetsproblematik avseende kvalificerade plattformar (luft och sjö) och utvecklingen av system i samverkan där vapenplattformar verkar med långräckviddiga robotsystem som avfyras och uppdateras på/med måldata som genereras genom realtidssensordatafusion mellan aktiva och passiva spaningsnoder (av vilka vapenplattformarna kan vara en typ av nod). Denna utvecklingstrend kan ses som en direkt parallell till utveckling av landbaserad A2/AD³² och kan exemplifieras med USAs CEC- och NIFC-CA-koncept.³³ Systemeffekten blir att kvalificerade fartyg med CEC- och NIFC-CA-förmåga utgör sjörörliga ”A2/AD-bubblor” som helt kan stänga stora sjö- och luftområden för aktörer som inte har motsvarande förmågor eller som på något annat asymmetriskt sätt kan kringgå förmågan.

”Sjöminröjning”

Den kanske mest tydliga trenden inom området sjöminröjning är att befintliga minröjnings-/minjaktsfartyg ersätts och/eller kompletteras med obemannade, och på sikt, till del även autonoma system.

Man kan se olika faser avseende denna utveckling. En första, till del genomförd, fas är att man opererar på distans med fjärrstyrda obemannade system från fartygsplattformar. Nästa steg, som här och var har börjat tillämpas, är att man använder autonoma/semi-autonoma självgående (ytgående och/eller undervattensfarkoster) system för detektion, klassificering och eventuellt även röjning av sjöminor. Dessa är dock huvudsakligen baserade på ”moderfartyg” av traditionell karaktär. De mer futuristiska stegen är utveckling av kvalificerade system av system där obemannade/autonoma farkoster i realtid samverkar med

³² Anti Access/Area Denial handlar om att ta kontroll över operationsområdet och att förneka motparten både access till och möjlighet att verka i detta område. Det amerikanska intresset för A2/AD kopplas bl.a. till den kinesiska förmågan till detta inom sin intressesfär.

³³ CEC står för Cooperative Engagement Capability, d.v.s. med svenska ord strid med system i samverkan. NIFC-CA står för Naval Integrated Fire Control – Counter Air.

varandra, utläggbara sensornoder samt traditionella minröjningsfartyg. En drivande förutsättning för detta är operativt införande av nätverk för undervattenskommunikation.

”Sjörörlig logistik”

Befintliga stödfartyg är ålderstigna och kan endast, avseende skydd/egenskydd, hantera logistikkoncept för låga konfliktnivåer. Motsvarande koncept kan fungera som ”dimensionerande bulk” för omfattande gångtider inom ramen för TI, men får nog anses bli lätta och kritiska mål i högre konfliktnivåer.

10.3.3 Koppling till andra teknikområden och krav på dessa

Avseende kvalificerad ytstridsförmåga med fartyg föreligger starka kopplingar och beroenden mot (behov av integrerad) utveckling inom luft- och ledningsarenan avseende sensorutveckling och länkar för generering och realtidsdistribution av luft- och sjölägesbild samt kvalificerad måldata över stora avstånd.³⁴

10.3.4 Utveckling av specifika delområden/teknologier

Stridsekonomi kan på sikt kräva okonventionella systemlösningar som baseras på *all-electric-ship*, d.v.s. att energiförsörjning avseende såväl framdrivningsförmåga som verkansförmåga (EMRG³⁵/laser etc.) och motmedel baseras på elproduktion och energilagring ombord.³⁶

Hotutveckling avseende kvalificerade egenskyddskoncept för ytstridsfartyg ställer hårda krav på framtida sjömålsrobotsystem avseende räckvidder, hastigheter (överljuds), måldatahantering genom länkar och målsökarteknik robust mot motmedel.

Operativt införande av mogna koncept för undervattenskommunikation är en grund för samverkande system inom bl.a. sjöminröjning med fartyg och obemannade/autonoma system.³⁷

10.3.5 Begränsande faktorer

De framtida kvalificerade sjömålsrobotarna bedöms vara så pass fysiskt stora att de kan vara svåra eller i värsta fall omöjliga att fysiskt integrera i de operativa sjöplattformar svenska marinen förfogar över idag.

Eventuellt införande av *all-electric-ship*-design innebär revolutionär påverkan på utformning av hela systemlösningen för plattformssystemet med dess effektgivande integrationssystem (energisystem, vapensystem, skyddssystem med mera), vilket ställer krav på tidig, välbalanserad totaldesign för helheten.

³⁴ Teknik för framtida stridsfältet, Projekt KV21, KKrVA <http://kkrva.se/kv-21/> (Besökt 2017-06-12). Samt CEC-/NIFC-CA, https://wikipedia.org/wiki/Cooperative_Engagement_Capability. (Besökt 2017-06-12).

³⁵ *Electromagnetic railgun*, en elektromagnetisk kanon som kan avfira projektiler med extremt hög hastighet. Utveckling av en sådan sker inom den amerikanska marinen.

³⁶ Larsson, A., Akyuz, M., Nyholm, S. E., Sjöqvist L., *Elektriska vapen på slagfältet – Litteraturoversikt rörande elektrifiering av plattformar, elektromagnetisk utskjutning och taktiska laservapen*, FOI-R--3962--SE, 2014.

³⁷ Komulainen, A., Nilsson B., Nilsson, J., Sangfelt, E., Öberg, T., *Undervattenskommunikation 2011-2014 Slutrapport*, FOI-R--4024--SE, 2014.

Ovan beskriven utveckling avseende kraftigt utvecklad samverkan eller till och med hård integration mellan luft- och sjöstridskrafter förutsätter att enskilda plattformssystem utgör noder i ett integrerat system-av-system där det egentligen inte är möjligt att särskilja sensorsystem från ledningssystem inkluderande kvalificerade länkar. I dag är det ett ytterligt fåtal globala aktörer som har förmåga att utveckla och operativt införa dessa förmågor och man kan nog förvänta sig restriktivitet med att delge kritiska teknologier och produkter till andra än närmaste partners på bilateral nivå. Detta kan få tydlig negativ påverkan på svensk interoperabilitet gentemot kvalificerade samarbetspartner.

Operativ nytta av ovan beskriven teknikutveckling förutsätter (bland annat) ekonomiska förutsättningar att utveckla/anskaffa associerade systemlösningar. Det bör i sammanhanget påpekas att:

- Tekniskt möjlig förmågeutveckling med associerad systemeffekt är något man antingen förfogar över eller inte. Som dimensionerande grund får man dock utgå från att en kvalificerad motståndare på olika sätt kommer att nyttiggöra potentialen i de beskrivna utvecklingstrenderna.
- Det är inte givet att det nödvändigtvis blir billigt/billigare att möta fåtalighetsperspektivet med införande av obemannade/autonoma system i en integrerad kontext.

10.3.6 Referenser

CEC-/NIFC-CA,

https://wikipedia.org/wiki/Cooperative_Engagement_Capability (Besökt 2017-06-12).

Komulainen, A., Nilsson B., Nilsson, J., Sangfelt, E., Öberg, T.,
Undervattenskommunikation 2011-2014 Slutrapport, FOI-R--4024--SE, 2014

Larsson, A., Akyuz, M., Nyholm, S. E., Sjöqvist L., *Elektriska vapen på slagfältet – Litteraturoversikt rörande elektrifiering av plattformar, elektromagnetisk utskjutning och taktiska laservapen*, FOI-R--3962--SE, 2014

Marinens utvecklingsplan 2016, FM2015-20223:1, 2015-10-25

Maritim samverkan – Betänkande av Maritimetredningen, SOU 2012:48, ISBN 978-91-38-23771-7, 2012

Slutrapport studie Minkrigssystemet 2025 (SJÖ 101205), FM 21 120:10622, 2012-12-14

Teknik för framtida stridsfältet, Projekt KV21, KKrVA, <http://kkrrva.se/kv-21/> (Besökt 2017-06-12).

10.4 Undervattensplattformar

10.4.1 Beskrivning av området

I detta underlag hanteras undervattensplattformar – d.v.s. ubåtar. Plattformarna utgör basen för att kontinuerligt över tid, inom ramen för hela konfliktskalan, möta skilda behov avseende TI och VA. Ubåtens utnyttjande baseras på dolt uppträdande under lång tid, i eget närområde såväl som framskjutet. Genom det dolda uppträdandet skapas osäkerhet, vilket binder ansenliga resurser hos en eventuell motståndare. Detta gör ubåten till ett strategiskt system.

Under de två världskrigen användes ubåten i huvudsak till sjöfartskrig. Under det kalla kriget utvecklades ubåten mot en mer utrerad underrättelse- och specialoperationsplattform för att numera omfatta de flesta företagstyper.

I korthet handlar det om ubåtar avsedda för följande företagstyper i hela konfliktskalan från djupaste fred till fullskaligt krig:

- Spaningsföretag
- Underrättelseinhämtningsföretag
- Specialföretag
- Undervattensinformationsföretag
- Undervattensarbetsföretag
- Minspaning/minröjning/minjaktföretag
- Minkrigsföretag
- Ubåtsjaktföretag
- Sjömålsföretag
- Markmålsföretag

Den sista företagstypen innefattar kryssningsrobotar från konventionella ubåtar såväl som från atomubåtar (SSG/SSGN), samt ballistiska robotar från strategiska atomubåtar (SSBN).

Utveckling, design och produktion av ubåtar är begränsat till ett mindre antal kvalificerade industriländer. Generellt sett är ubåtssystem investeringstunga avseende såväl utveckling, anskaffning och vidmakthållande som bemanning över tid. Detta gör att många länder har hamnat eller riskerar att hamna i ett otillfredsställande läge av kombinerad fåtalighetsproblematik och gradvis markant föråldring och förslitning av materielen med allt mer utdragna omsättningstakter. Detta har gjort att ubåtar som plattformar har ökat sin tekniska livslängd från 20 år upp mot 35-40 år under den senaste 30-årsperioden. Det medför även att delsystemen ombord på ubåtarna omsätts fler gånger under ubåtens livstid än tidigare. Detta sker normalt vid Generalöversyner (GÖ, var 6-8 år), Halvtidsöversyner (HTM, efter 12-15 år) och Livstidsförlängningar (LTF, efter 20-35 år).

Marinstridskrafternas övergripande roll i flera länder kan förenklat beskrivas som defensiv och stabiliserande samtidigt som ubåtarnas karakteristik baserat på det dolda uppträdandet ger en väsentlig tröskeleffekt och därmed stor del av denna stabilitet. Marina system som ubåtar är per enhet några av de dyraste komponenterna i ett lands försvar men ger också stora bidrag till tröskel- och

systemeffekt. Utvecklingen av marina stridskrafter i vårt närområde är därför beroende av den ekonomiska utvecklingen.

Ubåtsutvecklingen förutsätter fortsatt förmåga till enskild strid men där förmågan till strid med system i samverkan (*Cooperative engagement capability*, CEC) har börjat få en väsentlig påverkan på delsysteminnehållet som plattformen bär med sig. Detta innebär ett större fokus på nya sensorer, vapensystem och bredbandig informationsöverföring, såväl för den egna plattformen som för snabbt utläggningsbara system (*Rapid Deployable Systems*, RDS) och obemannade undervattensfarkoster (UUV:er) – allt för att få en bättre systemeffekt i ubåtens eller angränsande operationsområden. Parallellt sker därför en utveckling av obemannade och autonoma system som komplement till ubåtar, fartyg och helikoptrar eller som mer självständiga plattformar.

10.4.2 Övergripande trender fram till 2035

Oaktat svårigheterna att över tid vidmakthålla och utveckla ubåtsplattformen sker kontinuerligt militärteknisk utveckling av medel och motmedel inom områden som påverkar plattformarnas potentiella systemeffekt kopplat mot höga konfliktnivåer och väpnad strid, med yttersta syfte att vinna duellen.

Fåtalighet – Integration av komplexa system

Den numera långt drivna fåtaligheten av antalet ubåtar och den tekniska utvecklingen mot alltmer integrerade och komplexa fartyg med många funktioner och uppgifter för olika konfliktnivåer och företagstyper, har ökat de konventionella ubåtarnas storlek från några hundra ton till 1000 ton och många ligger nu i intervallet 1800-2200 ton. En trend är därför att försöka hålla ubåtarnas storlek nere samtidigt som de kompletteras med obemannad teknik så som RDS:er och UUV:er, inkluderande slussystem på moderubåten (jämför A26). Specialdesignade mini- och kustubåtar på mindre än 100 respektive 400 ton har därför åter börjat utvecklas och anskaffas.

Enskilt uppträdande – Strid med system i samverkan (CEC)

En annan övergripande trend kopplad till ubåten är kraftigt utvecklad samverkan eller till och med hård integration mellan luft- och sjöstridskrafter. Drivkrafter för detta är bland annat fåtalighetsproblematiken avseende kvalificerade plattformar (luft och sjö) och utvecklingen av system i samverkan där vapenplattformar verkar med långräckviddiga torped- och robotsystem som avfyras och uppdateras på/med måldata som genereras genom realtidssensordatafusion mellan aktiva och passiva spaningsnoder (av vilka vapenplattformarna kan vara en typ av nod). Denna utvecklingstrend kan ses som en direkt parallell till utveckling av landbaserad A2/AD³⁸ och kan exemplifieras med USAs CEC- och NIFC-CA-koncept.³⁹ Systemeffekten blir att kvalificerade plattformar med ”CEC-/NIFC-CA-förmåga” utgör sjörörliga ”A2/AD-bubblor” som helt kan för-

³⁸ Anti Access/Area Denial handlar om att ta kontroll över operationsområdet och att förneka motparten både access till och möjlighet att verka i detta område. Det amerikanska intresset för A2/AD kopplas bl.a. till den kinesiska förmågan till detta inom sin intressesfär.

³⁹ CEC står för Cooperative Engagement Capability, d.v.s. med svenska ord strid med system i samverkan. NIFC-CA står för Naval Integrated Fire Control – Counter Air.

neka stora sjö- och luftområden för aktörer som inte har motsvarande förmågor eller som på något annat asymmetriskt sätt kan kringgå förmågan.

Dolt uppträdande – Luftberoende system och signaturer samt fjärrstridsmedel

Konventionella ubåtar har idag 20 till 50 dygns operativ uthållighet, d.v.s. tiden till sjöss. Det innebär att ubåten bär med sig förråd i form av bränsle, mat och vatten för denna tid. Den operativa uthålligheten anger dock inte tiden under ytan (taktisk uthållighet). På grund av hotbildsutvecklingen är ubåtarnas fortsatta överlevnad än mer beroende av det dolda uppträdandet. Baserat på utvecklingen av luftberoende maskinsystem (LOM) som det svenska Stirlingsystemet och det tyska bränslecellsystemet kan ubåtarna nu vara under ytan i upp till en månad, vilket nästan är i paritet med den operativa uthålligheten. Även Ryssland, Frankrike och Japan utvecklar egna bränslecellsystem samtidigt som Sverige och Tyskland utvecklar nästa generations LOM-system. Samtliga länder följer eller driver även utveckling av Li-jon-batterier som komplement till LOM-systemen. Li-jon bedöms inom 10 år ersätta bly-syra-batterier (PB) på ubåtar. För att ubåten ska klara av de allt längre tiderna under vatten, från den batteribaserade uthålligheten på 2-4 dygn till 14-21 dygn och upp mot 30 dygn, måste även navigationssystem och livsuppehållande system såsom lufttning och syresättning klara av denna ökande uthållighet under vatten.

Utvecklingen av ubåtars signaturer, i huvudsak akustiska, elektriska och magnetiska, fortsätter. Duellen mellan sensorer och signaturanpassning är i många fall nere på direkt kollisionssavstånd mellan enheter då ubåten går långsamt och tyst. Svårigheten för framtiden ligger i att designa ubåtarna så att summan av alla signaturer ger en jämn och homogen nivå så att ingen signaturtyp sticker ut och drar till sig en motståndare.

Samtidigt försöker man att uppnå större skjutavstånd så att skjutmomentet, som i likhet med högre fart hos ubåten har en högre signatur, inte ska detekteras av målfartygen eller dessas eskort. Detta ställer i sin tur större krav på sensorer och målfaktorberäkningar då avståndet ökar bortom den optiska horisonten, varför det är naturligt att se bekämpningen som en del i en större bekämpningskedja enligt CEC. På detta sätt blir därför torpeders räckvidd och signatur tillsammans med andra fjärrstridsmedel och system (exempelvis UUV:er och AUV:er) som kan verka på andra sidan horisonten viktiga. Detta är orsaken till att missiler skjutna från ubåtar har haft en begränsad nytta då deras korta porté möjliggjort tidig detektering av skjutande ubåt. Redan dagens moderna missiler har sådana skjutavstånd att det blir svårt att detektera den skjutande ubåten. I framtiden då CEC antas vara inkorporerat hos motståndaren blir detta än svårare, då autonoma skjutande system också blivit ett viktigt komplement till plattformarna.

Man kan se olika steg i utvecklingen. Ett första, till del genomfört, steg är att man opererar på distans med fjärrstyrda obemannade system från ubåtsplattformar. Nästa steg, som här och var har börjat tillämpas, är att man använder autonoma/semi-autonoma självgående system för detektion och klassificering. De mer futuristiska stegen är utveckling av kvalificerade system av system där obemannade/autonoma farkoster i realtid samverkar med varandra, lägger ut sensor- och kommunikationsnoder samt genomför direkta insatser. En drivande

förutsättning för detta är operativt införande av nätverk för undervattens-kommunikation sömlöst kopplade till kommunikationsnätverk ovan ytan.

Kostnadsutveckling för plattformen – delsystemen

Samtidigt som ubåtarna har blivit dyrare, bland annat på grund av fåtalighetsproblemet, kortare serier samt integrationen av allt fler komplexa system, så har den direkta plattformskostnaden minskat per ton. Det är i allt större omfattning de integrerade delsystemen och speciellt ubåtens sensorer, effektorer och ledningssystem som står för en allt större del av den totala anskaffningskostnaden. Kostnadsreduktionerna för själva plattformen har drivits längre än för delsystemen. Samtidigt kommer den framtida konkurrensen mellan det större antalet delsystemleverantörer, i förhållande till antalet ubåtsvarv, att bli hårdare med effektiviseringar som även ger kostnadsreduktioner på sikt.

10.4.3 Koppling till andra teknikområden och krav på dessa

Avseende kvalificerad sjömålsförmåga med ubåtar, fartyg och flyg föreligger starka kopplingar och beroenden mot integrerad utveckling inom luft- och ledningsarenan avseende sensorutveckling (AESAs) och länkar för generering och realtidsdistribution av luft- och sjölägesbild (både för ytan och uv) samt kvalificerad måldata på stora avstånd.

10.4.4 Utveckling av specifika delområden/teknologier

Ovan har angivits några teknologier, funktioner och system som kommer att utvecklas. I framtiden bedöms ett starkt beroende kopplas till autonoma system som enskilt eller i samverkan kommer att lösa uppgifter. Utöver detta kan följande även nämnas:

- Motståndarens utveckling avseende kvalificerade egenskyddskoncept (hårda och mjuka motmedel) för ubåtar och fartyg ställer stora krav på framtida torpeder avseende räckvidder, hastigheter, signaturer, måldatahantering direkt eller genom länkar och robust målsökarteknik mot motmedel.
- Operativt införande av mogna koncept för flerdimensionell kommunikation, speciellt undervattenskommunikation, är en grund för strid med system i samverkan (CEC) inom speciellt följande företagstyper; ubåtsjakt, sjömålsstrid, kartering/sjöminröjning vad avser ubåtar, fartyg och obemannade/autonoma system samt flygande system som JAS och UAV:er.
- System för att generera omvärldsuppfattning, syntetisera och filtrera sensorers kontakter samt distribuera en given omvärldsuppfattning som grund för ledning och planering av insatser. Beroendet av GIS-data även för marina system kommer att öka drastiskt. Därtill utvecklas nya mer komplexa operatörsstödsystem som även behöver integreras för att exempelvis korta beslutstider.

10.4.5 Potentiella militära tillämpningar

I huvudsak inom de taktiska företagstyper som presenteras inledningsvis. Företagstyperna kan bedrivas i samtliga konfliktnivåer men med olika ambition.

10.4.6 Begränsande faktorer

Området genomgår en generationsväxling samtidigt som tillgången på kvalificerad personal med domänkunskap såväl som djup systemkunskap är begränsad. Det finns därför en risk för kompetensförlust i skarven under generationsväxlingen. Sedan murens fall och under de gångna 25 åren har utvecklingen av och tilltron till civila regleringar ökat markant vilket påverkat möjligheterna att utveckla militära system för direkt strid.

10.4.7 Referenser

https://wikipedia.org/wiki/Cooperative_Engagement_Capability (Besökt 2017-09-27).

Komulainen, A., Nilsson B., Nilsson, J., Sangfelt, E., Öberg, T., *Undervattenskommunikation 2011-2014 Slutrapport*, FOI-R--4024--SE, 2014.

FM studie, SJÖ 151601S Ubåtsoperationer, 2015-2016.

FM studie, SJÖ 141602S Ubåtsjakt, 2014-2016.

10.5 Luftplattformar

10.5.1 Beskrivning av området

Militärt delas flygområdet traditionellt in i stridsflyg, transportflyg, helikopter samt fjärrstyrda obemannade system. Frågan är hur väl denna uppdelning står sig i framtiden då de obemannade systemen fortsätter att bredda sina tillämpningar till allt fler områden.

10.5.2 Övergripande trender fram till 2035

Nya typer av plattformar

En av de tydligaste trenderna är utvecklingen av främst små och medelstora obemannade farkoster där diversifieringen till nya tillämpningar stadigt ökar. Det rör sig om rotorsystem, *fixed wing* och hybridsystem där båda principerna används.

Ökad automation – Pilotens roll och plats i systemet

Tydliga trender är ökad automation för både bemannade och obemannade flygsystem. Alltmer komplexa funktioner automatiseras. Automatlandning på hangarfartyg, lufttankning och formationsflygning är redan demonstrerade. System som är *optionally piloted* finns redan operativa och är en tänkbar utvecklingslinje för både stridsflyg och helikoptersystem.

Prestanda

- *Uthållighet – framdrivning/energilagring.* Uthålligheten förbättras både genom design (aerodynamik) och nya koncept för framdrivning och energilagring som studeras världen över. Utvecklingen skulle kunna medföra ett ”språng” i uthållighet/räckvidd för vissa typer av flyg-system, särskilt de som inte har krav på hög hastighet.
- *Hastighet.* Möjligen är hög hastighet (*hypersonic*) på farkostsidan en utveckling som är på väg att återigen få en taktisk/operativ relevans för spaning och vapeninsats. Området tangerar till viss del rymdbaserade förmågor och kommer endast vara aktuellt för de största länderna.
- *Manövrering.* Mer av allt – snabbare, högre och brantare.

Signaturanpassning

Det satsas fortfarande mycket forsknings- och utvecklingsresurser på signaturanpassning av flygfarkoster men utvecklingen av sensorer (hävdar en del) är ikapp och många av dagens signaturanpassade system kommer att bli synliga för moderna radarsystem. Hur detta kommer att fortsätta utvecklas är en öppen fråga men små (fysiskt) signaturanpassade flygsystem bedöms ändå förbli mycket svåra att upptäcka eller innebära mycket korta reaktionstider för den som vill bekämpa denna typ av system.

Stridsflyg

För nästa generations bemannade eller obemannade stridsflygsystem kommer integreringen av sensorer och egenskydd att förbättras ytterligare. Aktiva mot-medel som kan bekämpa inkommande luftvärns- och jaktrobotar har börjat studeras. Olika verkansprinciper studeras, såväl precisionsbekämpning med laser och manövrerande motmedelsmissiler som mer traditionella metoder som bygger på stora volymer av motmedel. Utvecklingen mot skrovintegrering (signaturanpassning) för vapen och sensorer kommer också att fortsätta.

Kostnaderna för stridsflygsystem har fortsatt att öka brant och trots att utvecklingskostnaderna delas mellan flera länder är nu styckepriiset så högt att antalet flygplan, som särskilt mindre länder kan köpa, blir väldigt lågt.

Om kostnadsutvecklingen för nästa generations stridsflygsystem fortsätter på samma sätt kommer många små och medelstora länder inte att kunna investera i dessa. Även om den sjätte generationens system (efter F22/F35) kan förväntas ha enastående prestanda kommer det mest sannolikt inte att kunna kompensera för behovet av en viss volym på flygplansflottan för att kunna vara närvarande i lufthavet över tid, och på flera platser samtidigt. Alternativet för många länder är att den utveckling vi ser idag fortsätter, vilket innebär mindre eller större uppgraderingar av befintliga flygsystem med nya sensorer och bättre vapensystem.

Även USA känner självklart av denna prisutveckling och det bedrivs studier avseende enkla och betydligt billigare (bemannade eller obemannade) flyg-system som ska fungera som vapenbärare, en ”AMRAAM-truck”. På dessa flygplan kan man välja att bära antingen vapen med mycket bra prestanda som avfyras på mycket långa avstånd eller enklare vapen som kan levereras i stora volymer.

Ytterligare en möjlig utvecklingslinje är att behovet av stridsflygplan med fenomenala prestanda inte blir lika uttalat i framtiden. Om robusta kommunikationssystem blir operativa på en större bredd finns möjligheten att strid med system i samverkan verkligen blir ett reellt alternativ till de "superenheter" som ett stridsflygsystem utgör. Spaning, målnmätning och bekämpning sker då i samverkan mellan olika system och plattformar.

Helikoptersystem

Större fjärrstyrda eller *optionally piloted* helikoptersystem är redan operativa och den utvecklingen kommer att fortsätta. Idag används systemen främst för spaning och mycket korta transporter av materiel. Större system för MEDEVAC/CASEVAC, längre transporter, ubåtsjakt m.m. kommer att utvecklas.

Användningen av mindre system för armétillämpningar är kanske det område där utvecklingen kommer att bli som störst.

Transportflyg

Följer i stort sett civil utveckling för större system. Sannolikt är transportflyg (civilt och militärt) den typ av större flygsystem som i framtiden blir först ut att operera fjärrkontrollerat.

10.5.3 Koppling till andra teknikområden och krav på dessa

Området luftplattformar har kopplingar bland annat till områdena automation, systemintegration och system i samverkan. Utvecklingen inom dessa områden är av stor betydelse för utvecklingen av framtidens luftplattformar.

10.5.4 Utveckling av specifika delområden/teknologier

De klassiska flygtekniska disciplinerna aerodynamik, flygmekanik och flyg-signaturer utgör fortsatt grunden för att ha förmågan att studera flygsystem i traditionella och nya tillämpningar.

10.5.5 Potentiella militära tillämpningar

Flygstridskrafternas stora betydelse för militära tillämpningar kommer bestå i hela skalan från stridsteknik på slagfältet upp till politisk-strategisk nivå där framtida förmågor från de mest komplexa flygsystemen bara blir tillgängliga för stor- och supermakter.

10.5.6 Begränsande faktorer

Många av de nya tillämpningarna sker med små (eller mycket små) system och frågan vad som i framtiden kommer att betraktas som "luftfart" är intressant av både kostnads- och säkerhetsskäl. Det finns regler idag för vad som är luftfart men hur (och om) dessa regler förskjuts är oklart. Trycket från den civila sektorn är stort, i februari 2015 släppte USA:s luftfartsmyndighet FAA reglementet för civil användning och mottog 181 000 driftsansökningar bara under de två första veckorna. Försvarsmakten i USA har fler än 11 000 plattformar. Det europeiska

projektet SESAR⁴⁰ som driver utveckling och implementation av nya metoder för flygtrafiktjänst i Europa förutser att år 2050 kommer 20 % av all flygtid över 150 meters höjd över marken att bedrivas med fjärrkontrollerade flygsystem. Under 150 meter kommer siffran att vara ännu högre.

För fredstida användning kommer de militära reglerna efterhand att harmoniseras med de regelverk som ICAO⁴¹ arbetar med. Ett civilt regelverk där fjärrkontrollerade och bemannade system uppträder på helt lika villkor är målet men bedöms ligga minst 15 år bort. Det kommer att utvecklas nationella militära (och civila) särlösningar i vissa länder för att kunna använda systemen mer flexibelt fram till dess att det internationella regelverket finns på plats.

Regler för uppträdande finns även i militär användning i kris och krig. Hittills är erfarenheterna från användning av större UAV-system från områden med luftherravälde. Hur ”fritt” denna typ av system ska kunna operera i framtida konflikter där luftherravälde saknas är något som studeras flitigt. Många av de tekniker som utvecklas (exempelvis störtålig navigering) syftar just till att farkosten ska kunna lösa sina uppgifter utan kontakt med operatören.

10.5.7 Referenser

AFRL and the 3rd Offset Strategy, McMurry, R. D. Jr., Commander of US Air Force Research Laboratory, Tal vid Aerospace Technology Congress, Solna 11 oktober 2016. Presentation: http://ftfsweden.se/wp-content/uploads/2016/10/FT2016-Plenary-1_AFRL-US_McMurry.pdf. (Besökt 2017-06-12).

Axell, E., Jändel, M. Lindahl, D. Linder, S., Rodhe, I. Westerdahl, L., (2013) *Robust kommunikation cybersäkerhet och artificiell intelligens för säkerhet i RPAS*, FOI-R--3825--SE.

DARPA Open Catalog. <http://www.darpa.mil/work-with-us/darpa-open-catalog>. (Besökt 2017-06-12).

Hultgren, K. Mårtensson, T. Rensfeldt, A. Stensbäck, N. Woltijer, R., (2013) *Flygsäkerhet för obemannade system*, FOI-R--3788--SE.

Report of the Defence Science Board Summer study on Autonomy, US Office of the Under Secretary of Defense, June 2016. <http://www.acq.osd.mil/dsb/reports/2010s/DSBSS15.pdf> (Besökt 2017-06-13).

Scharre, P., *Robotics on the Battlefield - Part I: Range, Persistence and Daring*, 2014, CNAS.

Scharre, P., *Robotics on the Battlefield Part II. The Coming Swarm*. 2014, CNAS.

The Third U.S. Offset Strategy and its Implications for Partners and Allies, As Delivered by Deputy Secretary of Defense Bob Work, Willard Hotel, Washington, D.C., Jan. 28, 2015 <http://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies>. (Besökt 2017-06-12).

⁴⁰ Single European Sky Air Traffic Management Research.

⁴¹ International Civil Aviation Organization.

11 Rymden

11.1 Beskrivning av området

Rymden är en egen arena vid sidan av luft, sjö, mark och information där komplexa tekniska system verkar enskilt eller integrerat med övriga arenor. Rymdrelaterade tjänster kan bidra till både en multiplikativ och strategisk styrkehöjande effekt (eng. *strategic force multiplier*) och möjliggöra helt nya militära förmågor som används i andra domäner. Satellitplattformar kan bland annat nyttjas för:

- Spaning och Övervakning från Rymden (SÖR)
- Satellitkommunikation
- Positionering, Navigering och Tidssynkronisering (PNT)
- Tidig förvarning (av missiluppskjutning)
- Insamling av vetenskaplig data.

Satelliter kan också nyttjas som vapen eller vapenbärare, både för att verka mot andra satelliter och mot övriga arenor. Utöver satelliter omfattar området även markstationer för att kontrollera och kommunicera med satelliterna, bärraketer och missiler, samt rymdfärjor. Rymdområdet täcker även in rymdmiljöns (rymdvädrets) påverkan på tekniska system i samtliga arenor samt uppskjutningsförmåga.

Rymdarenan karaktäriseras av ett stort antal närvarande aktörer som representerar såväl militära som civila och kommersiella intressen. Den komplexa situationen bidrar till att utvecklingen drar åt olika håll, men det finns behov som sammanfaller vilket i vissa fall gör det svårt att skilja intressena åt. Rymdområdet kännetecknas också av så kallade dubbla användningsområden (eng. *dual-use*), ett begrepp som innebär att ett rymdsystem eller rymdtjänst kan användas både civilt och militärt. Det är svårt att dra en gräns mellan militära och civila system då det är användaren av rymdtjänsten snarare än själva rymdsystemet som avgör vilken kategori det tillhör. Det krävs därför samordning mellan militära och civila aktörer för att belysa dessa frågor.

11.2 Övergripande trender fram till 2035

11.2.1 Säkerhetspolitisk utveckling

I dagens globaliserade miljö används rymdbaserade tjänster för allt fler syften. Tillgången till och efterfrågan på rymdtjänster ökar och förväntas fortsätta öka fram till 2035. Utvecklingen har möjliggjort att rymden som global allmänning i allt större utsträckning nyttjas av allt fler.

Såväl små som medelstora statliga och privata aktörer kan använda sig av rymdarenan och deras syften är tydligt kopplade till nationella och privata intressen. Utvecklingen av rymdsystem har i sig kommit att ha en säkerhetspolitisk dimension, oavsett systemens tilltänkta användningsområde eller förmåga. Det har därför blivit allt viktigare att förhålla sig till rymdverksamhet som en nationell strategisk resurs och ett säkerhetspolitiskt frågekomplex.

I Europa är säkerhets- och försvarsbehov numera en del i EU:s ambitioner för rymden. Europeiska kommissionen har nyligen tagit fram en rymdstrategi för EU.⁴² Syftet med strategin är att redogöra för en övergripande strategisk vision för EU:s rymdverksamhet fram till och med år 2030 som inbegriper såväl civila som militära och samhällskritiska behov. Detta ska samtidigt samordnas med och komplettera rymdverksamhet som bedrivs av EU-länderna individuellt och genom Europeiska rymdorganisationen (ESA).

11.2.2 Fler och nya aktörer i rymden

Antalet länder som har eller har haft egna satelliter i rymden fortsätter att öka under perioden. I dag består listan av ett 70-tal länder men nya tillkommer varje år allteftersom nyttan med egna rymdbaserade system blir uppenbar. Detta gäller för såväl forskning som industritillväxt och nationella försvars- och säkerhetsintressen.

Trots det stora antalet länder med satelliter är det endast elva som har egna bäraketprogram som medger oberoende kapacitet att skjuta upp satelliter. Tre av dessa har tillkommit under senare år och ytterligare ett antal länder och kommersiella aktörer har officiellt uttryckt ambitionen att utveckla egna bäraketprogram inom den närmaste framtiden.

11.2.3 Kommersialisering

Det är inte bara de statliga aktörerna som blir fler. Teknikutvecklingen på rymdsidan drivs allt oftare av privata aktörer och det blir vanligare med rent kommersiellt drivna idéer och projekt i rymdbranschen. Privata aktörer med kommersiella intressen finns nu närvarande i de flesta rymdbaserade tjänstesektorer, vilket har möjliggjort för mindre länder att köpa sig rymdbaserade tjänster. Framförallt USA har öppnat upp för mer kommersiellt användande av rymden och söker aktivt internationellt samarbete.

Parallellt med den snabba utvecklingen finns även ett behov av att vidareutveckla de existerande regelverken och internationella regimerna för rymdverksamhet för att hantera den ökande användningen av rymden och tillgodose nya aktörers intressen.

11.2.4 Teknikutveckling och teknikspridning

På tekniksidan är miniatyrisering och standardisering en trend som bidrar till att satelliter blir billigare och att utvecklings- och integreringstiden av hela satellitsystem minskar. Små samverkande satellitsystem kommer att till del ersätta de traditionellt stora tunga satelliterna. Nya billigare koncept för uppskjutning av små satelliter är under utveckling med målsättningen att kunna skjuta upp och sätta en satellit i bruk på mindre än en vecka, ett scenario som bedöms vara troligt att uppnå inom perioden fram till 2035.

⁴² Space Strategy for Europe, COM (2016) 705 final, 2016-10-26, Europeiska kommissionen, Bryssel, http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=8975&lang=en (hämtad 2016-11-08).

I dag och under den närmaste tiden framöver är samarbete ett vanligt tillvägagångssätt för framförallt mindre länder att bygga upp ett nationellt rymdprogram. Oftast via bilaterala avtal eller via en rent kommersiell aktör som erbjuder både utbildning och nära utvecklingssamarbete på plats. Kunskapen blir alltmer tillgänglig vilket leder till att det är relativt lätt att i dag bygga upp en nationell rymdkompetens om det finns ekonomiska förutsättningar och nationella prioriteringar som stödjer detta.

I dag är beroendet av rymdbaserade tjänster större än vad många inser. I många länder finns det inga redundanta lösningar till militära förmågor som en del satelliter bidrar till. Detta beroende kommer att fortsätta öka fram till 2035 då nya tjänster fortsätter att växa fram. Detta gör det allt viktigare att säkerställa tillträde till rymden, både avseende uppskjutningar och för att få tillgång till lämpliga banor. En annan utveckling är det ökande beroendet av kommersiella rymdtjänster hos militära aktörer. De privata aktörerna erbjuder kontinuerligt nya tjänster som kompletterar de militära satellitsystemen på olika sätt. Många länder, som till exempel Sverige, är beroende av kommersiella rymdtjänster.

Området mellan rymd och luft kommer sannolikt öka i betydelse. Ny teknologi möjliggör nya förmågor i gränslandet mellan de två arenorna. Det finns redan nu system som kan flyga i flera veckor på en höjd runt 20 kilometer vilket är betydligt högre än normal marschhöjd för flygplan.

Nya rymdbaserade tjänster skapar också ett ökande behov av radiofrekvenser, speciellt för kommunikation och radar. Det tillgängliga frekvensutrymmet är dock en begränsad resurs som delas av många användare och regleras nationellt av PTS⁴³ i Sverige och internationellt av ITU⁴⁴. Samma resurs är även efterfrågad av starka kommersiella aktörer inom mobilkommunikation vilket innebär en ökande konkurrens på senare år och denna trend förväntas fortsätta i framtiden.

11.3 Koppling till andra teknikområden och krav på dessa

Det finns många kopplingar mellan rymdområdet och andra teknikområden, både i form av teknik som utvecklas för andra domäner men som bidrar till en teknikutveckling av rymdsystem, och i form av rymdteknik som kan nyttjas i andra sammanhang. Exempel på detta är utvecklingen av miniatyriserad elektronik och system samt standardisering som *plug and play* som nu implementeras i satellitsystem för att minska såväl vikt som utvecklingstid, samt därmed minska kostnader för satellitsystem.

⁴³ Post- och telestyrelsen.

⁴⁴ Internationella teleunionen inom FN.

11.4 Utveckling av specifika delområden/teknologier

11.4.1 Uppskjutning och tillgänglighet till rymden

Inom perioden fram till 2035 förväntas uppskjutningsmöjligheterna öka, kostnaderna minska och antalet statliga och kommersiella aktörer bli fler. Uppskjutning av små satelliter har ökat under senare år och trenden bedöms fortsätta. Forskningsinstitut och universitet har tidigare fått acceptera att få skjuta upp sina små satelliter som *piggybacks* på bäraraketer med andra primära satelliter. Små satelliter har samtidigt blivit mer intressanta för den militära sektorn. Militära kravställare vill ha full kontroll på vilken bana satelliterna placeras ut i och när uppskjutningen ska ske. Detta kräver andra tillvägagångssätt vid uppskjutning som till exempel uppskjutning från en flygfarkost. Ett annat militärt intresse är att vid behov kunna skjuta upp en satellit med kort varsel. Här brukar begreppet *launch on demand* nämnas. En förutsättning för uppskjutningar med kort tidshorisont är att hanteringen av bränslet i bäraraketer blir mer lätthanterligt och billigare. Förkortning av tiden för uppskjutning tillsammans med kravet på reducerade kostnader för uppskjutning av satelliter driver på utvecklingen vad gäller nya och innovativa sätt att få tillgång till rymden. Det finns ett antal olika initiativ där uppskjutning via flygplan studeras och testas. På senare tid har även flera aktörer påbörjat utveckling av återanvändbara bäraraketer samt små bäraraketer lämpade för uppskjutning av små satelliter.

11.4.2 Satellitkommunikation

Satellitkommunikation, satkom, är tillsammans med kortvåg de enda långgräckviddiga kommunikationsmedel svenska försvaret har tillgång till om markbaserad kommunikationsinfrastruktur saknas eller är utslagen. Satkom är helt nödvändig vid internationella insatser men betydelsen ökar även i det nationella försvaret.

Under senare år har andelen rent militära kommunikationssatelliter minskat i takt med att den militära trafiken har övergått till kommersiella system. Om trenden står sig är det inte uteslutet att aktiv störning mot satelliterna kommer att öka fram till 2035 eftersom värdet av sådan störning ökar för motståndaren.⁴⁵ Samtidigt finns det i dagsläget obetydligt inbyggt skydd mot detta i de typiska kommersiella satelliterna. Utvecklingen av störskydd för kommersiella satelliter kommer sannolikt att påverka den militära användningen av dessa satelliter.

Andra teknikområden inom kommunikationsområdet som förutspås få ökad betydelse under perioden inkluderar så kallad kognitiv radioteknik. Optiska länkar förutspås även få ökad betydelse för kommunikation mellan satelliter och mellan rymd- och marksegmentet. Vidare utgör M2M (*Machine-To-Machine*) en ökande marknad för satellitkommunikation där övervakning, sensordatainhämtning, fordonsföljning och logistikstöd i avlägsna områden dominerar användningen. Stark utveckling förutspås inom det närmaste decenniet vilket bör skapa möjligheter till förbättrade och nya militära förmågor.

⁴⁵ Exempel på rapporterade störningar är när Libyen störde Thuraya under den arabiska våren i februari 2011 och Egyptiska Nilesat som blev störda på mer än 60 TV-kanaler under samma tidsperiod.

Satellitkommunikation används även i ökande grad som transmissionsnät för mobilnät, exempelvis vid katastrofinsatser och internationella militära operationer.

11.4.3 Spaning och Övervakning från Rymden (SÖR)

Inom området SÖR förväntas utvecklingen fram till 2035 gå mot tjänster som erbjuder övervakning i nära realtid, med både passiva och aktiva sensorsystem som samverkar mellan samtliga arenor. Ryldbaserade sensorer kommer att utgöra en fundamental komponent i en sådan utveckling som med stor sannolikhet kommer att medföra både nya militära möjligheter och en förändrad och mer komplex hotbild.

Inom både optisk och högupplösande Syntetisk Aperturradar (SAR) går utvecklingen tydligt mot att fler länder skaffar sig en egen förmåga genom egna system eller, alternativt, tillgång till motsvarande spaningsinformation i samarbete med andra länder eller kommersiella lösningar.

Satellitbaserad AIS⁴⁶ är också under stark utveckling och allt tyder på att vi inom en snar framtid kommer att få se en stor mängd satelliter som kan ta emot och tolka AIS-signaler från fartyg för positionering och identifiering. Kombinationen AIS och sensordata kommer också att utvecklas framöver.

Signalspaning från rymden är, förutom *early warning*-data, i princip det enda data som inte går att köpa kommersiellt. Möjligheterna framöver förbättras och blir billigare i och med mindre satellitplattformar och nya tekniker för antenner.

11.4.4 Rymdlägesbild (SSA)

Rymdlägesbild (SSA, eng. *Space Situational Awareness*) innebär en gemensam lägesbild av rymddomänen och kan användas som beslutsstöd vid egen planering såväl som vid bedömning av andras förmåga. Med information om rymdläget går det exempelvis att planera för egen bildinhämtning, vilseledning men även eventuella telekrigsinsatser mot andra aktörers ryldbaserade informationsinhämtning. Trenderna i dagens forskning och utveckling inom området rymdlägesbild är dels att andra stater än USA, bland annat med Europa i spetsen, har påbörjat ett utvecklingsarbete, dels att detta arbete till stor del genomförs i internationell regi. Problemets omfattning, och ren geometri för utplaceringen av SSA-sensorerna, är bakgrunden till globaliseringen av utvecklingsarbetet.

I Europa är det framförallt Tyskland och Frankrike som driver utvecklingen med att ta fram kapacitet för SSA, men fler länder förväntas öka sitt engagemang under kommande år. EU spelar en alltmer central roll och eventuellt kommer delar av de publika tjänsterna att hanteras inom EU.

Förutom ovanstående politiska/organisatoriska utmaningar är den stora forskningsmässiga diskussionen för ögonblicket hur de olika typerna av sensordata ska integreras på ett relevant sätt. *Sensor fusion*, *Space object dynamics* och *Space object measurement* är tre aktuella forskningsområden.

⁴⁶ AIS, Automatic Identification System, är ett identifieringssystem för sjöfarten som överför fartygsinformation (position, fart, MMSI, m.m.).

11.4.5 GNSS (Global Navigation Satellite System)

Med ett satellitnavigeringssystem (GNSS) kan en mottagare bestämma sin position och tid (PNT) globalt. Försvarsmakten är en ackrediterad användare av militär GPS som är under införande och användningen bedöms öka. Det finns plattformar och bekämpningssystem som är kritiskt beroende av GNSS för att erhålla avsedd verkan. Hotbilden (störning och vilseledning) mot det civila samhällets och Försvarsmaktens användning av GNSS är omfattande och ett flertal incidenter har skett. Inom GNSS-området finns därför flera trender som är av militärt intresse och som förväntas bli tongivande under de närmaste decennierna: GNSS-mottagare som nyttjar såväl GPS som Galileo och GLONASS⁴⁷ och som kan användas som komplement till militär GPS; Gruppantenn teknik för undertryckning av interferenser med inriktning på lågt SWAP-C ⁴⁸(*Size, Weight, Power and Cost*); Militära GPS-mottagare för M-kod⁴⁹; Mottagare som kan använda Galileo PRS⁵⁰; samt *spot beam* för att lokalt öka den mottagna signalnivån.

11.5 Potentiella militära tillämpningar

De militära tillämpningarna av rymden är många. I vissa avseenden nyttjas rymdsystem och rymdtjänster för att stödja och förstärka redan existerande militära förmågor för operationer i övriga arenor. I andra avseenden nyttjas rymdbaserade system för att skapa nya militära förmågor för operationer som annars inte skulle vara möjliga. Ytterligare ett avseende är att utöka den militära förmågan till att också innefatta militär förmåga för operationer i rymden, till exempel att använda satelliter som vapen mot andra satelliter eller mot marken.

Rymdarenan kan bland annat bidra med följande militära tillämpningar:

- **Precision i position och tid** – att med stor säkerhet träffa rätt mål med så kallade riktade attacker är ett sätt att nå önskad effekt och samtidigt begränsa eventuella skador på omgivningen. Genom att använda satellitnavigeringssystem som till exempel GPS i olika vapensystem uppnås en mer noggrann positionsbestämning.
- **Icke kränkande spaning** – Rymdbaserade sensorer kan utföra strategisk, taktisk och operativ spaning på global nivå och är de facto de enda systemen som inte kränker nationsgränser.
- **Global kommunikation och dataöverföring** – att kunna leda och koordinera en insats eller föra ut kritisk information till soldater i verkansmiljö är en nödvändighet. Det effektivaste sättet att kommunicera och föra över information snabbt och över stora avstånd, till exempel mellan Sverige och ett insatsland, är via satellit.

⁴⁷ Galileo och GLONASS är den europeiska respektive den ryska motsvarigheten till det amerikanska GPS-systemet.

⁴⁸ SWAP-C, ett begrepp som innebär att man eftersträvar mindre storlek, lägre vikt, lägre effektförbrukning och lägre kostnad.

⁴⁹ M-kod, eller militär kod, är den militära GPS-signalen som är designad för att vara mer robust mot telekrig.

⁵⁰ Galileo PRS, *Public regulated service*, utvecklas för användning av myndigheter och företag inom EU för säkerhets- och försvarstillämpningar.

- **Tidig förvarning** – Framskjutna ryddbaserade förvarningssystem för missilattacker kan komplettera andra förvarningssystem, vilket medger snabbare identifiering av en motståndare och möjlighet att sätta in lämpliga försvarsåtgärder.
- **Informationsöverläge och kunskap om hotbilden** – Vad pågår ovanför svenskt luftrum och vad vet vi egentligen om andra aktörers förmåga i rymden? Allt fler aktörer använder satellittjänster. I en strävan efter informationsöverläge är det nödvändigt att genom en så kallad rymdlägesbild ha kunskap om hotbilden i och från rymden.

11.6 Begränsande faktorer

I och med den allt mer omfattande rymdverksamheten har även mängden rymdskrot ökat på ett oroväckande sätt. Om inget görs åt ”nedskräpningen” kan den komma att försvåra fortsatt rymdverksamhet. Den minskar möjligheterna att skicka upp satelliter och framförallt ökar den risken för att satelliter krockar med varandra eller med rymdskrot. Detta tillsammans med insikten att både det civila samhället och militära operationer i dag är starkt beroende av rymdtjänster har gjort att utvecklingsinsatserna kring SSA har tagit fart de senaste åren.

Som påpekats finns det fler aktörer representerade i rymden i dag och de kommersiella aktörerna har blivit starkare. Fler länder har i dag förmåga att utveckla rymdsystem och skjuta upp dem och ännu fler kan använda systemen genom att köpa kommersiella tjänster på den öppna marknaden. I takt med att rymden blir en allt viktigare strategisk tillgång ökar också risken för en kapprustning i rymden. Dagens rymdlagstiftning är tyvärr i otakt med dagens teknologiska och politiska förutsättningar. Det finns ingen lagstiftning som förbjuder utplacering av vapen i rymden (förutom massförstörelsevapen). Utveckling, test och användandet av antisatellitvapen, ASAT, förbjuds inte heller. Det saknas även internationella juridiskt bindande överenskommelser som begränsar eller förhindrar avsiktligt skapande av rymdskrot.

11.7 Referenser

Andersson, C., Asp, B., Eklöf, F. M., Lindström, S., Ulander, L., (2013), *Teknisk prognos – Rymd*, FOI Memo 4541.

Future Operating Environment 2035, Strategic Trends Programme, First Edition, 2015, Development, Concepts and Doctrine Centre, Ministry of Defence, UK.

Joint Concept Note 3/12 (JCN 3/12), 2012, The Development, Concepts and Doctrine Centre, Ministry of Defence, UK.

Lindström, S., (2015), *FOIs inspel till Rymdutredningen*, FOI-2015-287.

Lindström, S., (red.), (2014), *Omvärldsanalys RYMD 2014 - Trender, möjligheter och hot för militär förmågutveckling*, FOI-R--3985--SE.

Lindström, S., Andersson, C., (2009), *FoRMA - Militärt nyttjande av rymden i ett 10-20 års perspektiv*, FOI-R--2834--SE.

Space Strategy for Europe, COM (2016) 705 final, 2016-10-26, Europeiska kommissionen, Bryssel, http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=8975&lang=en (hämtad 2016-11-08).

12 Signaturanpassningsteknik (SAT)

12.1 Beskrivning av området

Signaturanpassningsteknik (SAT, eng. *signature management, stealth*) handlar om metoder för att minska kontrasten mellan ett objekt och bakgrunden ur alla aspekter som kan detekteras av en sensor. SAT brukar sorteras under begreppet vilseledning. Området utvecklas i princip bara för militära tillämpningar. Dock finns civil FoU inom till exempel materialområdet som kan nyttiggöras också i SAT-tillämpningar. Kunskap rörande SAT behövs inte bara för att designa och kravsätta egen materiel utan också för att bedöma skyddsnivån hos andra aktörers skyddsmateriel.

Syftet med SAT uttrycks bra med det engelska uttrycket *sensor denial* och avser skydd mot de sensorer som uppträder på slagfältet. Främst handlar det om optronik (UV, visuellt, nära-IR, termisk IR och laser), radar (passiv radiometri, aktiv radar) och akustik. I specialfall kan det handla om elektriska eller magnetiska fält (fartygsfallet) eller andra emissioner eller spår som någon sensor detekterar.

SAT är ett systemområde där det är viktigt att kunskap om hela kedjan från hot-sensorer, miljö, maskeringssystem, formgivning och materialegenskaper finns med.

Dimensionerande för behovet av signaturanpassning är kapaciteten hos de sensorer som används på slagfältet avseende förmåga till upptäckt, klassificering, identifiering och möjlighet att följa målobjekt (*tracking*). En svår avvägning är bedömningen av när nya sensorteknologier kan förväntas vara operativa och införda i sikten, spaningssystem och vapensystem och därmed kräva en vässad skyddsnivå. I värsta scenariet kan en specifik skyddsåtgärd till och med underlätta för sensorn.

På grund av att det militära fokuset i Europa har legat på internationella insatser i konflikter med en mindre avancerad motståndare har utvecklingen inom signaturanpassningsområdet bromsat utom för de allra dyraste plattformarna som stridsflygplan och ubåtar. I ett scenario där en motståndare har tillgång till avancerade sensorer ökar betydelsen av signaturanpassningsteknik.

12.2 Övergripande trender fram till 2035

I duellen mellan sensorer och signaturanpassning har en upptrappning varit tydlig de senaste åren. Nedan beskrivs några trender på sensorsidan som kommit att förskjuta balansen och successivt ökar kraven på skyddsnivån för överlevnad allt eftersom ny sensorteknik införs i operativa system.

12.2.1 Sensorer

Framförallt har mängden sensorer på slagfälten ökat. Där hotet tidigare utgjordes av enstaka spaningsflygplan som genomförde spaningsuppdrag med våtfilm-kameror, finns idag en ökande flora av realtidssensorer som insamlar information, alltifrån civila mobilkameror, avancerade sikten på trupp till sensorer på

så gott som varje militär plattform. Sensortyper som för några år sedan endast fanns på fordon och i målsökare, såsom 3-5 μm IR-sensorer, finns nu tillgängliga för avsuttna soldater. Speciellt utgör UAV-utvecklingen ett trendbrott vad gäller hot mot våra skyddsobjekt. Det är obemannade plattformar som bär kvalificerade sensorer fram nära skyddsobjektet. Även sensorer i rymden måste beaktas, där sensorinformationen kan tillgodosgöras genom länkning i realtid.

En dramatisk förbättring av sensorernas upplösning noteras. Måligenkänning är möjlig även på radarsidan. Syntetisk aperturradar (SAR) producerar upplösta bilder.

Genom den snabba elektronikutvecklingen och datorutvecklingen utvecklas den sensornära signalbehandlingen. Man kan säga att sensorerna blir intelligentare. Sensorsystemen kan hjälpa operatören att sortera informationen och hitta det man söker även i mycket komplexa miljöer.

Den tekniska utvecklingen av nya sensortyper och sensorer med nya egenskaper aktualiserar behov av förbättrat skydd i form av signaturanpassning. Några exempel på detta är:

- Hyperspektrala sensorer samlar in information i fler våglängder, vilket används för att lättare upptäcka och identifiera militära mål. I urban miljö kan dessa sensorer särskilja militära från civila plattformar.
- Polarisationskänsliga sensorer kan användas för att hitta mänskligt tillverkade objekt (oftast polariserande) i en naturlig vegetationsbakgrund (oftast opolariserande).
- Sensorer tillkommer i våglängdsområden där det hittills inte funnits något hot, såsom Short Wave Infrared (SWIR) (1,1-2,5 μm). Signaturanpassade objekt kan upptäckas eftersom sensorer i dessa våglängdsområden hittills inte bedömts utgöra något hot vid design/kravställning. SWIR-sensorer ser dessutom bättre genom dimma och rök än många traditionella IR-sensorer.

12.2.2 Signaturanpassningsteknik

Några större trendbrott inom SAT kan, på grund av låg prioritering av området under de senaste åren, inte skönjas. Dock finns utvecklingar som kan tillgodosgöras om området åter prioriteras.

En stark utveckling av modellering och simulering möjliggör optimering av signaturlösningar som tidigare inte varit möjliga. Det kan handla om design av allt från hela lågsignaturplattformar till impedansanpassning av ytkonforma antenner eller radomer. En trend är också att införa simuleringsverktyg operativt i tyngre plattformar för att åstadkomma ”signature awareness”, det vill säga som beslutsunderlag för att avgöra hur sårbar plattformen är under rådande omgivningsförhållanden. Med god kännedom om aktuell signaturstatus kan man också anpassa sitt taktiska uppträdande.

Den civila utvecklingen på materialområdet har i vissa fall varit språngartad där nya lätta material ger möjlighet till nya skyddslösningar. Nya komponenter för att styra energi kan ge möjlighet till att realisera styrbar signatur.

12.3 Kopplingar till andra teknikområden

SAT kopplar starkt till sensorområdet, då duellsituationen driver på utvecklingen inom båda områdena så att skyddet ska matcha hotet och tvärtom. Den specifikt militära utvecklingen inom sensorområdet inriktas mot att klara icke-kooperativa mål, vilket avser förmåga att detektera lågsignaturmål eller hitta maskerade mål i en komplex bakgrund.

SAT kopplar till plattformsområdena för mark, sjö, luft och soldat. Internationellt pratar man om *integrated survivability* och avser en optimering och balansering av alla olika skyddsåtgärder. Det ska påpekas att förutom tekniska lösningar så inkluderas även taktikutveckling. Om signaturaspekter beaktas redan i designskedet kan kostnaden minskas och skyddsnivån ökas i förhållande till efterhandsanpassning.

Som skydd för plattformar samverkar SAT med telekrigområdet. I slutfasen, då vapnet är avfyrat och målsökaren låst på plattformen kompletterar SAT telekrigs- och skenmålsåtgärder i syfte att skydda plattformen från träff eller vilseleda målsökaren bort från plattformens vitalare delar. En lägre signatur på plattformen ökar sannolikheten att en robot ska låsa på motmedel (till exempel facklor) istället för på plattformen.

Kopplingen är också stark till området Vapen och skydd där det ballistiska skyddet utvecklas.

Inom Flygsystemområdet är signaturanpassning en viktig designparameter tillsammans med aerodynamisk optimering. Här finns också speciella utmaningar i integrationen av delsystem och last för att flygplattformen totalt ska erhålla låg signatur.

Materialteknik är ett område med en snabb civil utveckling, som kan komma till nytta för militära tillämpningar. Det gäller speciellt spektral design och adaptivt kamouflage, se nedan.

12.4 Utveckling inom specifika delområden

Många signaturanpassningsproblem kan lösas med skräddarsydda ytskikt som kan ges önskade egenskaper (reflektans, absorptionsförmåga, polarisation etc.) för att möta några av de nya sensortechnologierna som nämns ovan. Ytskikten kan vara kombinationer av materialval och struktur. Spektral design är en teknik där man med avancerad materialteknologi kan anpassa en ytas reflektans till bakgrunden inom ett brett våglängdsområde som till exempel kan inkludera synliga, nära infraröda, SWIR och termiskt infraröda band.

Multifunktionella material utvecklas för att sänka den totala vikten på ett system. Speciellt intressant är detta för personburna och flygande system. Det kan röra sig om lastbärande strukturer, radarabsorbenter som kan lagra vatten och/eller bränsle, batterier eller ballistiskt skyddande signaturmaterial.

Traditionellt har radarsignaturanpassning handlat mycket om formgivning av plattformar. Ny sensortechnologi, såsom bistatisk radar och lågfrekvensradar, möjliggör upptäckt av *stealth*-formgivna plattformar. Radarabsorberande material kan användas för att minska radarmålarean för dessa nya hot.

Magnetiska nanokompositer är ett exempel på en materialkategori som kan vara användbar vid signaturanpassning.

Signaturanpassning i IR handlar traditionellt mycket om att undvika att exponera varma delar av plattformen mot motståndarens sensorer. Detta kan göras genom avskärmning eller kylning. En alternativ metod, som tros få större betydelse i framtiden, är att använda lågemissiva material som gör att en varm yta ser svalare ut än den är för en IR-sensor. Fotonkristaller och keramiska multipelskikt är strukturer som studerats.

Grafen är ett relativt nytt material med intressanta egenskaper som kan komma till nytta för signaturanpassning i framtiden. Det är genomskinligt, elektriskt och termiskt ledande, lätt och dessutom mekaniskt mycket starkt. Den civila bildskärmsindustrin satsar stora resurser på utveckling av grafenteknologi för displaytillämpningar.

Inom biomimetik försöker man inspireras av naturen till signaturanpassningslösningar. Djur, såsom bläckfiskar, fåglar, kameleonter och skalbaggar, har ofta mycket avancerade material och strukturer som ger bättre kamouflage än vi lyckas åstadkomma. Sådana biologiska kamouflage studeras nu med målsättning att efterlikna och modifiera materialen för att uppnå bättre skydd mot nya sensortyper.

Adaptiv signaturanpassning, där signaturen kan ändras i realtid med avseende på bakgrund, väderförhållanden, hotbild eller uppdrag förekommer ännu inte operativt men forskning och utveckling pågår i ett flertal länder.

Modellering och simulering är verktyg som används alltmer både vid design av signaturanpassade plattformar och vid värdering av sensorsystem och duellsituationer sensor/signatur. Modellering och simulering kommer till nytta på alla systemnivåer, från materialval till stridssimulering på bataljonsnivå.

För värdering och validering av signaturnivåer hos skyddsobjekt samt för validering av simuleringsverktygen är kapaciteten för signaturmätningar viktig för att kunna arbeta inom området. Detta gäller inte bara tillgången till mätinstrumentering utan i minst lika hög grad kunskapsnivån och utveckling av metodik för signaturmätningar.

12.5 Potentiella militära tillämpningar

Signaturanpassningsteknik kan användas som skydd för alla typer av militära sensor- och vapenbärande plattformar: Flyg, fartyg, landfordon, avsuttna sol-dater och även i viss mån fasta anläggningar.

Syftet med signaturanpassningen är att förhindra eller fördröja upptäckt, klassificering, identifiering, och mållåsning av plattformen som ska skyddas. SAT kan även användas i kombination med skenmål för att vilseleda en motståndare och försvåra dennes underrättelseinhämtning.

Signaturpredikteringsverktyg kan också användas operativt som beslutsunderlag för att bedöma tillgänglighet för egna och motståndarens sensorer.

Vid en avvägning av olika skyddstekniker, till exempel ballistiska skydd mot signaturanpassning, måste hänsyn tas till hur olika förmågor hos enheten

påverkas. Tunga ballistiska skydd sänker till exempel rörligheten, vilket signaturanpassningsmateriel inte behöver göra i lika hög grad.

Ubåt är en extremt signaturanpassad plattform. Teknologin runt den beskrivs inte här.

12.6 Begränsande faktorer

Det är svårt att åstadkomma bra signaturanpassning mot alla typer av sensorer samtidigt. Att kombinera radarabsorbenter med visuell och termisk signaturanpassning kräver att det planeras redan i designskedet.

Bestyckning av befintliga plattformar med ny utrustning, såsom vapen, sensorer, och ledningsutrustning, kan försämra plattformens signatur kraftigt, speciellt i radar- och IR-områdena. Omvänt gäller också att extrem signaturanpassning kan försämra möjligheterna att verka med sensorer och vapen etc.

Rörliga plattformar är lätta att upptäcka under förflyttning, vilket är en utmaning för signaturanpassningsteknik. Inte ens de adaptiva kamouflagesystem som har demonstrerats klarar av att bevara god signaturanpassning under förflyttning.

God signaturanpassning försvårar även vår egen lägesuppfattning och bör kombineras med någon form av *blue force tracking* för att undvika vådabekämpning av egna förband. Några typer av IFF-funktioner⁵¹ kan kompromettera signaturanpassningen.

Olika miljöbetingelser begränsar också vilken signaturstatus som är möjlig att uppnå. I arktisk miljö är IR-signaturanpassning mycket svårt på grund av de stora temperaturskillnaderna mellan objekt och bakgrund.

12.7 Referenser

Björkert, S., *Polarimetrisk optisk signaturmodellering: Implementering av en polarimetrisk BRDF modell i PolSig*, FOI Memo 5540.

Kariis, H., & Savage S., *The sensor-signature duel*, Sensorsymposium 2012, Stockholm, Sverige. FOI-S--4136--SE.

Kariis, H., Andersson, K., Andersson, Å., Hallberg, T., Pohl, A., Savage, S., Åkerlind, C., Andersson, K., *Signaturmaterial 2014. Verksamhetsrapport*. FOI-R--4021--SE.

Kariis, H., *Camouflage requirements and solutions for the future*, FOI-S--4906--SE.

Pohl, A., Kindström, G., Alm, M., Magnusson, P., Hedenstierna, S., Kariis, H., Savage, S., Thunell, M., *The Soldier's Individual Protection Equipment*, FOI-R--3368--SE.

SAT-handbok Mark, FOI, ISBN 91-7056-114-1, 2003.

Savage, S., *Signaturmaterial: Trender och militär nytta 2015*, FOI MEMO 5521.

⁵¹ Identification Friend or Foe, igenkänningssystem.

Teknisk Vilseledning, studie ATK 99091S, Försvarsmakten, 13301:60353, 2003.

Zdansky, E., *Ground winter signatures, an inventory*, FOI-R--3509--SE.

Åkerlind, C., Arwin, H., Hallberg, T., Gustafsson, J., Kariis, H., Landin, J., Järrendahl K., *Biomimetics for future low emissive coatings: Optical properties of Cyphochilus insulanus*, FOI-S--4851--SE.

Åkerlind, C., Bergström, D., Hallberg, T., Valyukh, S., *Spectral polarimetric camouflage*, FOI-S--5463--SE.

13 Soldatsystemet

13.1 Beskrivning av området

Utvecklingen inom områden som bioteknik, materialteknik, sensorer och informationsteknologi kommer att kunna innebära att den enskilda soldatens förmåga utvecklas såväl fysiskt (exempelvis genom förstärkande exoskelett) som avseende förbättrad omvärldsomfattning och skyddsnivå (exempelvis genom material som anpassar sig till omgivningen). Soldaten kommer också sannolikt, liksom andra framtida plattformar, att integreras som en nod i ett nätverk med möjlighet att i (nära) realtid både leverera och erhålla data.

13.2 Övergripande trender fram till 2035

Soldatsystemet är en viktig del av den amerikanska tredje offsetstrategin, vilken beskriver teknikområden som bedöms vara av intresse för USA:s försvar i framtiden. Flera av de prioriterade områdena i denna relaterar till soldatområdet, specifikt samverkan mellan människa och maskin såväl i beslutsfattande som i strid samt förbättring av den mänskliga prestationsförmågan.

Syftet med utvecklingen av soldatsystemet är att:

- Öka soldatens prestationsförmåga både mentalt och fysiskt
- Öka effekten av soldaten som stridande system
- Lätta soldatens fysiska bördor
- Ge soldaten förbättrad omvärldsuppfattning
- Göra det möjligt för soldaten att effektivt samverka med “maskiner”, i framtiden kanske till och med genom att använda hjärn-dator-interface
- Utveckla bättre skyddssystem, till exempel genom att använda nya material
- Göra det möjligt att i realtid följa soldaternas fysiska och mentala status
- Göra det möjligt att implementera portabla medicinska diagnossystem och även metoder som kan underlätta behandling av soldater som är sjuka eller skadade, antingen direkt på plats eller med hjälp av telemedicin.

Utvecklingen inom områden som materialteknik, sensorsystem, bioteknik, neurovetenskap och informationsteknologi kommer, om de implementeras, ha potential att leda till stora förbättringar av soldaternas förmåga att utföra sina uppdrag.

Några av dessa utvecklingstrender – speciellt de som handlar om medicinska substanser eller direkt integration mellan den mänskliga hjärnan och datorn – har konsekvenser som bör analyseras utifrån etiska eller medicinska perspektiv, vilket kan påverka utvecklingen inom dessa områden.

13.3 Koppling till andra teknikområden och krav på dessa

Enligt ovan bygger de möjligheter som finns till utveckling av soldatsystemet på utvecklingen inom ett antal olika teknikområden. Några särskilt intressanta delområden presenteras i avsnitt 13.4 nedan.

13.4 Utveckling av specifika delområden/teknologier

Ett antal forskningsområden som kan bidra till utvecklingen inom soldatsystemet presenteras nedan. Forskning pågår inom alla dessa områden och det finns stor potential att nyttiggöra civil forskning för försvarets behov inom vissa av dem. På längre sikt kan alltmer kvalificerad samverkan och utbyte mellan människa och maskin bli möjlig.

13.4.1 Verkanssystem

Utvecklingen av soldatburna verkanssystem har de senaste decennierna huvudsakligen drivits av pågående lågintensitetskonflikter. Motståndaren har i dessa konflikter sällan varit utmanande ur verkanshänseende (oskyddad trupp, lättare fordon) varför mycket av utvecklingsfokus snarare legat på sådant som förbättrad mjukmålsverkan, viktnedskning av vapensystemen (till förmån för bland annat kroppsskydd) och minimering av tredjepartsrisk.

Ett ökat intresse för territorialförsvar mot kvalificerade motståndare medför betydande utmaningar för soldatburna vapensystem, dels på grund av att en modernt skyddad motståndare är betydligt svårare att bekämpa, dels för att motståndarens vapenporté och utbildningsstatus inte kan förmodas vara underlägsen vår egen och att eget luftherravälde inte kan förutsättas.

En avgörande framtidsfråga för såväl finkalibervapen som burna splitterstridsdelar är hur dessa ska dimensioneras för att ge verkan i väl skyddade mål. Utveckling av penetratorteknologier specifikt anpassade för detta kan vara en avgörande faktor för framtida eldhandvapen. Man kan också tänka sig verkansstrategier baserade på att motståndarens skydd kan penetreras (kaliber/viktsdrivande) och/eller att verkan erhålls i mindre väl skyddade delar av målet (till exempel genom ökad splittertäthet för granater eller alternativ elddoktrin/riktpunkt och kvalificerade sikten för direktriktade vapen).

För burna PV-vapensystem innebär moderna hotplattformar betydande utmaningar, på grund av dels ökade grund- och tilläggsskyddsnivåer, dels aktiva skyddssystem som riskerar att göra många äldre PV-vapen obsoleta. Därför finns det behov av att utveckla hotmålsanpassade PV-vapen och studera alternativa verkansprinciper för att vidmakthålla soldatens förmåga att bekämpa tyngre hotmål.

13.4.2 Kvalificerade sikten

En snabb utveckling pågår för närvarande vad gäller kvalificerade sikten för soldatburna vapen. Sensorer och funktionalitet som tidigare endast fanns i stridsfordon förekommer idag på burna vapen till en kontinuerligt minskande

kostnad. Detta omfattar allt från relativt enkla analoga dagsikten som med hjälp av ett laseravståndsinstrument bistår soldaten med ballistisk kompensation på längre skjutavstånd (korrigerad riktpunkt) till bildbehandlande multispektrala sikten som kan bistå med såväl upptäckt och målprioritering som ballistik-kompensation och framförhållning för rörliga mål.

Då ett kvalificerat sikte kombineras med ett elektriskt avfyrat vapen kan ytterligare funktionalitet erhållas, till exempel ”taggning” innan skott (att siktet medger ”provavfyringar”, tills önskad träffpunkt erhålls, varefter siktet följer målet och det skarpa skottet avfyras av siktet först när riktpunkten korresponderar med önskat träffläge) eller att siktet själv avfyrar vapnet baserat på igenkänningsalgoritmer då vapnet riktas mot målet med avtryckaren aktiverad (exempelvis baserat på typisk termisk signatur).

13.4.3 Sensorer och beslutsstöd

Teknologin blir tillgänglig i allt mindre format och avancerade sensorer blir vanligare på soldatnivå. Detta innebär att soldaten på individnivå har mer information för att fatta egna beslut än idag. Genom att sensorsystemen på enskilda soldater kommunicerar med varandra inom en grupp eller mellan grupper kan man dessutom genom att sätta samman sensordata få en mer komplett bild av till exempel omgivningens utseende eller motståndarens position. Men samtidigt kan det negativt påverka förutsättningarna för att agera dolt.

13.4.4 Nya material

Forskning inom materialområdet kan komma att möjliggöra såväl bättre skyddsnivå mot olika hot som lägre vikt för soldatens system och på sikt en alltmer effektiv signaturanpassning till omgivningen (minskad signatur). I det senare kan till exempel lärdomar från djurriket användas.

13.4.5 Framtidens uniform

Den framtida uniformen kommer, förutom att ha integrerade sensorer för att avläsa soldatens hälsostatus, också att kunna ha andra system integrerade – till exempel antenner som kan användas för kommunikation med obemannade flygande farkoster och teknik som kan skydda soldaterna från BC-ämnen, eld, väder och trubbigt våld.

13.4.6 Robotik

Ett sätt att lätta soldatens börda är att utnyttja robotiksystem som kan användas som ”mulor”. Sådana system blir allt bättre på att klara av att röra sig i olika terräng.

13.4.7 Samverkan mellan människa och maskin

I framtiden kommer möjligheterna till nära samverkan mellan människa och maskin att öka. Detta kopplar tekniskt till utveckling av maskinintelligens och maskinlärande, det vill säga att datorer alltmer kan efterlikna ”mänskligt” bete-

ende. Balansen mellan mänsklig kontroll och maskinell autonomi är en viktig fråga.

På lång sikt kan det också bli möjligt att integrera hjärna och dator, vilket möjliggör mental kontroll av utrustning (icke-fysisk växelverkan) och utbyte av in- och utdata mellan människa och maskin. Kopplingar finns till teknikområden som förstärkt (*augmented*) verklighet och analys av stora datamängder.

13.4.8 VR i kombination med direkt visualisering av sensordata

Utvecklingen inom virtuell verklighet och visualisering innebär att soldaten kan få en samlad bild av data från olika sensorer i nära realtid och därmed en bättre situationsuppfattning. Detta är också starkt kopplat till förstärkt verklighet.

13.4.9 Användning av sociala media

Idag, och kanske ännu mer i framtiden, kan sociala media utnyttjas för att erhålla information för att förstärka situationsuppfattningen och förståelsen för den miljö i vilken ett uppdrag ska lösas.

13.4.10 Exoskelett

Exoskelett kan lätta soldatens börda avsevärt genom att förstärka muskelfunktioner. Det pågår en hel del utveckling inom detta område och det finns redan system som kan hjälpa soldater att bära tunga bördor. Ett problem är dock att exoskelett kan innebära att soldaten får svårare att gå. Därför är ett fokus för utvecklingen att kombinera lättandet av soldatens bördor med att öka effektiviteten hos soldatens gång.

13.4.11 Kognitiva system

Soldatens kognitiva prestationsförmåga kan ökas med medicinska substanser, mental träning och olika typer av beslutsstödsystem (datorbaserade analysstödsystem, människa-maskin-samverkan etc.).

13.4.12 Artificiell intelligens

Utveckling av artificiell intelligens (AI) har diskuterats och debatterats länge, men idag är vi nära en realisering av sådana system. ”Maskiner” visar förmåga att besegra människor i spel – till exempel schack och, på senare tid, Go. Utveckling av system för så kallad *deep learning*, som möjliggörs av datorers allt mer ökade prestanda, bidrar också till utvecklingen av AI.

13.4.13 Övervakning av soldatens hälsa och förmåga

Teknikutvecklingen kommer att göra det möjligt att övervaka soldatens hälsostatus genom att avläsa parametrar av betydelse för denna. Detta kan göras exempelvis med hjälp av sensorer integrerade i uniformen. Ett resultat kan till exempel vara rekommendationer om när soldaten behöver vila eller få närings-tillskott.

13.5 Potentiella militära tillämpningar

Den framtida soldaten kan, genom den teknikutveckling som kortfattat beskrivs ovan, bli en allt mer kompetent plattform för inhämtning och styrning av informationsinhämtning såväl som för stridsinsatser. Soldaten kan också genom de förmågor som tillförs bidra med underlag till beslut och stödja insatser med andra system/förband.

13.6 Begränsande faktorer

Som framgår ovan finns det bland de framtida möjligheterna såväl prestationshöjande medicinska preparat som en potentiellt allt mer ökad samverkan (och kanske integration) mellan människa och maskin. En del av dessa kommer att bli omdebatterade och det är svårt att sja om hur mycket som tillåts realiseras.

13.7 Referenser

Eriksson, T. & Törne, A., *Koncept kring soldatfrågor – Den framtida soldatens förutsättningar*, FOI-R--4273--SE, 2016. Rapporten innehåller också en relativt omfattande referenslista.

Nyholm, S.E., Berefelt, F., Akyuz, M. & Bergh, M., *Skanning av området styrda finkalibriga projektiler*, FOI-R--3996--SE, 2014.

Förkortningsordlista

A2/AD	Anti Access/Area Denial
ABL	Airborne Laser
AESA	Active Electronically Scanned Array
AIS	Automatic Identification System
AMRAAM	Advanced Medium-Range Air-to-Air Missile
ASAT	Antisatellit
AUV	Autonomous Underwater Vehicle
BIOS/UEFI	Basic Input/Output System/Unified Extensible Firmware Interface
CASEVAC	Casualty Evacuation
CEC	Cooperative Engagement Capability
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CSA	Cyber Situational Awareness
CUAxs	Counter Unmanned Autonomous Systems
DDoS	Distribuerade överbelastningsattacker
DEAD	Defeat Enemy Air Defence
EA	Electronic Attack
ESA	European Space Agency
EMRG	Electromagnetic Railgun
FAA	Federal Aviation Administration (Amerikanska luftfartsmyndigheten).
FEL	Frielektronlaser
FoU	Forskning och Utveckling
GLONASS	Globalnaya navigatsionnaya sputnikovaya sistema
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GÖ	Generalöversyn
HPM	High Power Microwave
HSSW	High Speed Strike Weapon
HTM	Halvtidsöversyn

ICAO	International Civil Aviation Organization
IED	Improvised Explosive Device
IFF	Identification Friend or Foe, igenkänningsystem
IoT	Internet of Things ("sakernas internet")
IPR	Intellectual property rights
IR	Infrarött
ISTAR	Intelligence, Surveillance, Target Attack, Reconnaissance
IT	Informationsteknologi
ITU	Internationella teleunionen
LaWS	Laser Weapons System
LIDAR	Light Detection and Ranging
LOM	Luftberoende maskinsystem
LOT	Low Observables Technology
LTE	Long Term Evolution
LTF	Livstidsförlängning
M2M	Machine-to-machine
MCDC	Multinational Capability Development Campaign
MEDEVAC	Medical Evacuation
MMSI	Maritime Mobile Service Identifier
MoS	Modellering och Simulering
MTU	Motoren- und Turbinen-Union
NASA	National Aeronautics and Space Administration
NIFC-CA	Naval Integrated Fire Control – Counter Air
NIR	Near Infrared
OXA	Oexploderad ammunition
PB	Bly-syra-batteri
PDE	Pulsdetonationsmotorn
PNT	Positionering, Navigering och Tidssynkronisering
PRS	Public Regulated Service
PTS	Post- och telestyrelsen
RAM	Rockets, Artillery, Mortars
RDS	Rapid Deployable Systems
RMS	Regler för Militär Sjöfart
RPAS	Remotely Piloted Aircraft Systems

RSA	Krypteringsmetod uppkallad efter upphovsmännen Ron Rivest, Adi Shamir och Leonard Adelman
SAR	Syntetisk Aperturradar
SAT	Signaturanpassningsteknik
SEAD	Suppress Enemy Air Defence
SESAAR	Single European Sky Air Traffic Management Research
SQL	Structured Query Language
SSA	Space Situational Awareness
SSBN	Nuclear-powered Ballistic Missile Submarine
SSG/SSGN	(Nuclear-powered) Guided Missile Submarine
SWAP-C	Size, Weight, Power and Cost
SWIR	Short Wave Infrared
SÖR	Spaning och övervakning från rymden
TI	Territoriell Integritet
TRADOC	U.S. Army Training and Doctrine Command
UAS	Unmanned Air System
UAV	Unmanned Air Vehicle
UCAV	Unmanned Combat Air Vehicle
UGV	Unmanned Ground Vehicle
USD	United States Dollar
USV	Unmanned Surface Vehicle
UUV	Unmanned Underwater Vehicle
UV	Ultraviolett
VA	Väpnat Angrepp
XSS	Cross-site scripting

Bilaga 1

Experterna fick i uppgift att utifrån sin expertkunskap beskriva "sitt" område utifrån följande mallstruktur:

- *Karaktärisering/beskrivning av området (ca ½ sida)*
- *Övergripande trender → 2035 (ca 1-1½ sida)*
- *Ev. koppling till andra teknikområden och krav på dessa (ca ½ sida)*
- *Utveckling av specifika delområden/teknologier (ca 1-1½ sida)*
- *Potentiella militära tillämpningar (ca 1 sida)*
- *Ev. begränsande faktorer (tekniska, etiska etc.) (ca ½ sida)*
- *Referenser (ca ¼ sida)*

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.



FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se