# Militärteknik 2050

Göran Kindvall, Anna Lindberg, Cecilia During (red.)

FOI-R--5904--SE

Mars 2026

Göran Kindvall, Anna Lindberg, Cecilia During (red.)

# Militärteknik 2050

| | |
|---|---|
| Titel | Militärteknik 2050 |
| Title | Military technology 2050 |
| Rapportnr/Report no | FOI-R--5904--SE |
| Månad/Month | Mars |
| Utgivningsår/Year | 2026 |
| Antal sidor/Pages | 321 |
| ISSN | 1650-1942 |
| Uppdragsgivare/Client | Försvarsmakten |
| Forskningsområde/Research Area | Operationsanalys och strategisk planering |
| FoT-område | Inget FoT-område |
| Projektnr/Project no | E13952/E12545 |
| Godkänd av/Approved by | Malek Finn Khan |
| Ansvarig avdelning/Division | Försvarsanalys |

Bild/Cover: Shutterstock, AI-generad

# Sammanfattning

Denna antologis huvudsakliga syfte är att stödja Försvarsmaktens långsiktiga planering, benämnd Perspektivstudien. Antologin ger en bred beskrivning av möjlig teknikutveckling mot 2050 och resonerar kring hur denna teknik påverkar framtida militär förmåga. Detta görs mot bakgrund av ett försämrat säkerhetspolitiskt läge, krig i Europa, Sveriges Natomedlemskap och ett återtaget totalförsvar.

De potentiellt stora tekniska genombrott som kan komma att ske, konkurrensen om att leda denna utveckling, och den generella prioriteringen av teknik och innovation, ökar också behovet av en gedigen analys av teknikutvecklingens potentiella konsekvenser.

Detta är tredje gången FOI levererar en sammanställning om teknikutveckling till Perspektivstudien, och ambitionsnivån har höjts för varje utgåva. Med denna antologi tas ytterligare ett steg mot att ge en så heltäckande bild som möjligt av försvarsrelevanta teknologiska trender, med ett framåtblickande perspektiv som sträcker sig mot år 2050.

Antologin är framtagen både för att vara en inspirerande skrift i sammanhang där en uppfattning om den framtida teknikutvecklingen behövs och för att kunna användas i spel och seminariediskussioner om militärteknik i studiesammanhang. Som en del i arbetet har även seminarier och presentationer av många av kapitlen löpande genomförts för Försvarsmakten.

Nyckelord: perspektivstudie, militär teknik, teknikutveckling, framsyn

## Summary

The primary purpose of this anthology is to provide support for the Swedish Armed Forces' long term defence planning. It provides a broad description of potential technological developments toward 2050 and discusses how these may influence future military capability. This analysis is set against the backdrop of a deteriorating security environment, war in Europe, Sweden's NATO membership, and the re-establishment of total defence.

The prospect of major technological breakthroughs, the global competition to drive this development, and the increasing prioritisation of technology and innovation all underlines the need for a thorough assessment of the potential consequences of technological change.

This is the third time FOI has produced a compilation on technological development for the long term defence planning, with each edition raising the level of ambition. This anthology takes another step toward providing a comprehensive picture of defence relevant technological trends, with a forward looking perspective extending to 2050.

The anthology is intended both as an inspiring document in contexts where an understanding of future technological development is required, and as material for wargames and seminar discussions on military technology. As part of the work, many chapters have also been presented and discussed in seminars held for the Swedish Armed Forces.

Keywords: long term planning, military technology, technology development, foresight

# Innehållsförteckning

# Inledning

*Göran Kindvall, Anna Lindberg och Cecilia During*

## Bakgrund

FOI-projektet Stöd till militärstrategisk inriktning (SMI) har till uppdrag att ge stöd till Försvarsmaktens perspektivstudie. Ett av de områden som särskilt beaktas i perspektivstudien är teknikutveckling med relevans för militär förmåga. Denna antologi är ett bidrag till perspektivstudiens framsynsarbete och beskriver i kortform teknikområden som identifierats som intressanta och relevanta i ett 25-årigt tidsperspektiv.[1] Arbetet har också delfinansierats av Försvarsmaktens beställning Omvärldsbevakning FOI 25.

Detta är inte första gången ett sådant arbete görs. Under 2017 levererades en rapport som beskrev teknikutvecklingen fram till 2035 som ett underlag till Försvarsmaktens perspektivstudie 2016–2018.[2] Uppgiften från Försvarsmakten var att i skriftlig form redovisa en samlad och strukturerad övergripande sammanställning av utvecklingen inom ett antal teknikområden i tjugoårsperspektivet. Samma områden utgjorde grund för teknikspel under 2017.[3] Under 2020 gjordes en uppdatering och utveckling av rapporten från 2017 där fler teknikområden togs med och där fokus också lades på att skriva en sammanfattande analys med syfte att knyta ihop och dra slutsatser om teknikutvecklingen för främst det militära försvaret.[4]

Nu tar vi, genom att ta upp fler områden än tidigare, ytterligare ett steg mot att så heltäckande som möjligt beskriva försvarsrelevant teknikutveckling med ett framåtblickande perspektiv mot 2050.

## Målgrupp

Enligt ovan är den främsta målgruppen Försvarsmaktens perspektivstudie i deras arbete med att förstå teknikutvecklingen och dess roll i omvärldsutvecklingen. Dock är det vår ambition att antologin även ska vara av nytta för Försvarsmaktens

1 Perspektivstudien inriktas genom regleringsbrev och ger underlag till Försvarsberedningen och därigenom även indirekt till Försvarsbeslut. Tidsperspektivet är 25-årigt och underlaget är till stora delar ett framsynsarbete där konsekvenser för försvar studeras.

2 Kindvall, G. och Wiss, Å. (red.), Militärteknik i ett tjugoårigt perspektiv: Underlag till Försvarsmaktens Perspektivstudie 2017, FOI-R--4462--SE, november 2017.

3 Lindberg A. et al. (2017). Erfarenheter från teknikspel våren 2017. FOI Memo 6230, 2017-11-28.

4 Kindvall, G. och Lindberg, A. (red.), Militärteknik 2045 – Ett underlag till Försvarsmaktens perspektivstudie, FOI-R--4985--SE, november 2020.

huvudstudier i arbetet med framtagning av spelkort och koncept samt för Försvarsmaktens FoU-ansvariga som en sammanställning och profilprodukt för den verksamhet som de finansierar och inriktar.

Därutöver ser vi andra målgrupper, som personal i Försvarsmakten som inte är engagerade i Perspektivstudien eller huvudstudierna, anställda vid övriga försvarsmyndigheter samt försvarsindustri. Den förra rapporten – Militärteknik 2045 – rönte intresse även utanför dessa kretsar.

## Metod

Texterna i denna antologi syftar både till att redogöra för den tekniska utvecklingen och för vad denna kan innebära för verksamheten inom försvar och säkerhet. Ett nytt grepp denna gång är att vi tydligare separerar teknikområden och förmågeområden. Med det senare menas områden där teknikerna sammantaget och tillämpat tydligt kopplar an till försvarsgrenar, funktioner och domäner. Sådana områden är till exempel plattformar inom de olika domänerna.

Antologin har sin tyngd i beskrivningar av den tekniska forskningen och utvecklingen snarare än i konsekvenser för militär förmåga och effekter i operationer. Vi försöker dock, i den avslutande syntesen, att även resonera kring hur den militärtekniska utvecklingen påverkar Försvarsmaktens verksamhet.

Textunderlaget är framtaget både för att vara en inspirerande skrift i sammanhang där en uppfattning om den framtida teknikutvecklingen behövs och för att kunna användas i spel och seminariediskussioner om militärteknik inom Försvarsmaktens perspektivstudie. Som en del i arbetet har även seminarier och presentationer av många av kapitlen löpande genomförts för Försvarsmakten. Målgruppen för dessa har främst varit Perspektivstudien och Försvarsmaktens huvudstudier. Ett teknikspel genomfördes också 2024, där ett antal teknikområden prövades i operativa scenarier. Spelet genomfördes inspirerat av *Disruptive Technology Assessment Game* (DTAG), en spelmodell som utvecklades inom två Natostudier för ca 15 år sedan.[5]

Kapitelstrukturen har tagits fram i dialog mellan redaktörerna för antologin och personal i Perspektivstudien. Kapitlen inleds med en översiktlig beskrivning av området, varpå författarna beskriver trender ut mot 2050, specifika delområden, kopplingar till andra teknikområden och förmågor samt vilka de huvudsakliga aktörerna är inom forskning och utveckling. Ett antal lästips ges också.

På samma sätt som för rapporten Militärteknik 2045 identifierade redaktörerna, i dialog med bland annat FOI:s forskningsområdesföreträdare och linjechefer,

5 Kindvall, G, Värdering av disruptiv teknik: Erfarenheter från två NATO-studier, FOI-R--3655--SE, december 2013.

lämpliga författare på FOI inom respektive område. En del författare är återkommande och bidrog även i den förra rapporten.

Denna gång gjorde vi en tydligare uppdelning. I tabell 1 visas strukturen.

**Tabell 1** Antologins struktur och delar. Uppdelningen gjordes tidigt i arbetet då de områden som beskrivs i antologin har något olika karaktär avseende tekniskt innehåll, tillämpning och koppling till förmåga.

| Antologins struktur och delar |
|---|
| **Inledning** – bakgrund, metod, läsanvisning med mera. |
| **Del 1: Strategiska trender** – global utveckling, konkurrens om teknik och råvaror, snabb teknikutveckling, teknikens roll i konflikter med mera. |
| **Del 2: Teknikområden** – informationsteknologi, intelligenta system, data, kvantteknik, bioteknik, material, energi med flera. |
| **Del 3: Förmågeområden** – plattformar i mark-, sjö- och luftdomänen, rymd, cyberförsvar och cybersäkerhet, ledning, obemannade och autonoma system, mänsklig förstärkning med flera. |
| **Del 4: Syntes** – observationer från Del 1-3, diskussion och avslutande kommentarer. |

Författarna ombads följa den ovan nämnda kapitelstrukturen vid textframtagningen. De har sedan själva valt vilken information som ska lyftas fram. Detta innebär att det finns skillnader i hur områden presenteras och i bland annat användningen av referenser. Vi kallar därför dokumentet för en antologi där varje teknikkapitel avslutas med en sammanställning av lästips för den som vill veta mer om området.

Texterna har diskuterats och kommenterats av redaktionen och, i de fall författarna önskat, av kollegor inom och utom myndigheten. Redaktörerna ansvarade för att skriva inledningen samt Del 1 och Del 4.

Som läsaren kommer att upptäcka finns det många kopplingar mellan teknikområdena och det tas också upp i den avslutande syntesen. Underlagen är dock framtagna oberoende av varandra. Ingen gemensam och övergripande analys med författarna av underlagen har genomförts.

Kapitlen i Del 2 och Del 3 enligt tabell 1 har en likartad struktur. Dock finns det en nyansskillnad mellan kapitlen i dessa bägge delar, vilken förklaras i inledningen till respektive del.

## Läsanvisning

I Del 1 presenteras ett övergripande resonemang om trender som idag påverkar eller påverkas av teknikutvecklingen. Därefter presenteras de olika teknik- och förmågeområdena i Del 2 respektive Del 3. I Del 4 redogör redaktörerna för observationer utifrån antologins inledande beskrivningar av teknik och förmåga i Del 2 och 3. Därutöver lyfts aspekter om hur teknikutvecklingen kan komma att påverka det framtida försvaret och militär förmåga.

Antologin är inte i första hand skriven för att läsas från pärm till pärm. Den erbjuder flera möjliga ingångar, exempelvis att inleda med Del 4 för en samlad överblick och därefter fördjupa sig i relevanta teknikområden, eller att direkt läsa de kapitel som är av särskilt intresse.

I tabell 2 framgår ordningen mellan kapitel samt kapitelrubrik och författare. Samtliga författare är anställda vid FOI, eller var det när de skrev sina kapitel.

## Avgränsningar

Vi har valt att göra antologin till en öppen publikation som kan ges en stor spridning. Detta påverkar i olika grad hur utförligt det går att beskriva de olika teknik- och förmågeområdena och hur skarpa slutsatser som kan dras. Vår bedömning är dock att denna begränsning mer än väl vägs upp av att vi kan presentera teknikutvecklingen på stor bredd.

Vi har också valt att endast använda författare från FOI. Vi är därför väl medvetna om att en del av de teknikområden vi presenterar har en betydligt kortare historia på FOI än andra. Det rör till exempel kvantteknik, bioteknik och energi där verksamhet på FOI startat på senare tid och nu är i olika stadier av tillväxt. Begränsningen till FOI innebär att vi inte omhändertar alla trender eller teknikområden, då den forskning som bedrivs vid myndigheten i huvudsak syftar till att stödja totalförsvaret.

**Tabell 2** Ämnesområden och författare till de olika kapitlen.

| Kapitel | Titel | Författare |
|---|---|---|
| | **Inledning** | Göran Kindvall, Anna Lindberg, Cecilia During |
| **Del 1** | **Strategiska trender** | Göran Kindvall, Anna Lindberg, Cecilia During |
| **Del 2** | **Teknikområden** | |
| | Inledning | Göran Kindvall, Anna Lindberg, Cecilia During |
| | Informationsteknologi | Jan-Erik Mathisen, Henrik Petersson |
| | Kommunikationsteknik | Erik Axell |
| | Intelligenta system | Joel Brynielsson |
| | Data | Björn Pelzer, Sinna Lindquist |
| | Kvantteknik | Per Jonsson, Jonas Kjäll |
| | Bioteknik | Petrus Hemström, Anna Lindberg |
| | Material | Linda H Karlsson |
| | Energi | Wilhelm Sahlén, Mattias Elfsberg, Niklas Zettervall |
| | Sensorsystem | Christina Grönwall |
| | Signaturanpassning | Hans Kariis |
| | HPM (High Power Microwave) | Tomas Hurtig, Mattias Elfsberg |
| | Laservapen | Matts Björck, Lars Sjökvist |
| **Del 3** | **Förmågeområden** | |
| | Inledning | Göran Kindvall, Anna Lindberg, Cecilia During |
| | Plattformar i markdomänen | Johannes Andersen |
| | Plattformar i sjödomänen | Linus Fast, Ron Lennartsson |
| | Plattformar i luftdomänen | Tomas Mårtensson |
| | Rymd | Jonatan Westman, Linn Claesson |
| | Cyberförsvar och cybersäkerhet | Teodor Sommestad, Henrik Karlzén |
| | Informationssystem | Fredrik Söderström |
| | Ledning | Niklas Hallberg |
| | Telekrig | Göran Kindvall, Gunnar Marcusson |
| | Obemannade och autonoma system | Martin Hagström |
| | Vapensystem | Martin Hagström |
| | Kärnvapen | Mattias Waldenvik |
| | Soldatsystem | Britta Levin, Hans Kariis, John Ottosson, Wilhelm Sahlén, David Bergström |
| | Mänsklig förstärkning | Britta Levin |
| **Del 4** | **Syntes** | Anna Lindberg, Cecilia During, Göran Kindvall |

# Del 1 – Strategiska trender

*Göran Kindvall, Anna Lindberg och Cecilia During*

## Inledning

Inte alls förvånande ser vi att teknikutvecklingen, som alltid sagts gå allt snabbare framåt, nu verkligen också gör det. Därtill finns stora skillnader mellan olika områden avseende i vilken omfattning teknik produktifieras. Detta noterade vi redan i den rapport som utkom 2020.[6]

I denna del av antologin tar vi upp trender vi ser idag som påverkar eller påverkas av teknikutvecklingen. Det handlar om den globala utvecklingen och den teknikkonkurrens vi ser mellan främst stormakterna, till exempel vad gäller strategiska råvaror. Det handlar också om de satsningar som görs på försvarsinnovation och de erfarenheter som kan fås från dagens konflikter, och då framför allt Rysslands fullskaliga invasion av Ukraina. Andra viktiga teman är den gröna omställningen, potentiellt snabbare materielproduktion och kompetensförsörjning.

## En osäker global utveckling

Idag råder en osäker geostrategisk situation som kan utvecklas i olika riktningar. Konsekvenser kan till exempel bli en förändrad maktfördelning mellan stater och ett växande inflytande för kommersiella aktörer som exempelvis har kontroll över den allt viktigare digitala infrastrukturen.

I dagens värld kan människor umgås via digitala redskap och sociala medier över alla landgränser. I diktaturer görs försök att begränsa och kontrollera människors möjligheter att interagera genom att till exempel styra vilka verktyg som tillåts eller att, som i Iran under oroligheterna i början av 2026, stänga av tillgängligheten till internet och telefoni för sin befolkning. I demokratiska nationer diskuteras istället hur man kan skydda sin befolkning, och speciellt unga, mot delar av det innehåll som sprids. Australien införde till exempel en 16-årsgräns för sociala medier i december 2025 och liknande begränsningar diskuteras även inom EU.

Allteftersom utvecklingen av teknik och metoder för påverkansoperationer fortskrider kan detta också ge ökade möjligheter att kontrollera vad människor tänker och tycker genom kognitiv påverkan. Detta i kombination med artificiell intelligens

6 Kindvall, G. och Lindberg, A. (red.), Militärteknik 2045 – Ett underlag till Försvarsmaktens perspektivstudie, FOI-R--4985--SE, november 2020, sida 211.

och en digital infrastruktur kan bli ett oerhört kraftfullt vapen såväl i fred som i kris och krig.

Klimatförändringarna pågår också mitt framför oss. Extremväder ökar skrämmande snabbt med översvämningar, höga temperaturer och bränder som följd. Detta påverkar människors livsbetingelser och kan också vara konfliktdrivande. Behovet växer av att säkra tillgång till såväl vatten och mat som råmaterial samt platser viktiga för flödet av dessa varor.

## Teknikkonkurrens

Idag är det framför allt Kina och USA som konkurrerar om att leda teknikutvecklingen. Den kinesiska policyn talar tydligt om att nå framgång genom tekniska framsteg och Kina dominerar volymmässigt forskningen inom allt fler områden. Även spetsforskningens omfattning växer. Ännu finns dock ett stort antal av de mest kvalificerade forskningsmiljöerna i Väst och då särskilt i USA.

Enligt World Innovation Index 2025 är de tre mest innovativa ekonomierna Schweiz, Sverige och USA. Det kan dock noteras att Kina tagit sig in på topp 10 (som 10:a).[7] När det gäller de starkaste innovationsklustren är Shenzhen-Hongkong-Guangzhou i topp före Tokyo-Yokohama och San Jose-San Francisco. På topp 6 finns även Beijing och Shanghai-Suzhou.

USA har en trumf på hand, genom att de största och globalt dominerande techbolagen (Google, Apple, Microsoft, Amazon, Meta, Nvidia med flera) har sin bas i USA. Detta kommer nog att fortsätta gälla under de närmaste åren. Men hur blir det 2050?

Både Kina och USA har traditionellt strävat efter samarbeten med andra länder för att stärka sin egen roll, få avsättning för sina produkter och få tillgång till råvaror och arbetskraft. Sådana aspekter är säkert också vägledande i Kinas val att inte fördöma Rysslands fullskaliga invasion av Ukraina. Ryssland är en utmärkt port till de råvaror som kan bli tillgängliga när Arktis is smälter som en effekt av klimatförändringarna.

## Kritiska råvaror och globala värdekedjor

Moderna mikrochip kallas halvledare då de till största delen innehåller halvledarmaterial. Dessa chip är en förutsättning för det moderna, digitaliserade samhället och kommer fortsätta att vara ytterst viktiga för att den tekniska utvecklingen ska kunna fortsätta. Detta gäller även för militär materiel som i allt högre grad blir

7 World Innovation Index 2025, World Intellectual Property Organization (WIPO), https://www.wipo.int/en/web/global-innovation-index/2025/index.

digitaliserad; en utveckling som sannolikt inte kommer att bromsas i framtiden. Därmed kommer forskningen och utvecklingen av halvledare och halvledarmaterial att fortsätta vara av yttersta vikt för Sverige och vår försvarsförmåga. Under covidpandemin påverkades de globala försörjningskedjorna, vilket bland annat ledde till brist på halvledare. Detta minskade i sin tur produktionen av många industriprodukter, som fordon, där halvledare ingår som centrala komponenter.[8]

Halvledare är ett bra exempel på en global värdekedja. Utvinningen av de råmaterial som krävs inom halvledarindustrin domineras i många fall av Kina. Vad gäller raffineringen (reningen) efter utvinningen är Kinas dominans än större. EU, och i ännu högre grad USA, strävar efter att bli mer oberoende avseende kritiska råvaror och deras bearbetning. Detta är dock en process som kommer att ta lång tid.

När det gäller tillverkningen av de mest kvalificerade halvledarna har Europa, eller snarare det nederländska företaget ASML, en betydande roll. ASML tillverkar den litografiska utrustning som krävs för att tillverka de mest avancerade halvledarna. Tillverkningen sker dock i stor utsträckning i Taiwan, Sydkorea och Japan. En särskilt stark aktör är det taiwanesiska företaget TSMC, som har en nära samverkan med ASML.

Vi har sett att råvaror och teknik alltmer blir spelpjäser i den globala konkurrensen, där Kina nyttjar sin dominans när det gäller strategiska råvaror som behövs i kvalificerade produkter och för den gröna omställningen. En konsekvens av denna globala teknikkonkurrens är också det, i USA och Europa, växande intresset för exportkontroll och granskning av utländska direktinvesteringar,[9] vilket innebär att Kina idag inte har tillgång till den utrustning som krävs för att tillverka de mest avancerade typerna av halvledare. Istället får de nöja sig med att ligga någon teknikgeneration efter Väst. Med de stora satsningar på teknikforskning som görs i Kina talar dock mycket för att de kommer att hämta in Västs försprång.

Här ser man också hur värdekedjor är komplicerade och består av flera steg där utvinning, raffinering, design och tillverkning kan finnas på olika platser och där någon nation eller något företag kan ha en dominerande roll i ett eller flera av dessa steg. Det skapas härvid beroenden som blir verktyg i det globala spelet.

För att säkerställa leveranser och tillgång krävs därför fungerande globala försörjningskedjor, som kopplar ihop utvinning, raffinering och de produktionssteg som behövs innan leverans kan ske av färdiga produkter, vilka också kan vara militära system. Kvalificerade militära system behöver kvalificerade komponenter. Ett exempel

8 En beskrivning av hur vi kommit dit där vi är när det gäller halvledare finns till exempel i Miller, C., Chip War – The Fight for the World's most Critical Technology", Simon & Schuster, Inc., 2022.

9 En ny svensk lagstiftning om granskning av utländska direktinvesteringar trädde i kraft den 1 december 2023, se Förordning (2023:624) om granskning av utländska direktinvesteringar, https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-2023624-om-granskning-av-utlandska_sfs-2023-624/.

på hur beroende militära system är av många olika råmaterial ges i en rapport av *Hague Centre for Security Studies* (HCSS).[10] Deras exempel är en nederländsk fregatt och man fann bland annat att radarsystemen innehöll gallium, bauxit, järn, nickel, molybden, krom och guld. Av dessa bedömdes tillgången till gallium ha störst risk för störningar i försörjningskedjan. Fregattens vapensystem innefattar ett drygt 20-tal ingående råmaterial.

Det finns olika indelningar av grundämnen, mineraler och metaller som i varierande grad anses viktiga av olika aktörer. Kritiska råmaterial omfattar alla typer av material som är kritiska för en tillämpning, dvs. utan det grundämnet eller mineralen kan något inte tillverkas. Sällsynta jordartsmetaller är ett antal (inte alls särskilt sällsynta) grundämnen vars betydelse ökar i dagens värld och som är viktiga för den gröna omställningen.

För att minska takten i och effekterna av klimatförändringarna blir tillgången till dessa råmaterial allt viktigare liksom processer för att förädla dem till användbara produkter såsom mikroelektronik eller sensorer. Som redan nämnts ovan kontrolleras idag till exempel en stor del av världens kritiska råmaterial av Kina och deras samarbetspartners. Dessa material används i både civila och militära tillämpningar. En modern smarttelefon innehåller exempelvis många sådana grundämnen i elektronik, pekskärm och batteri. Den som kontrollerar dessa material och vitala processteg kan sätta stor press på andra som behöver materialen. Vi är beroende av dessa material i det moderna samhället och en förlust av dem kommer att påverka oss påtagligt. Så länge Kina dominerar de processer som behövs för att materialen ska kunna användas i olika tillämpningar är beroendet av Kina fortsatt stort.

## Snabb teknikutveckling och försvarsinnovation

Teknikutvecklingen beskrivs i rapporter som producerats av bland annat Nato.[11] Produktifieringen av tekniska landvinningar visas genom alla de innovationsinitiativ som etablerats av såväl nationer som organisationer (till exempel EU och Nato) för att exploatera såväl civil som specifikt militär teknikutveckling.

Försvarstillämpningarna av teknik och de produkter, materiel och tjänster som teknikutvecklingen skapar övervägs och debatteras. Att ligga i framkant forsknings- och produktionsmässigt samt att använda civil teknik för att förbättra militära offensiva och defensiva förmågor lyfts fram som viktigt samtidigt som totalförsvarets

10 Patrahau, I. and Girardi, B., Raw material and supply chain vulnerabilities in the Dutch defence sector: An analysis of the Air Defence & Command Frigate, oktober 2024. Arbetet har utförts i samarbete med PwC.

11 S&T Trends 2025-2045.Denna publiceras i tre delar, där del 1 beskriver ett antal makrotrender, del 2 beskriver hur teknikutvecklingen kan bidra till de fem Warfare Development Imperatives (WDI) som är en del av NATO Warfighting Capstone Concept (NWCC) ) och del 3 utifrån en scenariokontext beskriver potentiella motståndares användning av innovativ teknik.

och industrins roll i detta åter har tagit plats på agendan. Här kan från svensk sida till exempel nämnas den strategiska inriktningen för försvarsinnovation som publicerats av Försvarsdepartementet[12] och det civil-militära innovationsprogram som drivs gemensamt av Försvarsmakten och Vinnova.[13]

I Militärteknik 2045 från 2020 tog vi upp USA:s tredje offsetstrategi och dess fokus på bland annat artificiell intelligens, autonoma system och samverkan mellan människa och system.[14] Syftet med en offsetstrategi är att uppnå en asymmetrisk fördel gentemot sina motståndare, vilket är ett bärande motiv för exempelvis de strävanden som kollektivt görs inom Nato för att gemensamt upprätthålla teknologisk spets gentemot alla tänkbara motparter.

När detta skrivs har det amerikanska krigsdepartementet (som det amerikanska försvarsdepartementet nyligen bytt namn till) publicerat en ny prioriterad tekniklista. På den finns tillämpad AI, biotillverkning och tillämpningar av kvantteknik, och utöver dessa finns också en ambition att skala upp användningen av elektromagnetiska och hypersoniska vapen. Det sjätte området handlar om att kunna bedriva logistik under hög hotnivå på ett komplext slagfält.

I den senaste versionen av Natos *Science and Technology Trends*, med tidsperspektivet 2025–2045, fokuserar den första delen på att identifiera och beskriva ett antal så kallade makrotrender. De sex makrotrender som beskrivs har förmåga att både påverkas av och påverka teknikutvecklingen. De beskrivna trenderna är:

- Evolving competition areas
- Race for AI and quantum superiority
- Biotechnology revolution
- Resource divide
- Fragmenting public trust
- Technology integration and dependencies.

De tre första punkterna har ett i huvudsak tekniskt fokus och beskriver teknikområden som är intressanta både civilt och militärt. Trenderna visar sammantaget det ekosystem militär förmågeutveckling befinner sig i. Dagens materiel och försvarsförmåga är ett resultat av samverkande områden, aktörer och nationer i

12 Strategisk inriktning för försvarsinnovation, https://www.regeringen.se/contentassets/38380ae279be406a9775a6d54002503e/strategisk-inriktning-for-forsvarsinnovation.pdf.

13 Nytt program för civil-militär innovation, https://www.vinnova.se/nyheter/2024/06/civila-innovationer-ska-starka-sveriges-forsvarsformaga/.

14 Offset betyder här att det är en strategi för att ta tillbaka initiativet, det vill säga att åter bli övermäktig en motståndare som har anpassat sig till dagens vapen och taktik. De två tidigare offsetstrategierna har varit fokuserade på kärnvapenavskräckning respektive precisionsvapen och ISR (intelligence, surveillance, reconnaissance).

samförstånd och med bi- och multilaterala avtal. Mycket av det som är civilt relevant är även militärt relevant och vice versa.

De av Nato listade trenderna, då i synnerhet de tre sista punkterna, visar också på de strategiska, samhällsdrivna, ekonomiska och säkerhetspolitiska aspekterna av militär förmågeutveckling.

Idag lyfts också ofta att det råder en tilltagande osäkerhet vad gäller politiska allianser, ekonomisk utveckling och global handel, faktorer som kan komma att påverka alla världens nationer och tvinga fram nya samarbeten.

Storbritannien har under 2025 publicerat en *Strategic Defence Review* (SDR).[15] I beskrivningen av den strategiska kontexten mot 2040 lyfter de:

- Growing multipolarity and intensifying strategic competition
- Rapid and unpredictable technological progress.

Denna strategiska kontext behöver hanteras mot en bakgrund av klimatförändringar, fortsatta hot från terrorister och demografiska förändringar. De senare sker ojämnt och påverkar globala balanser och kan inverka på både nationell och regional stabilitet.

Sammantaget görs i SDR bedömningen att det brittiska försvaret behöver förbereda sig för en mer utmanande värld med hårdare konkurrens och ett större antal kriser och konflikter som kombinerar konventionell krigföring med ett ökat inslag av insatser under tröskeln samtidigt som det finns hot om användning av massförstörelsevapen.

## Disruptivt och konvergent

Mycket av intresset när det gäller teknikutveckling riktar sig mot det som brukar kallas disruptiv teknik och innovation. Andra ord som brukar användas synonymt med disruption är omvälvande eller banbrytande teknik. Oavsett ordval handlar det om teknikutveckling som innebär att etablerade beteenden och förutsättningar förändras. I försvarssammanhang kan det till exempel vara något som gör att existerande förmågor och system inte längre kan räcka till för att hantera de nya hoten. Sådana skeenden kan benämnas omslagspunkter.

Omslagspunkterna kan ses utifrån två perspektiv där det första handlar om att prolongera utvecklingen inom specifika teknikområden för att försöka förstå när de kan nå en punkt där konsekvenserna kan bli enorma, kanske genom konvergens med andra tekniker. Det andra sättet är att identifiera ett antal tillämpningar som verkligen skulle kunna förändra förutsättningarna för konflikter. I en tidigare

15 Strategic Defence Review. Making Britain Safer: secure at home, strong abroad, UK MoD 2025.

rapport diskuteras, som exempel på sådana genombrott, förmågan att vara osynlig på stridsfältet (osynlighetsmantel), att havsmiljön blir helt genomskinlig för spaning (transparent hav) eller artificiell superintelligens.[16] Vad som krävs för att dessa tillämpningar ska vara möjliga, om det överhuvudtaget är möjligt och när det i så fall inträffar återstår att se. Detsamma gäller den motmedelsutveckling som kommer att bedrivas parallellt.

Konvergens handlar om att områden samverkar i sin utveckling och till exempel möjliggör eller förstärker varandra. AI är ett exempel på ett sådant område genom sin förmåga att kunna identifiera nya potentiella material med önskvärda egenskaper eller biotekniska tillämpningar. Exemplen på konvergenser såväl på teknik- som systemnivå kommer att bli fler i framtiden och vi behöver successivt öka vår förståelse för konvergensfenomen.

## Teknikens roll i konflikter

Kriget i Ukraina har bidragit till att försvarsfrågor hamnat i blickpunkten. Det är, likt tidigare krig, en katalysator för teknisk utveckling och snabb innovation inom krigföring. Takten, och behovet av att snabbt kunna förändra metod och uppträdande i kamp med en kvalificerad angripare, är uppmärksammade utmaningar. Kombinationen av traditionella system och innovativa tillämpningar av till exempel drönarteknik har rönt stor uppmärksamhet i media, men också i många länders försvarsmakter. Drönare är en plattform som kommer i många olika skepnader och kan bära olika system och förmågor. De används för spaning, invisning, operationer i angriparens territorium, diverse typer av vapenverkan, för kommunikation och har till och med använts för att underlätta desertering.[17] Nya medel ger behov av motmedel. Ett exempel är det laservapen som Ukraina presenterade i april 2025. Laservapnet uppges kunna bekämpa bland annat drönare på flera kilometers håll.[18]

På samma gång som innovationerna uppmärksammats har kriget också innehållit moment som närmast liknar första världskrigets skyttegravskrig. Detta illustrerar att väpnade konflikter kan pågå i olika tekniska och taktiska generationer samtidigt. Kriget i Ukraina har också visat att åtgången av ammunition kan vara enorm i dagens krig.

16 Kindvall, G., och Tarras-Wahlberg, B., Det framtida tekniklandskapet: En översikt, FOI-R--5049--SE, april 2021.

17 Ukraine is offering Russian soldiers detailed instructions on how to surrender to its drones, New York Times, 26 december 2022, https://www.nytimes.com/2022/12/26/world/europe/ukraine-is-offering-russian-soldiers-detailed-instructions-on-how-to-surrender-to-its-drones.html.

18 Ukrainian Tryzub laser system shown for the first time: Revealed at what range it can destroy targets, Defense Express 13 april 2025, https://en.defence-ua.com/weapon_and_tech/ukrainian_tryzub_laser_system_shown_for_the_first_time_revealed_at_what_range_it_can_destroy_targets-14168.html.

## Klimatanpassning och grön omställning

I och med att klimatförändringarna blir allt påtagligare ökar behovet av att minska klimatpåverkan genom att ersätta traditionella material och produkter med miljövänligare varianter som kan återbrukas eller återvinnas. Grönare alternativ kan exempelvis vara att använda el som drivmedel eller att ersätta oljebaserad plast och smörjmedel med biobaserade alternativ. Ett annat sätt att minska klimatpåverkan är att minska vikt och öka tålighet och livslängd hos materiel för att minska energi- och underhållsbehoven. Idag är olika kritiska råmaterial vitala för tillämpningar som kan möjliggöra den gröna omställningen. I framtiden kan nya tekniska vinningar bidra till grön omställning men också ersätta en del av beroendet av de kritiska råmaterialen.

Beroende på vilka material och tekniker som kommer kunna ersätta traditionella material med stor miljöpåverkan kommer Försvarsmakten och försvarets förmåga att påverkas. En utfasning av diesel och bensin till förmån för el kommer ha stor påverkan på Försvarsmaktens materiel och doktrin. Arbetssätt och tankesätt kommer behöva förändras fram till år 2050. Nato bedriver arbete för att bedöma effekterna av klimatförändringarna på försvar och säkerhet, och studerar också hur militära resurser kan minska sina klimatavtryck.[19]

## Produktion av förmåga

Ett på senare tid trendande begrepp inom försvarssektorn är *rapid adoption*, i meningen att snabbt omsätta ny teknik till militär förmåga.[20] Detta är givetvis inspirerat av vad Ukraina lyckats med efter Rysslands fullskaliga invasion men ses också som ett alternativ för andra länder och i fredstid, både för att vara beredda vid en attack och för att verka avskräckande.

Fokuseringen på att snabbt skapa förmåga sammanfaller också med att teknikutvecklingen övergått från något som studerats i sig och med fokus på utvecklingen inom enskilda teknikområden till att bli en fråga om hur teknik bidrar till befintlig eller önskad förmåga och hur teknikutvecklingen inom olika områden konvergerar, dvs. hur de samverkande förstärker varandra.

I detta sammanhang är det också viktigt att hantera den globala konkurrensen om att leda teknikutvecklingen inom strategiskt viktiga teknikområden och försöken att försäkra sig om tillgång till alla steg i värdekedjan för relevanta produkter. Rådigheten handlar om kritiska råmaterial, komponenter som halvledare och tillgång

19 The Effects of Climate Change on Security, STO-TR-SAS-182, ISBN 978-92-837-2614-2, januari 2026. Rapporten är tillgänglig på https://www.sto.nato.int/document/the-effects-of-climate-change-on-security/.

20 Summary of NATO's Rapid Adoption Action Plan, 25 juni 2025, https://www.nato.int/cps/en/natohq/official_texts_236539.htm.

till industriell kapacitet kapabel att tillverka bland annat ammunition, vapensystem och militära plattformar i tillräckligt antal. En trend är därför ett tätare samarbete mellan stat(er) och industri i akt och mening att upprätthålla en uthållig försvarsindustri med tillräckligt stor produktionskapacitet över tid.

## Kompetensförsörjning

I Sverige diskuteras det hur man kan få en bättre matchning mellan arbetssökande och de lediga jobb som finns hos företag och andra arbetsgivare. Samtidigt som arbetslösheten inte går ner finns det stora behov nu och framåt inom bland annat tekniska yrken och inom vårdsektorn. Som exempel är behovet av cybersäkerhetspersonal betydligt större än tillgången på densamma. Sådana obalanser leder också till att tillväxten hämmas inom vissa branscher.

Dylika brister och obalanser påverkar också försvarssektorn. Under senare år har det genomförts arbete med att öka kunskapen om hur teknikutvecklingen kan påverka militär personalförsörjning på sikt. I en rapport från 2021 inom Försvarsmaktens FoT-beställning analyseras frågeställningarna ”Vad är forskningsläget på teknikutvecklingens påverkan på arbetsmarknaden i stort och på personalbehov inom organisationer?” och ”Hur kan detta appliceras på en militär kontext?”.[21] Rapporten bedömer att Försvarsmakten står inför vissa utmaningar, framförallt på kort sikt, när det gäller samspelet mellan teknik och personalförsörjning. Detta avser främst att på ett flexibelt sätt tillgodose nya och förändrade kompetensbehov i ljuset av en i vissa delar rigid personalförsörjningsstruktur med långa ledtider.

Mot 2050 kan dessutom behovet av mänsklig arbetskraft se helt annorlunda ut än idag även inom försvarssektorn.

21 Johansson, Teknikutvecklingens påverkan på militär personalförsörjning, FOI-R--5089--SE, februari 2021.

# Del 2 – Teknikområden

## Inledning

*Göran Kindvall, Anna Lindberg och Cecilia During*

I denna del fokuserar vi på teknikområden.

De teknikområden som kanske är föremål för mest hajp är kvantteknik, bioteknik och AI. Samtidigt finns det andra områden, till exempel material och energi, som bland annat är nödvändiga möjliggörare för många tillämpningar. Vi tar också upp elektromagnetiska vapen (HPM och laser) som var föremål för hajp på 90-talet, och som efter vissa tekniska motgångar åter seglar upp, nu bland annat för att de har potential mot ett av dagens (och, enligt många, framtidens) kanske mest diskuterade vapensystem – drönare. En annan fråga som är relevant både nu och i framtiden är förmågan att verka dolt i en värld av allt fler sensorer. Utvecklingen inom sensorteknik och signaturanpassning beskrivs också i denna del av antologin.

Ett område som vi hanterade relativt kortfattat i rapporten från 2020 (Militärteknik 2045) var informations- och kommunikationsteknik. I denna antologi har vi tagit ett större grepp på detta centrala område och i denna del beskriver vi utvecklingen inom informationsteknik, kommunikationsteknik, data och intelligenta system. I Del 3 beskriver vi sedan utvecklingen inom de relaterade förmågeområdena cyberförsvar och cybersäkerhet, informationssystem och ledning.

Strukturen för kapitlen i denna del är:

- Inledande beskrivning
- Trender och exempel
- Särskilda delområden
- Samverkande och förutsättande teknikområden
- Påverkan på militär förmåga
- Aktörer
- Lästips

# Informationsteknologi

*Jan-Erik Mathisen och Henrik Petersson*

## Inledande beskrivning

Begreppet informationsteknologi används här som ett samlingsbegrepp för metoder och teknik som understöder och möjliggör förmågor inom områden som informationssystem, intelligenta system, ledning och kommunikation. Exempel på informationsteknologier är datorsystem, beräkningshårdvara, molnteknologi samt metodik och teknik för överföring, lagring och bearbetning av data och information.

Datorers kapacitet att lagra, bearbeta och analysera information är fortsatt en avgörande drivkraft bakom den tekniska utvecklingen och det är rimligt att anta att informationsteknologins betydelse kommer att fortsätta öka fram till 2050. Huvuddelen av utvecklingen inom informationsteknologi drivs idag av den civila marknaden vilket ger hög tillgång och storskalighet men samtidigt skapar utmaningar gällande anpassningar som krävs för användning inom säkerhet och försvar. De stora framstegen kommer även fortsatt att drivas av konsument- och företagsmarknaden; framtida militära system kommer till största delen bestå av civila komponenter. Till följd av ökade krav på militära förmågor och växande försvarsbudgetar så är dock en möjlig eller trolig trend att riktad utveckling kan komma att ske inom nischade delar (av informationsteknologi) som är speciellt särpräglade och viktiga för militära tillämpningar. Det kan gälla komponenter som är strålningshärdade eller har inbyggda säkerhetsskydd – kretsar som saknar direkt motsvarighet i konsumentprodukter. Detta kan ge upphov till en tilltagande militär kapprustning inom informationsteknologi.

## Trender och exempel

Vid horisonten fram till 2050 finns det potentiellt revolutionerande tekniksprång. Kvantteknik är ett tydligt exempel. Kvantdatorer kan, om de når praktisk och storskalig mognad, kraftigt påverka många av dagens krypteringssystem samt ge beräkningsmöjligheter inom områden som är svåra eller omöjliga för klassiska datorer. Särskilt betydande är potentiella genombrott inom optimering, logistik, kvantkemi och materialvetenskap, där kvantdatorer och kvantsimuleringar kan omdefiniera hur problem modelleras och löses.

Kvantteknikens utvecklingstakt är dock osäker. Bedömningar varierar, men många experter placerar de första verkligt kraftfulla och felkorrigerade kvantdatorsystemen

någon gång mellan 2030- och 2040-talet.[22,23] Fullskaliga, allmänt tillämpbara system kan dröja längre. Kvantdatorutvecklingen drivs främst av de största IT-bolagen och tillgången sker idag huvudsakligen via molntjänster. På sikt kan kvantdatorer komma att erbjudas kommersiellt på ett sätt som liknar hur beräkningskluster anskaffas idag. Se även kapitlet om kvantteknik.

Bortsett från osäkerheten om när kvantdatorn blir verklighet så kommer tekniklandskapet för datorsystem att präglas av sammankopplingen av många framsteg: förbättrade konventionella chip (kanske ned mot atomär skala), innovativa arkitekturer (3D, specialkretsar), kvant- och optoteknik för särskilda ändamål (kryptering, navigering, signalbehandling), samt en allmän strävan efter högre prestanda i förhållande till energikonsumtion. Kombinationen av dessa faktorer avgör hur kraftfull vår informationsteknologi är år 2050.

### Datorkraft

Under de senaste decennierna har processorutvecklingen följt Moores lag, vilket har inneburit en fördubbling av antalet transistorer (och därmed beräkningskraft) som får plats på en processor ungefär vartannat år. Denna exponentiella tillväxt har drivit fram en enorm ökning av digital kapacitet som påverkat alla delar av samhället, inklusive det militära.

Nu när Moores lag närmar sig sina fysiska gränser (transistorer kan inte krympas i all oändlighet på kiselbaserade chip) tvingas forskare och industri att söka nya datorarkitekturer och material för att upprätthålla ökningen i prestanda. Under det kommande decenniet väntas konventionell kiselteknik stöta på hinder som enbart kan övervinnas med nya koncept och radikala innovationer. Parallellt med att transistortätheten planar ut har behoven inom militära system fortsatt växa. Stora datamängder, realtidskrävande tillämpningar och avancerad AI ställer krav på flera storleksordningar högre beräkningskapacitet än idag.

Förväntade behov av dramatiskt högre beräkningskapacitet har lett till intensifierad global forskning inom ett flertal teknikområden, som genom att utnyttja nya fysikaliska fenomen, arkitekturella paradigm eller tillverkningstekniker, syftar till att bryta igenom dagens prestandabegränsningar. Exempelvis utforskas fotoniska datorer bestående av komponenter baserade på ljus (fotoner) istället för elektroner. Neuromorfiska processorer använder kretsar och beräkningsarkitekturer som efterliknar hjärnans neuronnät. Man utforskar tekniker för tredimensionell hopkoppling av kretsar och undersöker potentialen hos halvledarmaterial bortom kisel (som galliumnitrid eller 2D-material).

22 "The timelines: when can we expect useful quantum computers?" IntrotoQuantum.org (2024). Där står att "the first applications could be within reach around 2035–2040.".

23 Boston Consulting Group (BCG). "The Long-Term Forecast for Quantum Computing Still Looks Bright." (2024). De delar upp utvecklingen i: NISQ-eran fram till ~2030, bred kvantfördel 2030-2040, och fullskalig felkorrigerad kvantdator efter 2040.

Stora aktörer, både nationer och företag, investerar inom dessa områden – Kina satsar t.ex. på nya halvledarmaterial för att uppnå ett teknologiskt försprång.

### Energiförbrukning

En bieffekt av ständigt kraftfullare datorer och samhällets digitalisering är stigande energibehov. Elanvändningen från datacenter/AI växer snabbt. IEA:s prognos visar runt 945 TWh[24] globalt 2030, vilket är en fördubbling mot idag. Detta understryker vikten av energieffektiva lösningar, t.ex. specialiserade kretsar, förbättrad kylteknik och energisnålare arkitekturer, för att upprätthålla utvecklingstakten. Redan idag planeras nästa generations superdatorer med fokus på att hålla strömförbrukningen hanterbar genom innovationer i både hårdvara och programvara.

### Lagring

Tekniken för dataminnen kommer sannolikt att genomgå en stor omvandling. Traditionellt dominerar separata hierarkier av snabbt men flyktigt primärminne (SRAM, DRAM) och långsamt icke-flyktigt lagringsminne (flash, magnetdisk). Fram till 2050 förväntas nya typer av icke-flyktiga minnen med hög hastighet – såsom resistiva RAM (ReRAM), magnetiska RAM (MRAM) och fasändringsminnen (PCM) – få ökad användning i utvalda segment och som komplement till DRAM/NAND[25]. Dessa kan fungera som *Storage Class Memory*, dvs. förena egenskaperna hos arbetsminne och lagring i en enda teknik. Det skulle minska flaskhalsar vid dataöverföring och möjliggöra att stora datamängder bearbetas närmare processorn. En annan trend är minnesnära och inbyggd lagring (t.ex. *High Bandwidth Memory*[26] staplade på CPU/GPU-kretsar) för att öka bandbredden och kapa tidsfördröjning mellan beräkningsenhet och minne. Alternativa minnesteknologier har dessutom fördelen att de ofta är strålningshärdiga, vilket är värdefullt för rymdbaserat och militärt bruk där hög strålningsnivå kan orsaka felaktig data. Samtidigt kvarstår utmaningar – nya material och tillverkningsprocesser behövs för att kunna skala upp dessa minnestekniker ur ett ekonomiskt och praktiskt perspektiv. Bedömare förutspår ändå att de kommande decennierna kommer att innebära ett genombrott där flashminnen och DRAM gradvis kan ersättas eller kompletteras av t.ex. MRAM i både inbyggda system och storskaliga minneschip. Resultatet blir att framtidens datorsystem kan lagra och flytta data mycket mer effektivt än idag, vilket är kritiskt för dataintensiva militära applikationer som realtidsanalys av sensorinformation.

---

24 IEA – Energy and AI: Energy demand from AI (Base Case ~945 TWh 2030): https://www.iea.org/reports/energy-and-ai/energy-demand-from-ai.

25 NAND-minne är en typ av icke-flyktigt flashminne som kan lagra stora mängder data och som behåller data även utan strömförsörjning.

26 All About Circuits (2025-04-28): HBM4 up to 2 TB/s & 64 GB per stack: https://www.allaboutcircuits.com/news/jedec-officially-releases-hbm4-memory-standard/.

## Särskilda delområden

### Teknologier för effektiv beräkning

Trenden är att modeller och system för artificiell intelligens blir allt mer komplexa och därmed allt mer beräkningskrävande. På olika sätt försöker man möta upp dessa krav med nya teknologier för effektiva beräkningar, oftast genom att specialisera hårdvaran för att passa den typ av beräkningar som är vanliga i AI-system.

#### *Fotoniska datorer*

Fotoniska datorer utnyttjar ljus (fotoner) för beräkningar istället för elektriska signaler. *Silicon photonics* (integrerad fotonik på kisel) har på senare år vuxit fram som ett lovande sätt att drastiskt öka hastigheten på dataöverföring och bearbetning. Genom att manipulera ljus i chip i stället för elektroner kan man uppnå mycket hög bandbredd och låg energiförbrukning, eftersom fotoner rör sig snabbare och utan resistiv värmeförlust. Dessa egenskaper gör fotoniken attraktiv för militär höghastighetsdatabehandling, exempelvis realtidsanalys av sensorinformation från radar och ISR-system (*Intelligence, Surveillance, Reconnaissance*) där enorma datavolymer måste bearbetas momentant. Fotoniska specialprocessorer kan också accelerera kryptering/dekryptering och signalbehandling, vilket gynnar säkra kommunikationer.

En underkategori är neuromorfisk fotonik, där optiska kretsar efterliknar neuronnät. Analoga och neuromorfiska fotoniska beräkningar erbjuder en väg att kringgå begränsningar hos traditionella datorer (med t.ex. von Neumann-arkitektur[27]). Genom att bearbeta information med ljus i neuronnätsliknande strukturer kan man potentiellt uppnå beräkningshastigheter som är många gånger högre än vad dagens elektroniska neurala nät klarar. Detta är särskilt intressant för AI- och ML-applikationer inom försvaret, som bild- och mönsterigenkänning i drönarsvärmar eller antimissilsystem som kräver blixtsnabba beslut. Redan idag finns experimentella optiska acceleratorer för t.ex. Fourier-transformer och konvolutioner, och fram till 2050 förväntas fotoniska datorer vara mogna för att hantera komplexa beräkningar med hög pålitlighet. Militära applikationer kan inkludera optiska datorer ombord på satelliter (för bildanalys utan radiolänkfördröjning) eller i stridsflygplan, där viktiga algoritmer kan köras mycket snabbare och med mindre värmeförlust jämfört med konventionell elektronik. Fotoniska datorer förväntas generellt vara mindre känsliga för transienta fel från strålning än traditionella elektroniska datorer, men inte helt immuna: de elektriska gränssnitten och materialen kan fortfarande påverkas. En utmaning är dock att integrera laserkomponenter och

27 En absolut majoritet av dagens datorer är konstruerade enligt en Von Neumann arkitektur. Arkitekturen beskriver en dator uppdelad i ett antal centrala komponenter: en kontrollenhet för sekventiell exekvering av instruktioner och beräkningar, en beräkningsenhet för aritmetiska beräkningar, ett minne för lagring av data och instruktioner, ett långtidsminne samt en mekanism för hantering av in- och utdata.

optiska vågledare på chip – tillverkning av fotoniska kretsar är fortfarande tekniskt krävande. Därför väntas hybrida lösningar, där elektroniska och fotoniska delsystem kombineras, dominera åtminstone under de närmaste årtiondena.

*Neuromorfiska processorer*

Neuromorfiska processorer är designade för att efterlikna den biologiska hjärnans beteende och arkitektur bestående av neuroner sammankopplade via nät av synapser. Istället för traditionella sekventiella beräkningar utnyttjar de parallellism och spikbaserad informationsöverföring[28] likt biologiska nervsystem. Syftet är att uppnå hög effektivitet vid kognitiva uppgifter som igenkänning, beslut och sensorfusion. Redan idag finns prototyper som IBM:s TrueNorth och Intels Loihi som innehåller motsvarande miljontals "neuroner" på ett chip. Amerikanska flygvapnets forskningslaboratorium (AFRL) demonstrerade 2018 världens då största neuromorfiska dator, *Blue Raven*, med 64 miljoner artificiella neuroner och 16 miljarder synapser – och som endast förbrukade 40 W effekt.[29,30] För militären innebär neuromorfiska chips möjlighet till AI direkt i fält; man kan placera intelligens i sensorer, fordon eller robotar utan att vara beroende av strömkrävande datacenter. Till exempel skulle en autonom spaningsdrönare med neuromorfisk processor kunna utföra avancerad målsökning, bildtolkning och beslutstagande ombord i realtid, med minimal energiförbrukning – något som ökar uthålligheten och minskar behovet av datalänksbandbredd.

Neuromorfiska processorer är särskilt lämpade för uppgifter inom mönsterigenkänning, klassificering och adaptivt lärande, vilka är centrala i militära tillämpningar som signalspaning, intrångsdetektion inom cybersäkerhet och förarstöd i fordon. Deras arkitektur ger också inneboende tolerans mot fel och brus, likt biologiska system, vilket är attraktivt ur robusthetssynpunkt i stridsmiljöer. Emellertid har de neuromorfiska systemen än så länge begränsad programmerbarhet – det krävs nya algoritmer och tänkesätt för att utnyttja dem fullt ut. Fram till 2050 förväntas dock utvecklingen leda till hybridlösningar där neuromorfiska enheter samverkar med konventionella datorer.

28 Spikbaserad informationsöverföring avser en kommunikationsprincip, där information kodas och överförs som diskreta händelser (spikar) snarare än som kontinuerliga signaler. Varje spik representerar en tidsbestämd signal från en artificiell neuron, och det är främst tidpunkten, frekvensen eller mönstret av spikar som bär informationen. Detta möjliggör mycket energieffektiv och parallell informationsbehandling, eftersom beräkning och kommunikation endast sker när spikar genereras.

29 DataCenterDynamics (2018-07-27): Blue Raven (~40 W): https://www.datacenterdynamics.com/en/news/us-air-force-ibm-unveil-worlds-largest-neuromorphic-digital-synaptic-supercomputer/.

30 USAF/AFRL (2018-07-24): Blue Raven neuromorphic system: https://www.wpafb.af.mil/News/Article-Display/Article/1582310/afrl-ibm-unveil-worlds-largest-neuromorphic-digital-synaptic-super-computer/.

*3D-chipintegration*

Traditionella integrerade kretsar är tvådimensionella, men genom 3D-chipintegration kan man stapla flera lager av halvledare och på så vis öka packningstätheten och förkorta avståndet mellan komponenter. 3D-integration finns redan i form av staplat minne (t.ex. HBM – högbandbreddsminne) på logikkretsar. Nästa steg är att även stapla logikenheter, analoga komponenter och diverse specialchip ovanpå varandra i ett heterogent 3D-paket. Fördelen är att man kan kombinera olika tillverkningsteknologier (olika material, noder, etc.) och skapa ett kompakt system-i-paket (SiP) istället för ett enda monolitiskt chip. Detta möjliggör fortsatt prestandaökning även när transistorförminskningen avstannat – flera mindre chip ("chiplets") kan integreras för att tillsammans fungera som en enhet med högre prestanda än vad varje enskilt chip klarar. I praktiken kan man exempelvis ha en stapel bestående av processorlager, minneslager, radiosändarmoduler och AI-acceleratorer, allt sammanbundet med vertikala förbindelser (kisel-genomföringar, optiska länkar etc.). För militära system innebär 3D-integration att mer funktionalitet ryms i ett litet format, vilket är kritiskt i t.ex. trånga plattformar (missiler, nanosatelliter, personburna wearables för soldater). Dessutom kan överföringshastigheten av signaler mellan lagren bli mycket hög och med låg fördröjning, vilket är viktigt för realtidskritiska tillämpningar som eldledning och aktiva självskyddssystem.

En betydande utmaning för 3D-chip är värmehantering. När flera lager av högpresterande logik staplas alstras mycket värme inom en liten volym, vilket idag begränsar antalet lager man praktiskt kan stapla. DARPA[31] har initierat forskningsprogram för att lösa detta, t.ex. genom att integrera nya avancerade strukturer och metoder för kylning inuti stapeln. Om detta och liknande forskningsprogram blir framgångsrika och dagens hinder orsakade av otillräcklig värmehantering övervinns kan vi år 2050 se 3D-kretsar med avancerade inbyggda system för kylning och därmed fullständiga system på chipstaplar där hela datorer med multipla processorer, minnen och sensorer är integrerade i en enda modul. Resultaten från teknikutvecklingen pekar mot att heterogen integration kommer vara en nyckelteknik för att uppnå fortsatta ökningar i beräkningskapacitet framöver. Militära högpresterande datorsystem, som stridsledningscentraler eller avancerade spaningssystem, kan dra nytta av 3D-integrerade processorer med betydligt högre effektivitet och packning. Även mindre system som precisionsammunition kan få inbyggd "smarthet" via 3D-kretsar som kombinerar sensorer och datorer i minimala format.

31 Defense Advanced Research Projects Agency. DARPA är ett oberoende forskningsinstitut inom det amerikanske försvarsdepartementet med uppdrag att bedriva och finansiera forskning i syfte att utveckla kvalificerad teknologi för militära ändamål.

## Arkitekturer

Utöver effektivare hårdvara kan beräkningar påskyndas genom teknologier för att utföra beräkningar distribuerat och parallellt. I kommersiella sammanhang används system för distribuerad beräkning flitigt för att möjliggöra t.ex. analys av stora datamängder (*Big data analytics*). Försvarsindustrin har börjat följa efter denna trend med arkitekturer som inkluderar molnbaserade datacenter, framskjutna serverlösningar och edge-enheter.

### *Nya datorsystemarkitekturer och AI-acceleration*

Traditionella (sekventiella) von Neumann-arkitekturer får allt mer sällskap av heterogena arkitekturer. För att höja både hastighet och energieffektivitet designas heterogena system där olika typer av processorer samverkar. Redan idag kombinerar system kraftfulla CPU:er med specialkretsar som GPU:er, AI-acceleratorer (t.ex. TPU:er) och FPGA:er för att hantera specifika uppgifter extremt effektivt. Denna trend väntas tillta – år 2050 är det troligt att majoriteten av datorsystem är skräddarsydda med flera samverkande beräkningsenheter optimerade för bland annat artificiell intelligens, signalbehandling och kryptografi. Utvecklingen inom AI är särskilt drivande; moderna AI-modeller kräver enorm beräkningskraft, och både civila bolag och försvarsorganisationer investerar i hårdvara som drastiskt kan snabba upp AI-beräkningar.

Sammanfattningsvis rör vi oss mot en era där specialiserad och parallell databehandling är normen, med klassiska flerkärniga CPU:er som en del av större ekosystem av beräkningsenheter snarare än en ensam huvudenhet.

### *Edge computing och distribuerade system*

En tydlig trend är att system och nätverk av datorresurser designas med en förflyttning av beräkningskraft ut mot nätverkets kant – så kallad *edge computing*. Istället för att all data skickas till centrala servrar eller molnservrar för bearbetning utförs mer analys lokalt på enheter som sensorer, fordon eller maskiner. Målet är att minska fördröjning, avlasta nätverkstrafik och öka robusthet. I civila tillämpningar ser vi redan hur enheter knutna till sakernas internet (eng. *Internet of Things*, IoT) och smarta sensorer får inbyggda mikroprocessorer för att direkt behandla data. Till 2050 väntas autonoma fordon, smarta städer och industriella IoT-system kraftigt öka mängden distribuerad intelligens vid nätverkets utkant.

Militära tillämpningar speglar detta mönster. Modern krigföring förlitar sig på ett nätverk av sensorer och plattformar – från drönare och soldatburna sensorer till stridsflygplan – som alla behöver kunna fatta snabba beslut utan att vara beroende av en central datalänk i realtid. *Edge computing* har redan introducerats i avancerade vapensystem. Exempelvis utnyttjar moderna stridsflygplan som Gripen E och F-35 en mängd inbyggda sensorer och datorer ombord för att i realtid sammanfoga

data (sensorfusion) och ge piloten en helhetsbild utan fördröjning.[32,33] F-35:ans system delar även information direkt mellan flygplanen i en gruppering.[34] Detta är praktiskt taget *edge computing* i luften, där varje flygplan är en nod i ett nätverk som bearbetar och utbyter data lokalt. Likaså utrustas soldater med kroppsburna sensorer och datorer som kan analysera omgivningen och hjälpa till med t.ex. måldetektion på fältet.

Till 2050 förväntas *Internet of Battlefield Things* (IoBT)[35] vara en etablerad realitet, dvs. ett stort antal uppkopplade enheter på slagfältet som kontinuerligt samlar in och delar data. För att detta ska fungera, trots störningar och hot, kommer lokal datorkraft ute på fältet vara avgörande. *Edge computing* ger militären möjligheten att ha tillgång till beslutsstöd, lägesbild och data även om kommunikationen till central infrastruktur bryts eller störs. Samtidigt återspeglar detta trenden i civilsamhället, där t.ex. autonoma bilar måste kunna fatta beslut även om molnuppkopplingen tillfälligt försvinner. Kort sagt suddas gränsen ut mellan central och distribuerad databehandling – framtidens system är i hög grad distribuerade för både civilt och militärt bruk.

### *Moln och molntjänster*

Molnteknologi har förändrat hur både civila och militära organisationer hanterar beräkning, lagring och tjänstetillgång. I den civila sektorn utvecklas molntjänster mot allt mer centraliserade *hyperscale*-datacenter, kompletterade av *edge* och *fog computing*[36] för att hantera fördröjning och tillgänglighet. Fokus ligger på kostnadseffektivitet, global integration och dynamisk skalbarhet.

I en militär kontext år 2050 förväntas ”molnet” däremot anta en helt annan karaktär. Istället för beroende av centrala resurser kommer en distribuerad och hierarkiskt organiserad infrastruktur att dominera. Den kan inkludera stridsspecifika ”taktiska moln” nära operationsområdet, robusta nationella och allierade försvarsmoln med hög säkerhetsklassning samt selektiv integration med civila resurser. Dessa molntjänster möjliggör flexibel tillgång till beräkningskraft, AI-modeller och sensorfusion i realtid, även under påfrestande elektromagnetiska och kognitiva konfliktförhållanden.

Ur ett ledningssystemsperspektiv blir molntjänster en central möjliggörare för nätverksbaserat försvar. Ett ”slagfältsmoln” kan samla och distribuera underrättelser, lägesbilder och orderflöden i nära realtid, samtidigt som beslutsstödsystem och

32 Lockheed Martin (2018): F-35 Mission Systems (public brief) inkl. Link 16/MADL: https://sustainability.lockheedmartin.com/content/dam/lockheed-martin/eo/documents/webt/F-35_Mission_Systems_Design_Development_and_Verification.pdf.

33 Saab – Gripen E-series, networked sensor fusion: https://www.saab.com/products/gripen-e-series.

34 Avionics International (2018-09-04): F-35 data fusion, MADL/Link-16: https://www.aviationtoday.com/2018/09/04/f-35-data-fusion/.

35 DEVCOM ARL – IoBT CRA overview: https://arl.devcom.army.mil/cras/iobt-cra/.

36 Fog computing: mellanlager nära nätverkets kant, ofta gateways eller lokala noder.

autonoma plattformar får direkt tillgång till de datakällor de behöver. AI-baserat beslutsstöd integreras i molnstrukturen och kan ge chefer på olika nivåer prediktiva analyser, riskbedömningar och rekommendationer, vilket stärker förmågan till snabba och välgrundade beslut. Autonoma system – från drönarsvärmar till obemannade mark- och undervattensfarkoster – kan kopplas in i denna digitala infrastruktur och operera mer självständigt men ändå koordinerat genom molnet.

Samtidigt driver Nato en omfattande digitaliseringsagenda med fokus på gemensamma molnlösningar, datadelning och AI-baserat beslutsstöd för multinationella operationer.

## Samverkande och förutsättande teknikområden

### Materialinnovationer

Alternativa halvledarmaterial utvecklas utöver traditionell kisel-CMOS (eng. *Complementary Metal-Oxide-Semiconductor*). Halvledare av tredje generationen som galliumnitrid (GaN) och galliumarsenid (GaAs) erbjuder högre elektronrörlighet och högre frekvenser, vilket kan ge snabbare och mer energieffektiva komponenter. Egenskaper såsom god tålighet mot höga temperaturer och effekter har gjort att GaN redan har använts i högfrekvensradar och annan elektronik inom försvar. 2D-material som grafen och molybdendisulfid utreds för användning i transistorer med extremt liten storlek och hög hastighet; grafen har till exempel exceptionell ledningsförmåga och kan möjliggöra flexibel elektronik eller transparenta elektroniksystem.

### Kommunikationssystemutvecklingen

En särskilt avgörande teknikutveckling som förväntas påverka informationsteknologin fram till 2050 är nästa generations kommunikationssystem, särskilt 6G och framtida satellitkommunikation (satkom). Medan 5G redan möjliggjort snabba trådlösa nätverk med låg latens, förväntas 6G erbjuda betydande förbättringar, med kapacitet och latens som förbättras med flera storleksordningar.[37] När dessa system kombineras med avancerad satkom – inklusive lågflygande konstellationer som möjliggör global täckning – skapas en miljö där realtidskommunikation mellan mobila system, sensorer och beräkningsresurser blir norm.

Detta har flera direkta effekter på utvecklingen av informationsteknologi:

- *Edge computing* stärks, eftersom processorkraft och datalagring kan decentraliseras till exempelvis drönare, fordon och soldatsystem.

37 ITU Press (2023-12-01): IMT-2030 framework for 6G: https://www.itu.int/en/mediacentre/Pages/PR-2023-12-01-IMT-2030-for-6G-mobile-technologies.aspx.

- Realtidsintegration mellan sensorer och AI-system möjliggör snabbare beslutsfattande i både civil och militär kontext.
- Säker, kontinuerlig uppkoppling stödjer autonoma och fjärrstyrda system även i svårtillgängliga miljöer.
- Människa-maskin-integration, inklusive förstärkt verklighet och bärbar sensorteknik, kan utnyttja stabil hög bandbredd för att ge soldater och operatörer förbättrad situationsförståelse.

I en militär kontext förstärker denna utveckling nätverkscentrerade operationer, förbättrar redundans i samband med cyberhot, samt möjliggör mobilitetsanpassade beslutsstödsystem. Kommunikationsteknologier som 6G och satkom utgör därmed inte bara en möjliggörare, utan även en drivkraft för framtida informationsteknologi. Se också kapitlet om kommunikationsteknik.

## Påverkan på militär förmåga

Analysen av framtidens datorhårdvara och nya arkitekturer visar att vi står inför en period av omvälvande teknologiska språng som i grunden kan omdefiniera militär förmåga. Fotoniska datorer kan leverera hastigheter och bandbredder som knappt går att föreställa sig idag, neuromorfiska processorer kan ge oss AI på varje nivå från sensor till högkvarter med minimal energiförbrukning, 3D-integrerade chip kan pressa in superdatorprestanda i taktiska system, och nya material kan ge förutsättningar för datortillämpningar i nya miljöer och former. Tillsammans kan dessa tekniker möjliggöra en försvarsmakt som är mer uppkopplad, intelligentare och med snabbare reaktionsförmåga än vad som varit möjligt tidigare.

### Militära operationer

Utvecklingen inom datorhårdvara kan komma att revolutionera hur militära operationer bedrivs fram till 2050. Ökad datorkraft och specialiserad AI-hårdvara ute på fältet innebär att mer analys och beslutsstöd kan ske i realtid nära händelsernas centrum, istället för att data skickas till bakre stabsplatser. Exempelvis kan autonoma fordon och drönarsvärmar utrustade med neuromorfiska eller fotoniska processorer reagera snabbare än vad mänskliga operatörer förmår, vilket minskar *sensor-to-shooter*-tiden och potentiellt överlistar fienden. Kombinationen av stora datamängder, artificiell intelligens och autonoma enheter förväntas ge en strategisk och operativ fördel i beslutsfattande och snabbare OODA-loopar (*Observe-Orient-Decide-Act*). På taktisk nivå kan detta betyda att förband med överlägsen datorkraft kan manövrera snabbare och utnyttja situationer innan motståndaren hunnit reagera. På operativ nivå möjliggörs mer komplexa samordnade insatser (t.ex. simultana angrepp av svärmar över olika domäner) tack vare förbättrad informationsfusion och kommunikation i realtid.

### Beslutsfattande och ledning

På strategisk och operativ nivå kan ledningsstrukturen förändras av att beslutsfattare har tillgång till kraftfull AI och simuleringar. Genombrott inom datorhårdvara möjliggör extremt detaljerade simuleringar av stridsscenarier, logistikflöden eller informationskampanjer. Med exaflop- och senare zettaflop-nivåers beräkningskapacitet kan miljoner parametrar och aktörer modelleras i (nära) realtid, vilket ger militära beslutsfattare verktyg för att förutse utfall och optimera planer med en precision som idag är omöjlig. Detta kallas ibland för digitala tvillingar av slagfältet. Beslutsstödsystem baserade på AI kan komma att föreslå optimala handlingsalternativ, identifiera dolda hotmönster och till och med koordinera vissa operationer autonomt under chefs uppsikt. En samverkande effekt uppnås när stora data, avancerad AI och autonoma system kopplas samman.

### Cybersäkerhet

Den ökade komplexiteten i hårdvara kan också introducera fler sårbarheter. Nya specialchip och integrerade system har större angreppsyta om säkerhet inte designas in från början. Säkerhet i försörjningskedjan blir kritisk – om en fiende lyckas sabotera eller plantera bakdörrar i avancerade kretsar (som kanske bara tillverkas på ett fåtal platser globalt) kan det få förödande konsekvenser.

## Aktörer

### Regionala perspektiv: USA, Kina, EU, Ryssland, och Indien

Den globala kapprustningen och samarbetet inom elektronik och datorsystem påverkas i hög grad av olika geopolitiska aktörer. USA, Kina, Ryssland, Indien och Europa (EU) står i fokus – både som konkurrenter och partners på olika områden. Här analyseras deras respektive styrkor, strategier och utmaningar fram till 2050.

#### *USA: Teknologiskt ledarskap och strategiska begränsningar*

USA har under många decennier legat i framkant inom datorarkitektur, halvledardesign och militära högteknologiska system. Mycket av den grundläggande IT-utvecklingen – från mikroprocessorn till internet – har antingen initierats i USA eller blomstrat där tack vare unika ekosystem av universitet, företag och statlig FoU (ex. DARPA).

En viktig amerikansk sårbarhet är att tillverkningen av avancerade chip till stor del har flyttat utomlands under globaliseringens era. Även om designen ofta sker i USA (t.ex. Apple, NVIDIA, AMD, Qualcomm med flera), produceras kretsarna nästan uteslutande i Asien – framförallt hos TSMC i Taiwan. Detta skapar både ekonomiska och säkerhetsmässiga risker. För försvaret innebär offshore-produktion dessutom en potentiell risk att komponenter manipuleras eller att leveranser kan strypas i händelse av konflikt. Som svar på detta har USA under 2020-talet

lanserat ambitiösa satsningar för att stärka inhemsk halvledarkapacitet. *CHIPS and Science Act* (2022) anslog över $50 miljarder för att stimulera uppförandet av nya halvledarfabriker i USA och stödja forskning – det mest omfattande federala stödpaketet någonsin för denna industri. Under de första åren har betydande satsningar skett, men utvecklingen präglas 2025 av både framsteg och konflikter med interna motsättningar mellan fri marknadsmodell och behovet av industripolitisk styrning i en geopolitisk kapprustning. I juli 2025 invigdes det federalt finansierade *National Semiconductor Technology Center* (NSTC)[38] i Albany, New York. Centret är utrustat med en EUV-lithografimaskin från ASML och ska fungera som nav för nästa generations halvledarforskning. Investeringen signalerar USA:s ambition att ta teknologisk ledning i utvecklingen av de mest avancerade tillverkningsprocesserna.

För USA:s militära del innebär framtiden fram till 2050 att man strävar efter att behålla ett teknologiskt övertag gentemot rivaler genom innovation och allians-byggen. Mycket pekar på att USA fortsatt kommer att vara ledande inom design av nya typer av system (t.ex. kvantdatorteknik, AI-programvara, autonoma system) och försöka integrera dem snabbt i försvaret. Samtidigt lär man vara medveten om att försprånget kan krympa. Amerikanska försvarsrapporter med framtidsblick noterar att även om USA introducerar ny teknik, kommer stora rivaler snabbt kunna replikera dem, vilket endast ger ett tillfälligt övertag. Detta driver fram en doktrin att ständigt ligga steget före och omsätta tekniska framsteg i praktiken snabbare än vad motståndaren kan göra.

### *Kina: Civil-militär fusion och självförsörjning*

Kina har under de senaste 30 åren transformerats från en marginell aktör till en teknologisk stormakt. Inom elektronik och datorsystem har Kina idag världens största konsumentmarknad och många inhemska företag som är bland de världsledande (exempelvis Huawei inom telekom, Alibaba och Tencent inom moln/AI, SMIC inom halvledartillverkning på medelnivå). Men vad gäller den allra mest avancerade chiptillverkningen ligger Kina ännu efter toppskiktet. Bedömningar 2022 pekade på att Kinas inhemska halvledarindustri ligger minst ett decennium efter de internationella ledarna i fråga om spjutspetsteknik.[39] Denna eftersläpning beror delvis på Kinas sena inträde i fältet, men också på handelshinder – exempelvis begränsad tillgång till kritisk utrustning från omvärlden.

För att hantera detta har Kina antagit en explicit strategi kallad *Military-Civil Fusion* (MCF) eller *junmin ronghe*. MCF syftar till att sudda ut gränserna mellan den militära och den civila teknologisektorn, så att resurser och innovationer kan flyta fritt däremellan. Tanken är både att låta civila företag enklare bidra till militära projekt

38 NATCAST – Grand Opening of NSTC EUV Accelerator (operations began 2025-07-01): https://natcast.org/grand-opening-nstc-euv-accelerator.

39 Stiftung Neue Verantwortung & East West Futures, China Semiconductor Observatory – Baseline Report 2022, 2022. Tillgänglig på: https://www.interface-eu.org/publications/downloadPdf/china-semiconductor-observatory-baseline-report.

*(spin-on)* och att omvandla militära forskningsresultat till kommersiella produkter *(spin-off)*. I praktiken investerar den kinesiska staten i nyckelområden som halvledare, AI, rymd, 5G, kvantteknik – alla med dubbla användningsområden. Till exempel kan en fabrik som gör mobilchip också få militära beställningar som håller den igång tills den når konkurrenskraft. Militären fungerar som en pålitlig kund åt inhemska tech-företag, även om deras produkter initialt inte är bäst i världen, vilket hjälper företagen att överleva och förbättras. Denna politik ska alltså både stärka Kinas militär och den civila industrin samtidigt, och minska beroendet av utländsk teknik.

På kort sikt har Kina fortfarande utmaningar – dess främsta tillverkare SMIC (*Semiconductor Manufacturing International Corporation*) ligger ett par generationer bakom TSMC (*Taiwan Semiconductor Manufacturing Company*). Kinesiska designer av avancerade chip (t.ex. för GPU/AI) finns, men de bästa måste fortfarande tillverkas utomlands, vilket sanktioner har försvårat. Exportrestriktioner från USA och allierade bromsar Kinas framsteg vad gäller de allra mest högpresterande komponenterna (t.ex. är högbandbreddsminnen, avancerade FPGA:er och vissa programvaruverktyg belagda med restriktioner). Detta har dock sporrat Kina att satsa än mer på oberoende lösningar. Man försöker utveckla egen litografiutrustning, egna EDA-mjukvaror (*electronic design automation*), och substitut för amerikanska produkter (som RISC-V-baserade processorer för att slippa x86/ARM-beroende). Effekten på längre sikt återstår att se – Kinas ambition är tydlig: teknologisk självförsörjning och suveränitet (*techno-independence*), senast uttryckt i policy av president Xi Jinping. Till 2050 kan vi mycket väl få se att Kina byggt upp en i stort sett komplett inhemsk leveranskedja för halvledare, från råmaterial till chip, vilket skulle minska effekten av västerländska exportkontroller.

Militärt innebär Kinas strategi att man snabbt integrerar ny civil teknik i Folkets befrielsearmé (PLA). AI används redan flitigt för övervakning och propaganda internt, och PLA utforskar autonoma vapensystem och "informatiserad" krigföring där data och nätverk är centrala. Kina har visat framsteg inom vissa militärteknologier parallellt med USA – exempelvis hypersoniska vapen och rymdteknik – där de ibland överraskat omvärlden. Elektronikens prestanda i dessa system beror dock också på chip. Utan tillgång till senaste generationens mikroelektronik kan Kinas vapensystem potentiellt ha prestandanackdelar, särskilt i sensorer och datalänkar. Dock ska det noteras att högteknologisk krigföring inte enbart handlar om att ha den minsta transistorn – systemintegration, doktrin och personal är också avgörande.

Ett intressant fenomen är att civil elektronik i Kina i vissa fall är mer avancerad än den militära. T.ex. är kinesiska konsumentdrönare (DJI) världsledande och exporteras globalt, och dessa har ironiskt nog använts av andra länders militärer. Det belyser att Kina redan är en ledare gällande mycket civil teknik. Frågan blir i vilken mån staten kan kanalisera detta till militära fördelar. MCF syftar just till detta, givet Kinas resurser och befolkning (tusentals ingenjörer examineras varje år inom

relevant teknik) är en rimlig förväntan att Kina 2050 inte längre ligger efter inom kritisk elektronik, utan kanske konkurrerar på jämbördig nivå med USA. Kanske finns då två separata teknologiekosystem: ett kinesiskt och ett västligt.

*EU: Samarbete och teknologisk suveränitet*

EU intar en något annorlunda position. EU består av flera länder med stark industriell bas (Tyskland, Frankrike, m.fl.) men har inte haft en samlad halvledarpolitik förrän nyligen. Europeisk elektronikindustri har traditionellt excellerat inom vissa nischer: telekomutrustning (Ericsson, Nokia), fordonselektronik (Infineon, NXP, STMicroelectronics för bilindustrin), industriautomation och inte minst produktionsutrustning (holländska ASML är ensam leverantör i världen av EUV-litografisystem, en kronjuvel inom halvledarsektorn). Däremot har EU saknat egen storskalig tillverkning av de mest avancerade logikkretsarna. Endast ~9% av världens halvledare tillverkas inom EU (2021), och den andelen riskerade minska ytterligare enligt branschexperter.

Detta såg EU som ett strategiskt problem, både industriellt och säkerhetsmässigt. 2022 presenterade därför EU-kommissionen *European Chips Act*[40], en storsatsning värd €43 miljarder i offentliga medel för att stärka Europas halvledarindustri. Pengarna ska gå till att etablera nya fabriker (både helt nya *first-of-a-kind*-anläggningar och expansion av befintliga, gärna med de allra modernaste processerna), samt investera i forskning och kompetensförsörjning. Man betonar behovet att omsätta Europas starka grundforskning inom exempelvis elektronik och material till kommersiella produkter – att gå från labb till fabrik är ett uttalat fokus.

På det militära området har EU-länderna traditionellt förlitat sig mycket på transatlantisk teknologi eller egna inhemska leverantörer inom respektive land främst för nationellt bruk. Exempelvis använder europeiska stridsflyg och satelliter ofta elektronik från USA eller internationella samarbeten. Frankrike och andra länder har dock egna spetsprojekt (Frankrike t.ex. inom radarelektronik och kärnvapenteknik). EU har på senare år lanserat en europeisk försvarsfond (*European Defence Fund*, EDF) för att finansiera gemensam utveckling, inklusive av högteknologiska komponenter, i syfte att öka självständigheten. Drivkraften är dels ekonomisk (stordriftsfördelar om länder utvecklar gemensamt istället för parallellt), dels säkerhetspolitisk – Europa vill inte vara helt beroende av USA för kritisk försvarsteknik. Samtidigt kvarstår Nato och bandet till USA som hörnstenar i europeisk säkerhet, så EU navigerar en mellanväg där man stärker teknologisk suveränitet utan att bryta samarbetet med USA. Ett exempel är att även EU infört restriktioner mot Kina i linje med USA:s (Nederländerna stoppade officiellt export av viss litografiutrustning till Kina från 2019).

40 https://www.csis.org/blogs/perspectives-innovation/european-chips-act-strategy-expand-semiconductor-production.

Till 2050 kan EU ha uppnått en starkare position om Chips Act och efterföljare till denna faller väl ut. I bästa fall har Europa då moderna halvledarfabriker som kan producera t.ex. 1 nm-chip eller vad standarden är då, kanske i samverkan med internationella företag men belägna på europeisk mark. Det skulle garantera tillgången för både civilt bruk (industri, fordonssektor, konsumenter) och för det europeiska försvaret. Europa har också unika tillgångar som kan behålla betydelse. ASML lär fortfarande vara dominerande i nästa generations litografi (om det är EUV eller kanske nya metoder), IMEC (belgiskt forskningscenter) är världsledande inom nanoelektronikforskning och involverar globala partners, och europeiska företag är starka inom inbyggda system och lågeffekt-chip (vitalt i t.ex. fordon och IoT). EU:s utmaning blir att orka investera tillräckligt och behålla talang inom regionen så att man inte halkar efter. Oavsett vad som händer kan vi förvänta oss att internationellt samarbete förblir viktigt för EU – man kommer troligen balansera relationerna åt båda håll, genom att samarbeta med USA (och Storbritannien) om standarder och försvar, samtidigt som man försöker behålla ekonomiska band med Kina men med vaksamhet för *dual-use*-risker.

I fråga om militär elektronikexklusivitet har EU generellt haft mindre fokus på egna lösningar än USA och Kina, och ofta förlitat sig på öppna marknaden eller samarbete. Detta kan förändras något med den nya betoningen på försvarsindustriellt samarbete inom EU, men det är osannolikt att Europa driver en strikt separat linje – snarare vill man försäkra sig om att kunna få tag på kritisk teknik när det behövs, genom antingen inhemsk kapacitet eller allierade.

*Ryssland: Importsubstitution under sanktionstryck och asymmetrisk anpassning*

Sedan 2022 har Rysslands utveckling inom informationsteknologi formats av omfattande exportkontroller, vilka initialt slog hårt mot tillgången på avancerade halvledare och produktionsutrustning. Leveranser av högpresterande kretsar föll kraftigt redan 2022–2023 och restriktionerna har därefter breddats för att även angripa tredjelandstransiter, särskilt via Kina och Hongkong. Trots detta har importflöden via omvägar delvis upprätthållits, vilket flera analyser pekar på som en delförklaring till Rysslands tekniska resiliens – men med högre kostnader, längre ledtider och osäker kvalitet.

Inhemsk halvledarkapacitet är i huvudsak begränsad till mogna tillverkningsprocesser (cirka 90–180 nm, med begränsade 65 nm-inslag). Tillverkningsklustret i Zelenograd (Mikron m.fl.) har försökt expandera volymen och byta till alternativ utrustning, men process-gapet mot ledande *foundries*[41] kvarstår, och projekt för 28/14 nm har skjutits på framtiden. Parallellt stoppades eller fördröjdes leveranser av ryskt designade CPU:er (Elbrus, Baikal) när utländska *foundries* avbröt samarbeten efter sanktionsbeslut. Effekten är att avancerade system ofta måste förlita sig

41 Foundries är specialiserade halvledarfabriker som tillverkar kretsar på uppdrag av andra företag. De står för själva produktionen men utvecklar vanligtvis inte egna slutprodukter, utan producerar chip baserat på kundernas konstruktioner.

på insmugglade/importerade kretsar och att inhemska designhus saknar konkurrenskraftig produktion.

På mjukvarusidan har staten accelererat importsubstitution (t.ex. inhemska OS-distributioner) och satsat på AI-ekosystem runt de stora bank- och teknikkonglomeraten. Satsningarna hämmas dock av begränsad tillgång till GPU:er och en modern EDA-verktygskedja för design och konstruktion av elektroniska system, vilket pressar aktörer att antingen bygga på äldre hårdvara eller förlita sig på grå import och molnlösningar utomlands.

Ryssland förväntas fortsätta en asymmetrisk anpassning: (1) maximal exploatering av civila/mogna tillverkningsprocesser för vapen- och sensorelektronik, (2) kringgående av sanktioner för utvalda högpresterande komponenter, och (3) ökad integration av mjukvara/algoritmer för att kompensera för brist på hårdvara. Om väst upprätthåller ett bestående försprång i <5 nm-klassen och i avancerade minnen/packaging, kommer ryska system sannolikt ha lägre energieffektivitet och prestanda per watt i sensortunga, nätverks- och telekrigintensiva tillämpningar. Samtidigt talar erfarenheten sedan 2022 för att teknologiska luckor kan överbryggas med volym, förenklad design, och snabb fältanpassning – vilket gör att teknisk överlägsenhet inte automatiskt översätts i operativ dominans.

Ryssland har viss forskningskompetens inom kvantfysik, fotonik och neurovetenskap, men saknar bred industriell bas. Till 2050 är det möjligt att man uppnår nischade kvantdatorer (för kryptoanalys, materialvetenskap och radaroptimering) men inte system i samma skala som USA eller Kina. Inom optiska processorer kan tillämpningarna begränsas till specialsystem för försvar (höghastighetskommunikation, signalbehandling). Vad gäller neuromorfiska processorer kan Ryssland däremot relativt snabbt bygga användbara militära system, genom att kombinera enklare chip med avancerade algoritmer för drönare, autonoma fordon och telekrigföring. Sammantaget blir Rysslands roll 2050 mer präglad av asymmetriska tillämpningar än av globalt teknologiskt ledarskap.

*Indien: Från IT-tjänster till kisel – byggandet av en inhemsk halvledarkedja*

Indien går in i 2030-talet med en bred satsning på digitalisering av samhället som indirekt ger en stor marknad för inhemsk hårdvara, säkerhet och nätverk. Sedan 2023 har regeringen en expansiv halvledarstrategi. Micron etablerar en större test- och förpackningsanläggning i Gujarat i två faser, samtidigt som staten godkänt flera nya fabriker (bl.a. Tata Electronics med taiwanesiska PSMC som teknikpartner; CG Power med Renesas/Stars). Dessa investeringar syftar till att bygga en inhemsk värdekedja för fordon, telekom, försvar och IoT. Tillverkningsmålen är initialt inriktade på mogna tillverkningsprocesser och högvolymproduktion.

Med en stor civil marknad, djup mjukvarubas och växande komponentproduktion har Indien potentiell handlingsfrihet att koppla samman digital offentlig infrastruktur, 6G/satkom, och sensortäta plattformar till *dual-use*-system för gräns-,

rymd- och marinövervakning. Om de pågående fabs-projekten realiseras, och monterings- och testkapaciteten skalas upp, kan Indien vid 2040–2050 vara självförsörjande på en stor del av försvarsrelevant elektronik (radar-/RF-komponenter, kraft- och bil-/aero-MCU:er, minnen och förpackning) samtidigt som man integrerar internationell spjutspetsteknik där det är kostnadseffektivt. Detta skulle ge strategisk autonomi utan att nödvändigtvis kräva ledarskap i tillverkningsprocesser för halvledare.

Indien har redan initierat en nationell kvantstrategi med målet att nå stabila system på hundratals qubits till 2030-talet. Till 2050 är det möjligt att landet har egna kvantdatorer i mellanklassen, med tillämpningar inom bland annat kryptering och materialvetenskap. Inom optiska processorer kan Indien dra nytta av stark telekomindustri och växande halvledarkedja för att utveckla optiska kretsar för datacenter, moln och satellitkommunikation. På området neuromorfiska processorer kan Indien bli särskilt framgångsrikt. Genom stor AI-kompetens, tillgång till låg-kostnadsproduktion och en expansiv civil marknad kan landet 2050 vara globalt relevant inom neuromorfa chips, särskilt för autonoma system, sensornätverk och militära plattformar. Sammantaget kan Indien fram till 2050 gå från att vara beroende av import till att bli en regionalt självständig och globalt relevant aktör på flera fronter.

### Exklusivitet kontra spridning inom informationsteknologi

Utvecklingen inom informationsteknologi bedöms fortsatt drivas av den civila sektorn och präglas av snabb global spridning. Möjligheterna till militärteknisk exklusivitet minskar därmed. Ett framtida informationsövertag väntas i stället bero på förmågan att snabbt anpassa, integrera och skydda civil teknik i militära system. Den ökade användningen av globala plattformar och leverantörskedjor bedöms samtidigt öka sårbarheten. Fram till 2050 kan exklusivitet inom informationsteknologi i första hand komma att avgöras av systemarkitektur, datasuveränitet och cybersäkerhet, snarare än av tillgång till unik hårdvara.

## Lästips

NATO Science & Technology Organization, Science & Technology Trends 2023-2043 cesmar.it.

Photonics21, Europe's Age of Light - Photonics Roadmap 2021-2027 photonics21.org.

Shivakumar, S., & Wessner, C. (2021). Semiconductors and national defense: What are the stakes? Center for Strategic and International Studies.

Teer, J., Bertolini, … (2022). Winning interdependence: semiconductor and CRM rivalry in a de-globalising world. In Reaching breaking point: The semiconductor and critical raw material ecosystem at a time of great power rivalry (pp. 60–77). Hague Centre for Strategic Studies. http://www.jstor.org/stable/resrep44057.8.

Trueman, C. (2024, 7 oktober). TSMC could account for 24% of Taiwan's electricity consumption by 2030. DataCenter Dynamics.

Tillväxtverket (2024). Halvledaraktens tillämpning i Sverige. Stockholm: Tillväxtverket. Tillgänglig: https://tillvaxtverket.se/download/18.55c7246818d2a8dfbde26694/1706257087076/Halvledaraktens%20till%C3%A4mpning%20i%20Sverige.pdf.

FMV (2022). Teknisk prognos: Tema halvledare (Nr 2/2022). Stockholm: Försvarets materielverk. Tillgänglig: https://www.fmv.se/globalassets/dokument/om-fmv/teknisk-prognos-nr2-2022-halvledarteknik.pdf.

Försvarsmakten. (2023). Digital transformation och uppbyggnad av "digital ryggrad". I HT 2-2023 inlaga. Kungl. Krigsvetenskapsakademien. Tillgänglig: https://kkrva.se/hot/2023:2/sigholm-datadrivna-forsvarsformagor.pdf.

# Kommunikationsteknik

*Erik Axell*

## Inledande beskrivning

Kommunikationsteknik för militärt samband omfattar teknik för överföring av information mellan enheter, exempelvis mellan eller inom militära förband. Väl fungerande samband är avgörande för ledningsförmågan. Informationen som överförs kan bestå av exempelvis tal, video, eller filer med data. All informationsöverföring i moderna kommunikationssystem sker dock i praktiken genom överföring av digitala data.

En förutsättning för militär ledningsförmåga är att information kan skickas mellan enheter i alla domäner och mellan samverkande nationer, exempelvis från sensorer och andra källor till ledningsplatser eller från ledningsplatser till stridande enheter oberoende av vilken stridskraft dessa tillhör. Den förväntade, och därmed dimensionerande, normalbilden är att kommunikationssystem utsätts för telekrigföring, dvs. fientlig påverkan på kommunikationen genom exempelvis radiostörning. Allt detta ställer i sin tur krav på förmågan hos kommunikationssystem i form av exempelvis datatakt, fördröjning, mobilitet, interoperabilitet och tillgänglighet i form av t.ex. störtålighet.

Ökande krav på snabbare beslut baserat på större informationsmängd ställer större krav på dataöverföring. Snabbare stridsfält, distribuerade och mobila ledningsplatser och agil ledningsförmåga mellan domäner ställer större krav på mobilitet, flexibilitet och anpassningsförmåga hos kommunikationssystemen.

Att uppfylla militära särkrav såsom störskydd och låg signatur tvingar ofta fram kompromisser med andra typer av kommunikationsprestanda, såsom datatakt och räckvidd. En försvårande omständighet är att det tillgängliga frekvensutrymmet för militär användning är begränsat. Det är därför viktigt att utveckla anpassningsförmåga för att nyttja resurser så bra som möjligt i varje situation oavsett vad som just då är viktigast – att överföra så mycket information som möjligt så fort som möjligt, att kommunikationen fungerar överhuvudtaget trots fientlig påverkan eller att motståndare har svårt att upptäcka kommunikationen.

På grund av fysikaliska lagar kommer det alltid finnas kompromisser mellan prestanda i egna kommunikationssystem å ena sidan och motståndares möjlighet att upptäcka eller påverka kommunikationsförmågan å andra sidan. Exempelvis ger ökad räckvidd i egna radiosystem även ökad möjlighet för motståndare att upptäcka, identifiera och lokalisera radiosändare. Ökad tålighet mot radiostörning kan skapas genom att kompromissa med minskad datatakt. Detta gäller nu och i framtiden. Kraven på kommunikationsprestanda och motståndskraft (t.ex. störtålighet och låg upptäcktsförmåga) varierar i olika scenarier och kan förändras över tid.

Om krav på snabb och pålitlig kommunikation eller krav på att inte bli upptäckt får högst prioritet på framtida transparenta stridsfält är svårt att sia om. Sannolikt ligger sanningen någonstans däremellan och det blir viktigt att system kan anpassas för att hantera detta.

## Trender och exempel

Det finns flera intressanta kommunikationstekniker som har utvecklats och studerats under de senaste 10–20 åren inom den akademiska forskningen och som fortsätter att utvecklas, i vissa fall som komponenter av nya kommunikationsstandarder. Dessa kommunikationstekniker är av intresse inte bara för civil användning, utan även för militära tillämpningar. Nedan beskrivna teknikområden bedöms intressanta för framtida militär kommunikation. Inom dessa områden bedrivs omfattande forskning och utveckling och inom flera av dem har det skett signifikanta framsteg de senaste åren.

Flerantennteknik för spatiell multiplexing och lobformning med många (digitalt styrbara) antennelement har studerats under ett par decennier och ingår idag i flera kommersiella kommunikationssystem. Inom detta område kan nämnas begrepp såsom MIMO (*multiple input, multiple output*, dvs. kommunikationsströmmar via flera antennelement hos både sändare och mottagare), *massive* MIMO[42] (även *gigantic*[43] och *holographic*[44] MIMO), *mmWave*, och RIS[45] (*reconfigurable intelligent surface*) eller IRS (*intelligent reflecting surface*). Storleken på antennelement och avståndet mellan dem är beroende av i vilket frekvensområde de fungerar; ju högre frekvens, desto mindre antennelement och mindre avstånd mellan dem. För att nyttja flerantennteknik krävs flera antennelement, vilket gör tekniken tillämplig för höga frekvenser. Radiosignaler vid högre frekvenser dämpas dock kraftigare, speciellt vid påverkan av terräng, och har därför kortare räckvidd än signaler vid lägre frekvenser. Det är troligt att användningen av flerantennteknik på högre frekvenser än de som traditionellt används för militär radiokommunikation kommer att bli mer intressant i framtiden, till exempel för kommunikation mellan flygande obemannade plattformar och med sensorer på korta avstånd.

42 E. G. Larsson, O. Edfors, F. Tufvesson and T. L. Marzetta, "Massive MIMO for next generation wireless systems," in IEEE Communications Magazine, vol. 52, no. 2, pp. 186-195, February 2014.

43 E. Björnson, F. Kara, N. Kolomvakis, A. Kosasih, P. Ramezani and M. B. Salman, "Enabling 6G Performance in the Upper Mid-Band by Transitioning From Massive to Gigantic MIMO," in IEEE Open Journal of the Communications Society, vol. 6, pp. 5450-5463, 2025.

44 C. Huang et al., "Holographic MIMO Surfaces for 6G Wireless Networks: Opportunities, Challenges, and Trends," in IEEE Wireless Communications, vol. 27, no. 5, pp. 118-125, 2020.

45 E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M. -S. Alouini and R. Zhang, "Wireless Communications Through Reconfigurable Intelligent Surfaces," in IEEE Access, vol. 7, pp. 116753-116773, 2019.

Flexibel spektrumanvändning med (främst digital) signalbehandling av större bandbredd än tidigare (exempelvis s.k. stirrande mottagare) är ett område som har utvecklats under de senaste ca 20 åren. Inom många civila kommunikationsstandarder finns stor grad av flexibilitet i nyttjandet av frekvensspektrum.[46] Av flera skäl, bland annat robusthet, säkerhet och mobilitet utan tillgång till fast infrastruktur, är spektrumanvändningen i militära system inte agil i samma utsträckning. För att nyttja frekvensspektrumet mer effektivt och för att hantera interferens och fientlig störning krävs ökad flexibilitet i spektrumanvändningen.

AI-stödd och kognitiv kommunikation, som adaptivt kan optimera t.ex. bandbredd, frekvensband och val av bästa kommunikationsväg[47] är en tydlig trend under de senaste tio åren. Inom mobilutvecklingen (6G) nämns exempelvis att den nya standarden ska vara *AI native*[48], dvs. att den redan från början ska ha stöd för införandet av AI-baserade funktioner i mobilnäten.

Rymdbaserad kommunikation är på stark frammarsch både civilt och militärt. Det omfattar exempelvis system baserade på många små satelliter i låg (LEO) bana såsom Starlink och Oneweb, satellitsystem som utgör rymdsegment i 5G och framtida mobilnät[49], men även andra satellitsystem baserade på större satelliter i högre omloppsbana.

Användning av mobilnät (5G/6G/*future G*/*next G*) och andra civila system (i kombination med militära system) är en annan tydlig trend, inte minst på grund av sådan användning i kriget i Ukraina. Det sker kontinuerlig utveckling av teknik och standard för mobilnät. I maj 2025 tog Försvarsmakten beslut att använda mobilnät för militär kommunikation.[50] Mobilnäten är inte utvecklade specifikt för att hantera militära särkrav på exempelvis tålighet mot störning. Däremot har systemen tekniker för att hantera t.ex. interferens och systemen använder sig av mobiloperatörens alla tillgängliga frekvensband, vilket också skapar tålighet mot störning.

Användning av Multi-RAN (*radio access networks*) på militära plattformar, antingen med flera samverkande (civila och militära) radiosystem eller med flera radiosystem integrerade i samma mjukvaruradio kommer sannolikt att krävas i framtiden. Dock kräver fysikaliska egenskaper fortfarande viss specifik hårdvara, exempelvis antenner som är anpassade till respektive frekvensband och bandbredd.

---

46 P. Eliardsson, E. Axell, K. Hägglund, G. Bark, ”Flexibel frekvensanvändning för Försvarsmaktens radiosystem – Omvärldsbevakning”, FOI-R--5601--SE, 2024.

47 E. Axell, P. Eliardsson, K. Hägglund, P. Brännström, C. Svensson, “Overview of Machine Learning in Communication Systems”, FOI-R--5275--SE, 2022.

48 J. Hoydis, F. A. Aoudia, A. Valcarce and H. Viswanathan, “Toward a 6G AI-Native Air Interface,” in IEEE Communications Magazine, vol. 59, no. 5, pp. 76-81, May 2021.

49 M. M. Azari et al., “Evolution of Non-Terrestrial Networks From 5G to 6G: A Survey,” in IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2633-2672, 2022.

50 Inriktning gällande Försvarsmaktens nyttjande av mobilnät samt nästa generationers trådlösa nät, FM2025-11451:1.

God samverkan mellan trådlös kommunikation, telekrigföring (spaning, störning) och radar är nödvändig för att uppnå elektromagnetisk överlägsenhet över motståndare. Multifunktionssystem, som medger samverkan mellan dessa förmågor i samma system, kan vara ett sätt att realisera detta. Civil forskning fokuserar framförallt på att kombinera kommunikation och radar, vilket ofta beskrivs med begreppen *joint sensing and communication* (JSAC) eller *integrated sensing and communication* (ISAC).[51]

Kvantteknik för kommunikationstillämpningar, t.ex. beräkningar, datorer och kryptonyckelöverföring (*quantum key distribution*) och tekniker för post-quantum (dvs. teknik som inte kan knäckas av kvantdatorer), kan bli viktigt i framtiden.

Fri optisk kommunikation, dvs. laserbaserad kommunikation, kan ha fördelar i vissa tillämpningar. Sådan kommunikation kräver fri sikt mellan kommunicerande enheter, men har otroligt stor bandbredd och är svår att störa, upptäcka eller avlyssna jämfört med radiokommunikation. Optisk kommunikation kan komma att nyttjas mellan exempelvis flygande plattformar (t.ex. UAV, satellit, stridsflyg).

## Särskilda delområden

Störskydd förväntas fortsatt vara en central förmåga i militära kommunikationsnät. Ökad adaptivitet och intelligens i systemen, med avseende på exempelvis radioresursallokering och länkadaption (t.ex. antenn, tid- och frekvensallokering, effektreglering, modulation och felrättande kodning) kan till viss del hantera detta, men även traditionella bandspridningstekniker (t.ex. frekvenshopp) förväntas fortsatt krävas i vissa radiosystem för att öka störtåligheten. Vid nyttjande av högre frekvenser finns större möjligheter att nyttja flerantennteknik (lobformning och spatiell multiplexning) med möjlighet att styra sändning och mottagning i olika riktningar för att t.ex. undertrycka störning eller undvika upptäckt.

Låg signatur (smyg-/stealth-kommunikation) förväntas också vara en central förmåga i vissa framtida militära scenarier. Utveckling av teknologi som ger bra smygegenskaper (*low probability of intercept/detect*, LPI/LPD) och gör det svårt för motståndare att upptäcka, positionsbestämma eller avlyssna signaler är därför av vikt.

Mobila ad hoc-nät, mesh-nätverk och decentraliserade system som är oberoende av fast infrastruktur förväntas fortsatt vara en del av militärt samband för att garantera yttäckning, tillgänglighet och oberoende av annan infrastruktur. I framtiden förväntas radionäten i större utsträckning vara självkonfigurerande och självläkande.

För militär användning förväntas undervattenskommunikation, både med radiosignaler på låga frekvenser och akustiskt, vara nödvändig.

51 N. González-Prelcic et al., "The Integrated Sensing and Communication Revolution for 6G: Vision, Techniques, and Applications," in Proceedings of the IEEE, vol. 112, no. 7, pp. 676-723, July 2024.

Trådbunden kommunikation, via optisk fiber, t.ex. som kärnnät för mobilnät och som anslutning mellan fasta punkter, kommer fortsatt att vara nödvändig även för militär telekommunikation.

### Samverkande och förutsättande teknikområden

Behov av dataöverföring drivs av flera faktorer, bl.a. digitalisering av ledningsstödsystem, utveckling och användning av sensorsystem, graden av autonomi och samverkan mellan framtida tekniska system, datadrivet beslutsstöd och ledningsplatsers utformning genom t.ex. spridning, mobilitet och virtualisering.

Utveckling av elektronik och beräkningskraft möjliggör mer avancerad signalbehandling, t.ex. mottagning med väsentligt större bandbredd med tillräcklig dynamik och beräkningskraft för att utföra digital signalbehandling.

Informationsskydd kan sätta begränsningar genom t.ex. krav på fysisk separation av hårdvara och begränsad delning av information. Detta kan ge ökad säkerhet på bekostnad av mindre effektiv telekommunikation.

### Påverkan på militär förmåga

Kommunikationsteknik spelar en avgörande roll inom det militära området och fungerar som ryggrad för ledning, kommunikation, datorer, underrättelseverksamhet, övervakning och spaning (eng. *command, control, communications, computers, intelligence, surveillance, and reconnaissance*, C4ISR).

Militär telekommunikation säkerställer att information flödar säkert, snabbt och tillförlitligt mellan alla nivåer av ledning och vid alla konfliktnivåer. Dess effektivitet påverkar direkt utfallet av operationer och personalens säkerhet.

Kommunikationsprestanda kan bli gränssättande för framtida informationssystem. Det är av stor vikt att applikationer och nyttjande av data som kräver telekommunikation är anpassade att hantera variationer av prestanda i form av t.ex. datatakt och fördröjning. Informationssystem bör inte konstrueras så att de är beroende av kontinuerligt tillgänglig kommunikation med hög kapacitet för att fungera. Samtidigt bör de konstrueras för att kunna nyttja hög kapacitet när den är tillgänglig.

### Aktörer

Utvecklingen av kommunikationsteknik sker till stor del genom civil industri (t.ex. mobilindustrin) och i akademiska forskningsmiljöer. Den civila utvecklingen sker ofta i sammanslutningar av flera aktörer genom standardiseringsorgan (inom t.ex. 3GPP) som drivs av kommersiella intressen. Det finns även samverkansprojekt inom t.ex. Nato och EDF för studier av militär användning av mobilnät (5G och framtida generationer).

Försvarsindustrin utvecklar radiosystem för militär användning och tillkommande särskilda krav avseende exempelvis störtålighet, räckvidd och oberoende av fast infrastruktur. Även för utveckling av militärspecifik kommunikationsteknik finns viss samverkan för standardisering, exempelvis inom Nato. Dock finns inte samma gemensamma drivkraft som inom den civila utvecklingen, av flera skäl, exempelvis militära krav på säkerhet och robusthet samt nationella särkrav.

## Lästips

E. Björnson, L. Sanguinetti, H. Wymeersch, J. Hoydis, and T. L. Marzetta, Massive MIMO is a reality. What is next? Five promising research directions for antenna arrays, Digital Signal Process., vol. 94, pp. 3–20, Jan. 2019.

T. Gong et al., Holographic MIMO Communications: Theoretical Foundations, Enabling Technologies, and Future Directions, in IEEE Communications Surveys & Tutorials, vol. 26, no. 1, pp. 196-257, 2024.

E. Björnson, H. Wymeersch, B. Matthiesen, P. Popovski, L. Sanguinetti and E. de Carvalho, Reconfigurable Intelligent Surfaces: A signal processing perspective with wireless applications, in IEEE Signal Processing Magazine, vol. 39, no. 2, pp. 135-158, March 2022.

Y. Liu et al., Reconfigurable Intelligent Surfaces: Principles and Opportunities, in IEEE Communications Surveys & Tutorials, vol. 23, no. 3, pp. 1546-1577, 2021.

O. Simeone, A Very Brief Introduction to Machine Learning With Applications to Communication Systems, IEEE Trans. on Cogn. Commun. Netw., vol. 4, no. 4, pp. 648–664, Dec. 2018.

T. O'Shea and J. Hoydis, An Introduction to Deep Learning for the Physical Layer, IEEE Trans. on Cogn. Commun. Netw., vol. 3, no. 4, pp. 563–575, Dec. 2017.

K. B. Letaief, W. Chen, Y. Shi, J. Zhang and Y. -J. A. Zhang, The Roadmap to 6G: AI Empowered Wireless Networks, in IEEE Communications Magazine, vol. 57, no. 8, pp. 84-90, August 2019.

N. González-Prelcic et al., The Integrated Sensing and Communication Revolution for 6G: Vision, Techniques, and Applications, in Proceedings of the IEEE, vol. 112, no. 7, pp. 676-723, July 2024.

# Intelligenta system

*Joel Brynielsson*

## Inledande beskrivning

Intelligenta system är datorsystem som designats så att de har ett intelligent beteende avseende att kunna registrera, analysera, förstå och reagera på omgivningen. Begreppet används ofta synonymt med AI eller AI-system. Under de senaste åren har området präglats av genombrott inom maskininlärning, det vill säga att låta datorer lära sig själva med hjälp av data. Exempel på framgångsrika tillämpningar är självkörande bilar, röstigenkänning och språköversättning. På samma sätt som i civila tillämpningar erbjuder AI inom försvarsområdet en förmågehöjande komponent, som påverkar alla vapengrenar. AI ger övertag till den sida som snabbare och bättre än sin motståndare kan inhämta och använda sig av tillgänglig information. Olika användningsområden innefattar underrättelsetjänst, logistikplanering, sårbarhetsanalys, hotanalys, resursplanering, händelseigenkänning, ledning samt spel och simuleringar för träning och övning. Specifika forskningsutmaningar kopplade till försvars- och säkerhetsområdet som behöver beaktas de närmaste åren handlar om sårbarheter och transparens hos AI-system samt tillgång till data.

## Trender och exempel

Utvecklingen inom it-området har under de senaste decennierna varit snabb, och i stor utsträckning styrts av enskilda tekniska genombrott, både på hård- och mjukvarusidan. En stor mängd av de elektronikprodukter, exempelvis fordon, telefoner och kameror, som kommer ut på marknaden i dag innehåller någon typ av it-system. Datorer har gjort sitt intåg i kylskåp, kaffeautomater, dörrlås, klimatanläggningar och i många andra produkter som kan tänkas behöva beräkningskraft och lagringsförmåga. Datorers förmåga att spara, hantera och analysera data ligger till grund för en stor del av vår teknologiska utveckling de senaste femtio åren, och det finns anledning att tro att it kommer att spela en än större roll i framtiden, eftersom att it i dag påverkar hela samhället.

En tydlig trend är att mängden tillgänglig information ökar (se det följande kapitlet om data), och att olika tekniska system i allt större utsträckning kopplas ihop – direkt eller indirekt. Sammankoppling av olika system ger stora möjligheter för både privatpersoner och organisationer att optimera och planera. Samtidigt ökar det samhällets sårbarhet mot haverier, systemfel och it-attacker. En annan trend inom it-området är att överlåta alltmer databehandling och analys till datorer, på samma sätt som att man i den fysiska världen har överlåtit stora delar av arbetet till maskiner och robotar. Några av de främsta anledningarna är att datorer är snabba, och har perfekt minne och beräkningskraft som ökar explosionsartat för varje år.

Dessa förmågor kommer att fortsätta att öka framöver. Den förmåga som fram till i dag i mångt och mycket har saknats hos datorer är att kunna fusionera olika typer av information, och att analysera betydelsen av denna på en hög abstraktionsnivå. På senare tid har dock stora framsteg gjorts avseende just analysförmågan hos datorer. I dag kan datorer användas för att transkribera tal till text och för att göra översättningar mellan olika språk i realtid, men också för att skapa rapporter, analysera och sammanfatta texter med mera.

I dag finns redan många exempel på avancerade AI-system som presterar bättre än människor inom vissa områden. Generellt är den här typen av system ännu inte tillräckligt pålitliga för att kunna ersätta mänskliga experter, utan används främst som stöd och komplement. Man kan emellertid förvänta sig att de förmågor som nämnts ovan successivt kommer att förbättras till en nivå där datorprogram helt kan ta över vissa förhållandevis avancerade analysuppgifter som i dag måste utföras manuellt.

En aktuell AI-trend handlar om agentisk AI, en typ av artificiell intelligens som inte bara reagerar på instruktioner, utan agerar självständigt och autonomt för att bidra till att uppnå ett högre mål. Sådana AI-agenter kan liknas vid ”lagkamrater” som arbetar outtröttligt, lär sig kontinuerligt, anpassar sig perfekt till en användares behov, och har förmågan att på egen hand observera, planera och agera. Agenterna används exempelvis för att ta fram nya applikationer från ax till limpa. Givet en enkel instruktionsprompt kan en agentisk AI göra hela arbetet med att skapa en webbplats eller app inklusive alltifrån att analysera målet och målgruppen, ta fram förslag på struktur, design och innehåll, anpassa texter till målgruppen och så vidare. Agenten samordnar även olika steg som kodning, testning och publicering, genom att använda vanliga datorverktyg och samverkan med andra AI-agenter och med människor, och övervakar slutligen projektets framsteg, identifierar problem och gör justeringar till dess webbplatsen är färdig och lanserad. På lång sikt har agentisk AI potential att nydana och förändra hur människor arbetar, innoverar och styr teknik, genom att AI bistår med att självständigt fatta beslut, samarbeta och utföra komplexa uppgifter. Militärt har denna utveckling förutsättningar att i grunden påverka till exempel hur man planerar komplexa operationer, där agenterna självständigt skulle kunna kombinera underrättelsearbete, planering och logistik med att samverka med mänskliga militära och civila beslutsfattare och handläggare.

Utvecklingen mot alltmer självständiga och måldrivna AI-system aktualiserar även frågan om artificiell generell intelligens (AGI). Med AGI avses system som inte enbart är tränade för specifika uppgifter, utan som kan resonera, planera och tillämpa kunskap på ett flexibelt sätt inom vitt skilda områden, på ett sätt som i viss mån liknar mänsklig intelligens. Även om praktiskt fungerande AGI-system ännu ligger långt fram i tiden, väcker utvecklingen betydande tekniska, säkerhetsmässiga och etiska frågeställningar. Försvarsorganisationer kan på sikt påverkas av denna utveckling genom att framtida militära system i högre grad kan komma att fatta självständiga

beslut i komplexa och snabbt föränderliga situationer, vilket skulle kunna innebära ett paradigmskifte avseende hur militär teknik utformas och används.

En utveckling inom AI-området som kan förväntas de kommande tio åren är att datorer och maskiner i större utsträckning kommer att interagera med människor i den fysiska världen. Datorer används alltmer för att kontrollera olika typer av fordon; autopiloter i flygplan och självkörande bilar är kända exempel. Enkla hushållsrobotar har i dag gjort sitt intåg i våra hem i form av dammsugare och gräsklippare. En anledning till att robotar och autonoma system ännu inte förekommer i samhället i större utsträckning, är att de inte förstår sammanhang och situationer lika bra som människor, och därför inte klarar av att hantera en föränderlig omvärld tillräckligt bra. Förmågan att tolka sensordata behöver förbättras, och förmågan till en mer generell lägesförståelse måste utvecklas. Inom dessa områden görs i dag stora framsteg. Juridiska och etiska aspekter begränsar samtidigt de möjliga användningsområdena. På längre sikt kan man tänka sig en utveckling där gränsen mellan dator och människa blir allt mer diffus, och där tekniska hjälpmedel exempelvis används för att förstärka de mänskliga sinnesintrycken. En sådan utveckling är etiskt kontroversiell, men ur teknisk synvinkel fullt möjlig.

## Särskilda delområden

För dataanalys, beslutsstöd och underrättelsetjänst kan intelligenta system antingen ensamt, eller i samarbete med en mänsklig analytiker, gå igenom stora mängder data på kort tid. Datorer kan utrustas med en analysförmåga som gör att den insamlade informationen blir mer relevant för användaren. Användningsområden för dataanalys och beslutsstöd inbegriper exempelvis logistikplanering, sårbarhetsanalys, uppgiftsfördelning, strid, hotanalys och resursplanering. Tillämpad forskning inom analys- och beslutsstöd bedrivs traditionellt inom försvarsdomänen, men tillämpning av AI-tekniker sker ännu inte i någon större utsträckning. Utmaningen är att kunna tillämpa och utveckla försvarsförmåga, baserat på den snabba utvecklingen som sker inom den civila AI-utvecklingen, snarare än att utveckla helt nya lösningar.

Händelseigenkänning handlar om att utan mänsklig inblandning kunna förstå en situation som exempelvis har observerats med kamera eller återfinns i en rapport. Detta kan bland annat användas för kameraövervakning (förståelse för vad personer i bilden gör), för lägesförståelse (förståelse för vad som exempelvis händer på en karta med aktörer), i strid (för att känna igen fientligt flyg och/eller missiltyper), eller för att med ansiktsigenkänning kunna skilja mellan egna soldater och andra personer vid vaktposter. Just bildigenkänning, det vill säga förmågan att förstå vad som finns i en bild föreställande exempelvis händelser, ansikten eller fordon, har på senare år varit ett stort framgångsområde för AI-området. Genom så kallad djupinlärning kan en dator numera beskriva enklare situationer och känna igen ansikten som den ser på en bild eller genom en kamera. Att förstå komplexa samband som

observeras i övervakningskameror är fortfarande svårt, men datorer kan redan följa människor genom flera kameror, och förstå om de exempelvis springer eller slåss.

Att öva strid i okända miljöer och fjärran länder är ofta omöjligt. Spel och simuleringar används därför i allt större omfattning för scenarier som brandmän, poliser och militär personal inte kan träna för på övningsfältet. I dessa scenarier kan AI simulera med- och motspelare, och generera en spelvärld som känns realistisk. 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 som befolkar den har ett normalintelligent beteende. Försvarsforskningen inom detta område arbetar med att ta fram intelligenta datorgenererade aktörer som kan användas i simuleringar.

Som nämnts i föregående avsnitt kan AI även användas för att transkribera tal till text, översätta mellan olika språk, analysera text, summera och skapa rapporter etcetera. Alla dessa uppgifter är viktiga för försvaret och görs i dagsläget ofta av människor, eller i värsta fall inte alls. Det finns många tänkbara användningsområden, såsom transkribering av order, direktöversättning när personal pratar med lokalbefolkning, eller automatiskt skapande av rapporter, vilka kan frigöra resurser och underlätta militära operationer. För försvars- och säkerhetssektorn är användning av AI för språkhantering ett relativt outvecklat område, även om tekniker för exempelvis textanalys utvecklade inom universitetsvärlden och industrin till viss del används.

Stora framsteg har de senaste åren åstadkommits avseende utveckling av så kallade generativa modeller. Dessa AI-modeller har på kort tid givit upphov till en häpnadsväckande förmåga att på konstgjord väg generera bilder, texter, inspelningar av mänskligt tal och videofilmer, som en människa inte kan avgöra är datorgenererade. Tekniken bygger på en kombination av oövervakad maskininlärning och datorkraft, där befintliga datamängder från internet direkt kan användas, och ger upphov till en oöverträffad uttrycksfullhet, helt utan att något arbetsintensivt mänskligt arbete har gjorts. Denna utveckling kommer att fortsätta, vilket ger upphov till både hot och möjligheter sett ur ett försvars- och säkerhetsperspektiv, där det blir allt svårare att avgöra om bilder, ljud, nyhetsartiklar etcetera speglar verkliga händelser eller inte.

## Samverkande och förutsättande teknikområden

Utmaningarna för AI inom försvars- och säkerhetsområdet handlar om att kontinuerligt kunna tillämpa och utveckla förmågor baserat på god kunskap om både forskningsfronten och befintliga tekniker. Civil forskning och utveckling behöver därför kompletteras med specifika insatser avseende försvarsspecifika utmaningar rörande dataförsörjning, sårbarheter, transparens, etik, juridik med mera.

## Påverkan på militär förmåga

De delområden/teknologier som beskrivits ovan är intressanta ur militär synvinkel eftersom de kan ingå som komponenter i mer omfattande system för specifika militära tillämpningsområden. Men snarare än att det går att peka på vissa system och förmågor som kommer att påverkas, är det i stället rimligt att tänka på intelligenta system som en framtida designmetod som kan antas bli en naturlig del av alla militära system och påverka den stora bredden av militära förmågor. Några exempel ges nedan.

### Beslutsstödsystem

Eftersom information används som underlag för beslutsfattande såväl civilt som i 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.

I förlängningen handlar utvecklingen av beslutsstödsystem om att skapa och upprätthålla ett informationsövertag i komplexa och föränderliga miljöer som karaktäriseras av att det finns en motståndare som vill göra samma sak. Den sida som snabbare och mer tillförlitligt än sin motståndare kan inhämta, bearbeta och omsätta tillgänglig information till välgrundade beslut kommer att ha ett försprång. AI-baserade beslutsstödsystem möjliggör just detta genom att kombinera hög beräkningskapacitet, adaptiv analysförmåga och kontinuerlig uppdatering där AI:n lär sig och blir bättre alltefterson situationen utvecklar sig. I takt med att systemen integreras i allt fler lednings- och underrättelsefunktioner kan beslut fattas både snabbare och med högre precision, vilket stärker såväl operativ effektivitet som förmågan till strategiskt tänkande. Samtidigt aktualiseras nya utmaningar kopplade till transparens och mänsklig kontroll. Den framtida utvecklingen av beslutsstödsystem kan därmed ses som en central del av den pågående förflyttningen mot ett mer datadrivet försvar, där förmågan att utnyttja data och AI är avgörande för vem som får övertaget.

### Autonoma fordon

I ett militärt sammanhang kan autonoma eller semiautonoma 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 av fordonen

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, och dessa frågor kan tänkas bli allt viktigare i takt med att forskningen gradvis leder till att maskiner kan erhålla en mer generell lägesförståelse. En sådan generell lägesförståelse skulle kunna användas för att uppnå ett helt autonomt beteende när det kommer till att kunna agera inom mer öppna systemgränser och kunna reagera på mer svårförutsägbara och i förväg okända händelser. Autonomt fordonsunderhåll och automatisk förflyttning i syfte att uppnå skydd utgör exempel på de mer komplexa uppgifter som då skulle kunna lösas. Se även kapitlet om obemannade och autonoma system i Del 3 i denna antologi.

### 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 på scenarier som av praktiska eller ekonomiska skäl inte är möjliga att öva på i verkligheten. Det kan till exempel handla om strid i främmande miljöer eller om 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 simulerade världen, uppvisar ett lagom intelligent beteende. Ett kostsamt alternativ är att låta alla personer i den simulerade världen styras av verkliga människor. Ett mindre kostsamt alternativ är att datorgenerera beteendena för åtminstone de personer i den simulerade världen som är mindre centrala. För att kunna återskapa ett sådant trovärdigt mänskligt beteende hos de automatgenererade aktörerna är utvecklingen inom AI central. Även autonoma system som ska användas i verkligheten kan tränas upp med hjälp av simuleringar, vilket gör att utvecklingen av simulatorer för övning och träning också anknyter till utveckling av verkliga system.

Det finns dock många utmaningar med övningar i simulerade verkligheter. Miljöer, situationer eller verktyg som inte är anpassade efter verkliga förhållanden riskerar att leda till felinlärning. Det kan handla om att alltifrån enklare teknik såsom vapensikten till mer komplexa verktyg och datahantering behöver vara representativa med avseende på det lärande som eftersträvas. I en spelsituation är det också viktigt att incitamentsstrukturen i spelet/simuleringen avspeglar verkligheten såtillvida att det vinnande beteendet korrekt avspeglar det önskvärda beteendet i en verklig situation.

## Aktörer

Många vanliga arbetsuppgifter handlar i dag om it: utveckling av programvara, datorsystem och relaterad hårdvara, drift och underhåll av it-system, utbildning av användare, projektledning, planering av it-stöd och driftsäkerhet. Kompetens inom området efterfrågas inom nästan alla branscher och är ett vanligt förekommande utbildningsämne. Kopplat till denna rådande samhällsutveckling sker forskning och utveckling i stor skala med fokus på i första hand civila tillämpningar inom alla samhällssektorer, och utförarna återfinns hos snart sagt alla teknikdrivna lärosäten, forskningsinstitut och teknikintensiva företag.

Utöver att det är de civila behoven som är drivande så skiljer sig intelligenta system från andra forskningsämnen genom att en stor del av forskningen sker i industrin, och ofta är det där de bästa förutsättningarna finns. Exempelvis sker de stora forskningsframstegen ofta hos stora it-aktörer såsom Google, NVIDIA och Microsoft samt Alibaba, Tencent och Huawei, vilka hyser forskningsavdelningar och har resurser utöver vad som finns vid traditionella lärosäten och forskningsinstitut.

De stora AI-företagen har traditionellt haft sina säten i USA, men AI:s karaktär av att i grunden handla om ingenjörskunskap och tillämpning av nya forskningsrön, möjliggör dels att det sker snabba förskjutningar av maktbalanser, dels att nya aktörer snabbt kan få ett försteg och övertag enbart baserat på en god idé. Under de senaste tre decennierna har framför allt Kina utvecklats från en grundläggande industrination till en ledande högteknologisk stormakt med utbildningsprogram i världsklass. Landets satsningar på forskning, digitalisering och teknologisk innovation har lett till att Kina nu jämförs med USA när det gäller offentliga forskningsinvesteringar och teknologiskt ledarskap. Kina har också snabbt byggt ut avancerade AI-baserade övervakningssystem, vilket stärker både den inhemska industrin och den kinesiska statens kontrollmöjligheter.

Ett exempel på att nya aktörer snabbt kan få ett försteg är Lovable. Det är ett snabbväxande svenskt företag som på kort tid uppnått stor ekonomisk omsättning och en stark position med agentisk AI där de byggt vidare på en god idé: de låter användare skapa appar och webbtjänster genom att beskriva vad de vill ha med naturligt språk utan att behöva skriva en enda rad programkod.

## Lästips

Brynielsson, J., Carp, A., & Tegen, A. (2025). Detection of Emerging Cyberthreats Through Active Learning. I U. Onyekpe, V. Palade, & M. A. Wani (Red.), Recent Advances in Deep Learning Applications: New Techniques and Practical Examples (s. 123–144). CRC Press. https://doi.org/10.1201/9781003570882-9.

Franke, U., Andreasson, A., Artman, H., Brynielsson, J., Varga, S., & Vilhelm, N. (2022). Cyber situational awareness issues and challenges. I A. A. Moustafa (Red.), Cybersecurity and Cognitive Science (s. 235–265). Academic Press. https://doi.org/10.1016/B978-0-323-90570-1.00015-2.

Varga, S., Brynielsson, J., Horndahl, A., & Rosell, M. (2020). Automated text analysis for intelligence purposes: A psychological operations case study. I M. A. Tayebi, U. Glässer, & D. B. Skillicorn (Red.), Open Source Intelligence and Cyber Crime: Social Media Analytics (s. 221–251). Springer. https://doi.org/10.1007/978-3-030-41251-7_9.

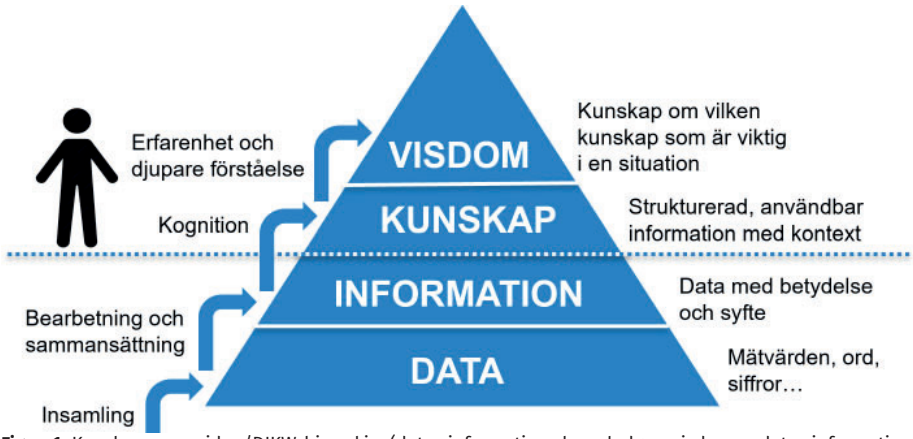
Varga, S., Sommestad, T., & Brynielsson, J. (2023). Automation of cybersecurity work. I T. Sipola, T. Kokkonen, & M. Karjalainen (Red.), Artificial Intelligence and Cybersecurity: Theory and Applications (s. 67–101). Springer. https://doi.org/10.1007/978-3-031-15030-2_4.

# Data

*Björn Pelzer och Sinna Lindquist*

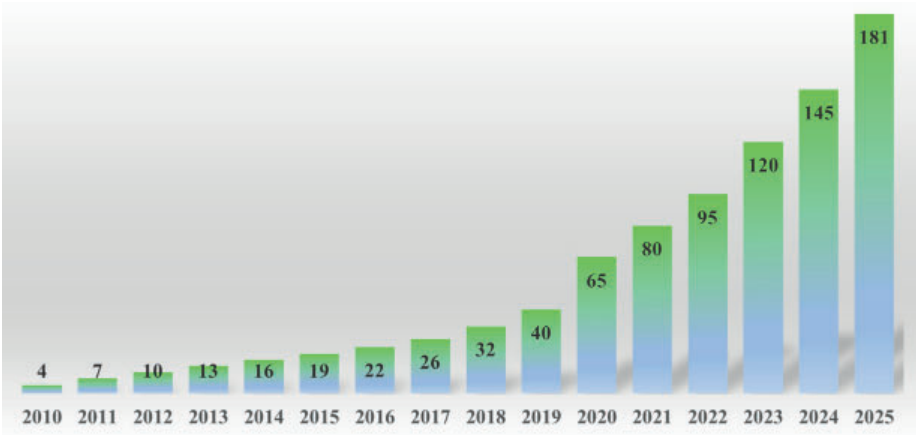
## Inledande beskrivning

Traditionellt definieras begreppet *data* som den minsta och minst abstrakta enheten av information. Den formar basen i kunskapspyramiden (se figur 1) som försöker modellera en hierarki av olika informationsnivåer. Data analyseras för att skapa information och när människan tar till sig och begriper information blir den till kunskap. Genom erfarenhet av tillämpning av kunskap blir den till slut visdom för människan. Pyramiden är en populär modell, samtidigt som den kritiseras för att vara alltför enkel, och i praktiken är gränserna mellan nivåerna otydliga. Typiska exempel för respektive nivå är att enskilda ord utgör data, meningar och avsnitt utgör information, och böcker representerar kunskap. Moderna maskininlärningssystem använder ofta tusentals böcker som träningsdata.




**Figur 1** Kunskapspyramiden/DIKW-hierarkin (data, information, knowledge, wisdom - data, information, kunskap, visdom). (Bildkälla: modifierad version av bild i Wikipedia, licens CC BY-SA 4.0).

Det finns flera definitioner av begreppet data, men ett vanligt perspektiv är att data är informationsråvara, dvs. att data är den primära råvaran i det moderna informationssamhället. Den globala produktionen av data exploderar. Världen gick in i ”zettabyte-eran” på 2010-talet, en period där zettabyte (ZB, 1 miljard terabyte) är den lämpliga enheten för att mäta mängden data som skapas, lagras, överförs och konsumeras över hela världen. Den årliga mängden har ökat i en accelererande takt, från 4 ZB under 2010 till 65 ZB år 2020, och 2025 förväntas mängden uppnå 181 ZB (se figur 2). Man uppskattar att 90 procent av alla världens data idag skapades inom de senaste två åren. Med den hastigheten vore det omöjligt och oseriöst att försöka förutspå datamängden för 2050, men utvecklingen pekar mot att nästa period, ”yottabyte-eran” (YB, 1 biljon terabyte), kommer att inledas cirka 2030.




**Figur 2** Global produktion av internet-data i zettabyte per år (bildkälla: Shirvani Moghaddam, 2024).

Orsakerna till den enorma ökningen av dataproduktion är många, men viktigast är kanske att världens befolkning växer och att digitaliseringen på global nivå ökar. Strömningstjänster, dvs. överföring av ljud, bild eller annan media via internet i realtid, svarar idag för hälften av datavolymen som transporteras över internet. Sakernas internet (IoT) och *edge computing*, som kortfattat kan beskrivas som distribuerade programmeringsramverk som möjliggör programmering och datalagring närmare datakällan, skapar dataproduktion och insamling av stora datamängder inom nya områden. Sedan cirka år 2020 påverkar även framstegen inom AI utvecklingen av data, där de moderna systemen som oftast bygger på djupinlärning kräver stora mängder träningsdata och därmed driver efterfrågan, och där generativ AI snabbt kan skapa nya data till många tillämpningsområden.

Inom Försvarsmakten har data alltid spelat en viktig roll, från underrättelser till värdering av vapenverkan till kvantifiering av militära förmågor. Detta kommer i framtiden öka i betydelse, genom att påverka och förbättra allt fler aspekter av verksamheten, samtidigt som nya beroenden och risker införs.

## Trender och exempel

Djupinlärning (*deep learning*, maskininlärning med stora neuronnät) har öppnat upp möjligheten att förbättra prestandan hos i stort sett alla datorbaserade system, från personlig utrustning till hela ekonomier – förutsatt att det finns lämpliga data tillgängliga för att träna upp systemen. Tanken bakom maskininlärning är att använda data snarare än programmering för att utveckla systemen. Ingen expert behöver skapa exakta regler som visar datorn hur den ska hantera en uppgift, utan istället tränas datorn med exempel tills den uppnår en generell förståelse av uppgiften. Vanligtvis behöver dessa träningsexempel fortfarande annoteras, dvs. ges metainformation, som mappar exemplet till svaret som förväntas av datorn.

Ett exempel är en detektor för hatpropaganda på sociala medier. Detektorn tränas med tusentals textexempel som är annoterade med antingen *hat* eller *icke-hat*, tills detektorn har lärt sig att känna igen olika exempel på hat i text. Annotering kräver ofta att människor annoterar och blir därmed kostsam, men djupinlärningen presterar vanligtvis betydligt bättre än system med explicit programmerade regler. Dessutom kan träningsdata återanvändas för att träna nya system, kombineras med andra data eller förfinas. Man kan säga att träningsdata är en flexibel råvara. I vissa fall behövs inte någon annotering (*unsupervised learning*), eller så kan befintliga data användas som annotering. Många internetforum, som exempelvis Reddit, har en funktion där skribenter kan markera andras textbidrag som hjälpsamma eller inte (*upvote*/*downvote*), och de markeringarna kan vara en värdefull resurs för maskininlärning.

Det som är beskrivet ovan är motiv för storskalig datainsamling, eller för att skapa data. Miniatyrisering och stordriftsfördelar gör det också möjligt att installera sensorer och datorer för datainsamling i allt fler och allt mindre enheter. Även om konsumenterna idag översköljs av tvivelaktiga prylar, som t.ex. AI-utrustade tandborstar, visar den underliggande tekniska utvecklingen hur genomgripande datagenerering och datainsamling kommer att bli.

Stora mängder data har redan samlats in under årtionden, t.ex. inom stora organisationer som företag, underrättelsetjänster och försvarsmakter. Denna ”råvara” och värdefulla resurs av data samlades (och samlas fortfarande) oftast inte in med maskininlärning i åtanke. De är istället ostrukturerade datamängder och lagras ofta i format som är olämpliga för direkt automatiserad bearbetning, t.ex. i PDF-filer eller på pappersdokument, eller i form av bild- och videomaterial. Det hävdas att över 80 procent av all data är ostrukturerad.[52] Det kommer därmed att krävas stora insatser för att digitalisera dessa data, men det kommer att vara motiverat om det ger ett försprång gentemot konkurrenterna, både inom näringslivet och inom försvarssektorn.

Den accelererande tillväxten av data gör alla försök till långsiktiga förutsägelser opålitliga. Två aktuella och sammanflätade trender kommer dock att påverka utvecklingen och skapa framtida vägskäl vars konsekvenser kommer att förstärkas av den totala datatillväxten. Dessa trender är generativ AI och juridikens utveckling, dvs. utveckling av lagar och regelverk, avseende data generellt och dataanvändning specifikt.

Generativ AI avser AI-system baserade på vanligtvis mycket stora generativa modeller tränade på stora mängder data, vilket ger dem förmågan att skapa nya data, såsom texter, bilder och videor. Framträdande exempel är stora språkmodeller, s.k. LLM:er (*large language models*) så som amerikanska ChatGPT (OpenAI), som är kapabla

52 Unstructured Data and the 80 Percent Rule | Breakthrough Analysis, The Unseen Data Conundrum, Big Data Statistics 2025 (Growth & Market Data), Unstructured Data Is Exploding. Is Your Infrastructure Ready? — Files.com.

att skriva texter på en nivå jämförbar med mänskliga författare men på kortare tid än en människa. Med dessa LLM:er kan man bedriva textbaserade konversationer för att lösa textbaserade uppgifter som t.ex. att sammanfatta artiklar eller skriva datorprogram.

Generativ AI har fått stor uppmärksamhet från allmänheten sedan början av 2020-talet, och i skrivande stund råder både stor hajp och stor oro kring tekniken. Kommersiella aktörer framhåller tekniken som vägen mot AGI (*artificial general intelligence*, artificiell allmän intelligens), dvs. en typ av (över)mänsklig AI som kommer att kunna lösa praktiskt taget alla uppgifter. Kritiker oroar sig för att AI ersätter mänskliga jobb och för miljöpåverkan av den extremt energikrävande teknologin. Andra är mer skeptiska till de utlovade förmågorna och påpekar att de kommersiella AI-aktörerna fortfarande går med förlust och saknar hållbara affärsmodeller, och att grundläggande brister som ”hallucinationer”, dvs. generering av icke-faktisk information, förblir olösta. Enligt en nyligen genomförd undersökning bland AI-forskare tror 76 procent inte att generativ AI kommer att leda till AI på mänsklig nivå.[53]

Oavsett vem som i framtiden får rätt, så kan redan idag generativ AI producera stora mängder av åtminstone till synes rimliga data. Dessa syntetiska data kan potentiellt förändra alla områden där sanningsenlighet och detaljriktighet kan vara mindre avgörande, till exempel inom konst och underhållning, eller inom vissa simuleringar, inklusive militära sådana. Syntetiska data kan också användas som träningsdata för andra maskininlärningssystem, vilket minskar behovet av kostsam inhämtning och annotering. Omvänt finns det en risk för att genererad data översvämmar media med desinformation, och att den, avsiktligt eller oavsiktligt, hindrar inhämtningen av icke-syntetiska träningsdata, eftersom de två typerna blir allt svårare att särskilja. Generellt kan man säga att data som används för att träna en AI-modell påverkar hur väl en modell fungerar, vilket innebär att säkerställande av datakvalitet är av avgörande betydelse.

Den andra trenden med stort inflytandet och osäkra konsekvenser är juridikens utveckling i relation till AI-baserade system och data som AI-modellerna är tränade på. Framväxten av sociala medier under 2000-talet har ökat medvetenheten om värdet av personuppgifter, och i många jurisdiktioner har man skapat lagstiftning för att skydda befolkningen från kommersiell dataexploatering, särskilt inom EU. Utöver detta började företag omkring 2020 använda automatiserade så kallade webbspindlar (eng. *crawlers*) för att samla in praktiskt taget all tillgänglig internetdata och sedan träna AI-system, såsom de stora generativa modellerna. Resultatet är en alltmer motstridig global utveckling med en oklar framtid. I USA ser vi juridiska försök från upphovsrättsinnehavare att skydda sina datatillgångar mot utnyttjande av AI-företag. Till exempel har New York Times stämt OpenAI och försöker

53 https://aaai.org/about-aaai/presidential-panel-on-the-future-of-ai-research/.

stänga ner ChatGPT. AI-företagen däremot vill urholka upphovsrättslagen genom att försöka etablera generösa tolkningar av *fair use*-klausuler. I EU begränsar kombinationen av GDPR och *AI Act* de lagliga möjligheterna för datainsamlingsföretag. Skillnaderna mellan nationella datalagstiftningar är problematiska för internationella företag och orsakar redan idag politiska spänningar mellan USA och EU. Oavsett resultatet ökar dessutom det praktiska motståndet från dataägarna mot kommersiellt utnyttjande. Allt fler tekniska lösningar dyker upp som ska skydda data mot AI-företagen genom exempelvis traditionella betalväggar, sofistikerad detektering och blockering av automatiserade webbspindlar. Till detta kan läggas de senaste generativa labyrintmetoderna där webbspindlarna kör fast i oändliga mängder av värdelösa syntetiska data. Framtidens globala datalandskap kommer att vara stort och rikt, men troligen splittrat i hårt skyddade ”silos”.

## Särskilda delområden

Få områden illustrerar fördelarna och riskerna med maskininlärning så väl som utvecklingen av självkörande bilar. Det är omöjligt att exakt beskriva alla situationer som en bil kan stöta på, och därför har de senaste årens framsteg främst berott på storskalig maskininlärning. Ändå är kvaliteten och täckningen av träningsdata fortfarande avgörande, eftersom avsaknaden av minsta detalj kan få allvarliga konsekvenser. Till exempel kan tillfälliga vägmarkeringar i vissa länder ha en annan färg än i tillverkarens träningsområde. En autonom bil kan då ha miljontals timmars träningsdata, men om en sådan detalj saknas kan fordonet orsaka allvarliga olyckor. Därför är tillverkare angelägna om att samla in enorma mängder realistiska träningsdata. Riskerna och kostnaderna för detta ger en fördel för stora tillverkare som kan utnyttja data från sensorer i sina befintliga icke-autonoma fordonsflottor. Det är attraktivt att falla tillbaka på syntetiska data, till exempel genom att köra virtuellt i simulerade världar, eller helt enkelt genom att använda generativ AI för att analysera befintliga träningsdata och sedan skapa mer av sådana data. Det är lätt att se hur ett sådant tillvägagångssätt snabbt kan producera stora mängder träningsdata, men om simuleringen eller genereringen saknar trovärdighet kan kvaliteten hos syntetiska träningsdata vara otillräcklig.

Dynamiken i denna situation, dvs. avvägningar mellan syntetiska och verklighetsbaserade data, där större och äldre aktörer eventuellt kan ha konkurrensfördelar, kommer att bli relevant inom fler och fler områden under de kommande åren. Aggressiva försök att överbrygga eventuella datagap gentemot konkurrenterna kommer sannolikt att bli allt vanligare. Data kommer att samlas in när och var som helst genom att alla möjliga apparater kopplas upp och görs ”smarta”, och kommer att samlas in från tillgängliga källor, oavsett om detta är lagligt eller inte. Maskininlärningens princip gör det svårare att bevisa att ett givet AI-system faktiskt tränades på vissa specifika data. De neurala nätverken lagrar inte kopior av sina träningsdata, träningen ändrar bara interna numeriska vikter i nätverksnoderna.

Ändå har forskningsområdet AML (*adversarial machine learning*, fientlig maskininlärning) producerat metoder som så kallade extraktionsattacker och *membership inference attacks* som med viss framgång indikerar vilken data ett AI-system tränades på. Sådana metoder har redan använts i rättegångar, till exempel av New York Times mot OpenAI för att visa att ChatGPT ibland återger tidningsartiklar ordagrant, eller av Getty Images mot StabilityAI för att visa att deras AI-bildgenerator har tränats på Gettys fotokatalog utan tillstånd. Aktörer som inte har möjlighet att skaffa tillräckliga träningsdata på egen hand kommer sannolikt också att använda liknande metoder för att extrahera data från konkurrenternas AI-system. OpenAI har anklagat det kinesiska företaget Deepseek[54] för att exploatera ChatGPT när de skapade ett liknande AI-system till avsevärt lägre kostnad, en situation inte utan ironi med tanke på den tvivelaktiga juridiska statusen för OpenAI:s egen datainsamling.

Oavsett ovannämnda kvalitetsrisker kommer sannolikt syntetiska data fortsatt vara attraktiva och dessutom utgöra en ökande andel av alla globala träningsdata inom de flesta områden av främst två skäl – låg kostnad och möjlighet till undvikande av juridiska fallgropar. Om AI-träning på AI-genererade data blir vanlig kan konsekvensen bli en utbredd stagnation för AI:s framsteg, på grund av ett fenomen som kallas modellkollaps, i vardagsspråket även känt som ”AI-incest”. Det innebär att brister som introduceras genom datasyntes ackumuleras och förstärks från generation till generation. Detta misstänks redan idag bromsa utvecklingen av stora språkmodeller. Dessa förlitar sig alltmer på syntetiska träningsdata, eftersom alla lågt hängande frukter av lättillgängliga internettexter redan har bearbetats, och att nya texter med växande sannolikhet har genererats av AI. De vetenskapliga åsikterna är fortfarande delade om de långsiktiga effekterna av modellkollaps och om det finns effektiva metoder för att övervinna problemet.

Utöver maskininlärning kommer utvecklingen kring data sannolikt att ha jämförbara effekter i andra områden. Data kommer att skapas och lagras överallt, och syntetiska data kommer att utgöra en allt större andel. Vi ser redan idag hur media experimenterar med AI-genererade nyhetsartiklar. Genererade bilder och till och med videor har uppnått en kvalitet som ibland kan vara tillräcklig för publicering. Detta kan vara ofarligt i vissa fall, till exempel genererade bilder som dekoration, eller syntetiska diagram. Men det blir problematiskt när syntetiska data presenteras som data baserat på verkligheten, det vill säga som texter skrivna av mänskliga författare eller fotografier tagna i verkliga situationer. Manipulation av media har alltid varit möjlig, men de tekniska hindren var tidigare högre än idag, och foton och videor kunde vanligtvis antas motsvara verkligheten. Detta håller på att förändras, och vi är sannolikt i en övergångsfas nu där människor i allt större utsträckning misstror bilder. År 2050 kommer en hel generation att ha vuxit upp i en miljö där vem som helst snabbt kan producera realistiska presentationer av praktiskt taget

54 DeepSeek: Ändamålsenlighet och tillförlitlighet, Edward Tjörnhammar m.fl. Öppen FOI-rapport, under publicering.

vilket innehåll som helst till en försumbar kostnad. Effekterna på vårt samhälle är svåra att uppskatta.

Det här innebär också att media, underrättelsetjänster och dataanalytiker i allt högre grad kommer att behöva hantera en värld där syntetiska data blir omöjlig att skilja från verklighetsbaserade data. Idag är det emellanåt fortfarande möjligt att detektera den skillnaden för ett givet dataprov, baserat på mer uppenbara brister i syntesen, t.ex. när en bildgenerator ritar händer med för många fingrar. Men syntesen förbättras ständigt, och sådana brister kommer snart att vara ett minne blott. Digital vattenmärkning av data är en metod för att säkerställa att distinktionen förblir möjlig genom att vattenmärka syntetiska data så att den kan detekteras, eller genom att vattenmärka verklighetsbaserade data så att den kan kännas igen som äkta. Båda tillvägagångssätten kan tillämpas på nästan alla typer av data, men båda tillvägagångssätten är också långt ifrån perfekta. Oseriösa användare av generativ AI kommer helt enkelt inte att vattenmärka sina syntetiska produkter. Befintliga äkta data är vanligtvis inte vattenmärkta, och det måste analytiker ta hänsyn till. Det finns dessutom metoder för att ta bort och kopiera digitala vattenstämplar, vilket ytterligare försvagar tillförlitligheten för dessa metoder.

Dessa osäkerheter gör att det blir allt viktigare att upprätthålla en god dataförvaltning (*data governance*). Detta avser kombinationen av policyer, metoder och teknologier inom en organisation för att säkerställa att data hanteras på ett korrekt och spårbart sätt. I synnerhet blir det allt viktigare att upprätthålla dokumentation av datahärkomst (*data lineage* eller *data provenance*),[55] alltså att dokumentera var data kommer ifrån, och i vilka steg den har bearbetats eller transformerats, och när och av vem. Detta möjliggör identifiering av system som påverkas av data, samt att dra tillbaka ändringar, ta bort delar av data som visats sig vara problematiska, eller att reproducera bearbetningskedjan. Det finns också säkerhetsaspekter, exempelvis att säkerställa att inga datamanipulationer har introducerats av illvilliga aktörer. Dataförvaltning är idag vanlig inom områden som exempelvis regleras av GDPR och som kan ge höga straff ifall data hanteras på fel sätt, men den kan förväntas bli relevant inom alla områden där det är viktigt att upprätthålla datakvaliteten av prestandaskäl.

## Samverkande och förutsättande teknikområden

Data är den immateriella resurs eller om man så vill, den abstrakta råvaran, som driver det moderna informationssamhället. Den genereras inom alla tekniska områden och påverkar alla tekniska områden men även icketekniska områden, i och med en ökad datadriven utveckling av t.ex. beslutsfattande. Alla områden med tekniska system

55 Vissa engelska källor ser subtila skillnader mellan *data lineage* och *data provenance*, men det finns ingen konsensus om hur termerna skulle definieras individuellt eller vad den faktiska skillnaden skulle vara i praktiken. Andra källor betraktar termerna som helt synonyma, en uppfattning vi delar här.

som involverar kommunikation producerar och processar data. Alla områden och tekniska system med mätbara prestandamått kan potentiellt producera data som sedan kan analyseras och användas för att förbättra prestandan.

Data är abstrakt och existerar inte oberoende utan en hårdvaruinfrastruktur. De ständigt ökande datamassorna kommer att behöva transporteras och lagras, så alla aspekter inom informationsteknologin behöver skalas upp i relation till datautvecklingen. Resultatet är unik datateknik där miniatyrisering möjliggör lagring av allt större datamängder i allt mindre enheter, och med framtidens 6G-mobilnät kommer allt fler enheter att kunna kommunicera data.

Samtidigt öppnar detta upp nya angreppsytor för motståndare som vill stjäla eller manipulera data. Cybersäkerhet kommer därför att fortsätta växa i betydelse och behöver anpassas till att data kan skapas och bearbetas praktiskt taget överallt.

Ett växande behov av att kunna nyttja mer befintliga data kan förväntas leda till framsteg inom teknologier som kan digitalisera, extrahera och sammanfatta data. Exempel på det är bättre OCR-metoder för att digitalisera data på papper, AI-metoder för att hantera ostrukturerade digitala data (som PDF-filer) och automatisk analys av videodata.

Ledningssystem har stort behov av snabb tillgång till rätt data. Beslut måste fattas baserat på aktuella och korrekta data och information vid varje given tidpunkt. AI och informationsfusion kommer i allt högre grad att kunna kombinera data från olika källor till lättförståeliga samlade lägesbilder, vilket avsevärt kan gynna beslutsfattandet. Detta måste dock balanseras med den tid som läggs på databehandling och potentiella nya risker och osäkerheter som införs. Mindre förfinad eller rå data kan vara att föredra i vissa situationer.

## Påverkan på militär förmåga

Framtidens utveckling inom dataområdet har potentialen att påverka praktiskt taget alla militära förmågor. Dessa beskrivs främst i andra kapitel i denna antologi, och de nämns här bara kort. Fokus för detta kapitel är de mer direkt datarelaterade konsekvenserna för försvaret.

Autonoma vapensystem verkar idag oundvikliga med tanke på deras löfte om att minska både behovet av och risken för mänskliga soldater, och prestandan hos sådana system är direkt kopplad till tillgången på högkvalitativa träningsdata. Detsamma gäller militära beslutsstödsystem där tillgång till stora mängder lämpliga data möjliggör träning av mer och mer komplexa AI-modeller som kan analysera situationer i djupare detalj och producera resultat för effektivare beslut. Soldater kommer att kunna dra nytta av mer realistiska simuleringar som därför förbereder dem bättre inför faktiska stridshandlingar, samtidigt som detta minskar kostnaderna och riskerna jämfört med att genomföra övningar i verkligheten. Konventionell

utrustning kommer att samla in mer data om sin prestanda, vilket underlättar utvärderingen och vidareutvecklingen, samt möjliggör en mer exakt simulering av utrustningens användning. Detta kommer också att i hög grad påverka livscykelhanteringen av utrustningen, eftersom mer exakta data kommer att möjliggöra mer exakta förutsägelser av underhållsbehov, dvs. prediktivt underhåll.

I likhet med den kommersiella civila sektorn kommer ett försprång i tillgången till högkvalitativa data att ge militären ett försprång i prestanda gentemot konkurrenterna, det vill säga militära motståndare. Kostnaderna och säkerhetsriskerna för krigsmateriel utesluter dock realistiska tester i en skala jämförbar med t.ex. utvecklingen av självkörande bilar. Inom försvarssektorn är data därför mer värdefulla, och försvarsstyrkorna i olika länder skiljer sig mycket åt i storlek, budget och praktisk erfarenhet, vilket leder till skillnader i tillgång till data. Till exempel måste vi anta att Ryssland har samlat in betydande mängder (verklighetsbaserade) data, till exempel avseende materielsystem och deras prestanda samt data för förbandens agerande i terrängen, under sin invasion av Ukraina. Detta kan ge ryska försvaret en fördel i framtida utveckling som är svår att kompensera för försvarsmakter med mindre praktisk erfarenhet.

Försvarsmakter har alltid skyddat sina data, och skyddsbehovet kommer fortsätta öka, både skydd emot motståndare, och i viss grad även skydd mellan allierade. När data skapas och används överallt uppstår också fler och nya möjligheter att komma åt en annan nations försvarsdata. Praktiskt taget all utrustning kommer kunna generera, lagra och överföra data, och alla sådana enheter bli värdefulla underrättelsemål. Cybersäkerhet kommer att behöva anpassas för att skydda militära data i sammanhang där detta tidigare var irrelevant.

Utöver traditionell cybersäkerhet kommer försvaret också att behöva ta hänsyn till nya sårbarheter som introduceras genom djupinlärning. System baserade på djupinlärning betraktas ofta som ”svarta lådor”. Visserligen gör de det man har tränat dem för, men därutöver har man ingen insyn i hur de ”resonerar” eller ”tänker”. De tidigare nämnda extraktionsattackerna utgör dock en ny form av exploatering där motståndare faktiskt kan få insikter i de data som ett givet AI-system tränats på. Detta kan i sin tur göra det möjligt för motståndarna att träna sina egna system för att nå likvärdiga prestanda, eller att upptäcka brister i det aktuella systemet. Till exempel kan det vara möjligt att identifiera situationer som systemet inte har tränats tillräckligt i att hantera.

Även data i sig kan vara, och i ökad utsträckning bli, ett vapen i samband med maskininlärning. Dataförgiftning avser att infoga värdelösa eller kontraproduktiva data i en till synes användbar och korrekt datamängd för träning (träningsdatamängd). Till exempel skulle en statlig aktör anonymt kunna publicera en öppen datamängd som utger sig att vara lämplig för att träna upp AI-system för identifiering av stridsfordon, men där delar av datasetet manipulerats på ett sådant sätt

att alla system som tränas avsiktligt kommer att felaktigt identifiera just de stridsfordon som används av den aktör som skapade datasetet. Sofistikerade metoder kan dölja sådana manipulationer av data, och försvarsstyrkor som försöker överbrygga sina egna databrister genom att förlita sig på öppna data måste vara medvetna om dessa risker.

## Aktörer

Det är svårt att peka ut några speciella datarelaterade aktörer i en framtid där data skapas och används överallt. Det nuvarande landskapet av aktörer kommer att fortsätta att skalas upp tillsammans med den snabba ökningen av data. Generellt kan kompetensen att hantera data förväntas öka inom alla områden. Lagar och internationella överenskommelser kommer att minimera nuvarande gråzoner och kryphål, även om det är svårt att förutse vilken specifik riktning som denna utveckling kommer att ta. I takt med att medvetenheten om värdet av data växer kommer kommersiella aktörer i allt högre grad att söka möjligheter att tjäna pengar på all data som de har till sitt förfogande. Ett exempel på detta idag är diskussionsplattformen Reddit, som ursprungligen finansierades genom att sälja reklam riktad till sina användare, men som 2024 började sälja tillgång till sina användardiskussioner som träningsdata för AI-företag. Specialiserade datamäklare som säljer aggregerade och kurerade data till de som vill utöka sin egen datagenerering kommer att bli allt vanligare. Företag som Palantir kommer att tillhandahålla datahantering och analys inom alla områden, vilket hjälper dem som ännu inte är utrustade att hantera den ständigt växande datasfären.

## Lästips

Shirvani Moghaddam; Shahriar (2024). The past, present, and future of the Internet: A statistical, technical, and functional comparison of wired/wireless fixed/mobile Internet. Electronics. 13.1986.10.3390/electronics13101986.

Kamrani, Farzad; Kanestad, Linus; Luotsinen, Linus; Pelzer, Björn; Sabel, Johan; Sandström, Viktor; Tegen, Agnes (2023). Attacking and deceiving military AI systems. FOI-R--5396--SE. FOI.

Shumailov, Ilia; Shumaylov, Zakhar; Zhao, Yiren; Papernot, Nicolas; Anderson, Ross; Gal, Yarin (2024). AI models collapse when trained on recursively generated data. Nature. 631 (8022).

Guo, Yanzhu; Shang, Guokan; Vazirgiannis, Michalis; Clavel, Chloé (2024). The curious decline of linguistic diversity: training language models on synthetic text. arXiv:2311.09807.

Carlini, Nicholas; Tramer, Florian; Wallace, Eric; Jagielski, Matthew; Herbert-Voss, Ariel; Lee, Katherine; Roberts, Adam; Brown, Tom; Song, Dawn; Erlingsson, Ulfar; Oprea, Alina; Raffel, Colin (2020). Extracting training data from large language models. arXiv:2012.07805.

# Kvantteknik

*Per Jonsson och Jonas Kjäll*

## Inledande beskrivning

Kvanttekniker är tekniker som nyttjar kvantfysikens lagar. Kvanttekniker som påverkar vårt samhälle är exempelvis transistorn, lasern och atomklockan. I dag står vi inför nästa kvantteknikrevolution. Anledningen är den senaste tidens forskningsframsteg som gör att system nu kan designas på atomnivå, där kvantfysikens lagar dominerar. Exempel på kvanttekniker som förutspås revolutionera sina områden är kvantdatorn, kvantsensorer och kvantkommunikation.

Andra läsvärda beskrivningar av framtidens kvanttekniker återfinns exempelvis i FMV:s tekniska prognos nr. 1 2023[56], Chalmers populärvetenskapliga översikt av området[57] och den översikt av området som gjordes av Chalmers Industriteknik på uppdrag av FMV[58]. FOI har tidigare studerat området, 2019 och 2020.[59]

Kvantfysiken[60] beskriver världen på den mest fundamentala nivån, i form av partiklar, exempelvis elektroner och atomer, samt deras växelverkan. Sedan dess upptäckt i början av 1900-talet har kvantfysik varit ett viktigt forskningsområde. De senaste åren har vår möjlighet att skräddarsy kvantmekaniska system med önskade egenskaper ökat markant. Detta skapar nya möjligheter, där kvantfysikaliska effekter kan utnyttjas istället för att betraktas som okontrollerbara störningar, vilket tidigare ofta varit fallet.

Viktiga kvantfysikaliska fenomen är partikel-våg-dualitet, kvantisering, superposition, sammanflätning och osäkerhetsprincipen. Kvantobjekts, t.ex. atomer och ljus, partikel-våg-dualitet betyder att de ibland behöver beskrivas som en partikel och ibland i form av en våg. Kvantobjekts partikel-våg-dualitet tillåter interferometri[61], t.ex. kan atomers vågegenskaper användas för extremt noggranna mätningar. Att fysikaliska storheter är kvantiserade betyder att de endast kan anta vissa diskreta värden, t.ex. energinivåerna hos en atoms elektroner. Ett kvantobjekt kan befinna sig i en så kallad superposition av flera olika kvantiserade tillstånd, vilket betyder att det ”tycks befinna sig i två (i den klassiska fysiken) oförenliga tillstånd samtidigt”.[62]

56 Teknisk prognos Rapport Nr 1 2023, Tema Kvant, FMV dokumentbeteckning: 22FMV1402-25, https://www.fmv.se/globalassets/dokument/om-fmv/teknisk-prognos-nr-1_20232.pdf.

57 https://www.chalmers.se/centrum/wacqt/upptack-kvantteknologi/.

58 S. Charpentier (red.) ”Framtida utveckling inom Kvantteknologi”, 2022-11-24.

59 J. Kjäll, P. Jonsson, ”Kvantteknologier-2019”, FOI Memo 7034, 2020.

60 https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/kvantfysik. Kvantfysik används ofta synonymt med kvantmekanik och kvantteori.

61 Mätning av interferens mellan koherenta vågor från en och samma källa. https://sv.wikipedia.org/wiki/Interferometri.

62 https://it-ord.idg.se/ord/superposition.

Exempelvis gör superposition att kvantbitar kan hålla en kombination av de digitala värdena 1 och 0 samtidigt, vilket nyttjas av en kvantdator i beräkningar. Detta är en viktig skillnad mot digitala system, vars bitar deterministiskt håller antingen 1 eller 0. I beräkningar vars resultat är en superposition erhålls endast ett av värdena med en sannolikhet svarande mot den kombination kvantbiten beskriver.

Ett sammanflätat objekt består av objekt som vi normalt betraktar som separata, exempelvis två atomer, men som nu beror så starkt av varandra att de inte kan beskrivas separat, utan måste beskrivas som ett gemensamt kvantobjekt. Både superposition och sammanflätade kvantobjekt är förutsättningar för kvantdatorer.

Osäkerhetsprincipen säger att det finns en begränsning i hur noggrant vissa par av fysikaliska storheter kan bestämmas. Exempelvis blir, vid väldigt noggrann bestämning av ett systems position, dess rörelsemängd mer osäker. Att kvantfysiken i grunden är icke-deterministisk gör att den sällan är intuitiv och inom området har många fenomen upptäckts som saknar motsvarighet i den värld vi upplever.

Kvanttekniker använder kvantfysikaliska fenomen för att skapa nya tillämpningar och tekniker. Idag används flera tekniker som kan benämnas kvanttekniker. Laser är ett exempel som funnits i över 50 år, där användningsområden utvecklats över tid och nu finns inom kommunikation, mätning, medicin och skärning för att nämna några. De flesta befintliga kvanttekniker kan förklaras med semi-klassisk teori, dvs. det räcker att atomerna kvantiseras medan elektromagnetiska vågor beskrivs klassiskt. Dessa tekniker utnyttjar ett fåtal kvanttillstånd men inte sammanflätning och partikel-våg-dualitet. Andra exempel på tillämpningar baserade på kvantteknik är t.ex. halvledarteknik, supraledande magnetometrar och atomklockor som bland annat används i globala satellitnavigeringssystem (GNSS). Betydligt fler tillämpningar är på gång, som kvantaccelerometrar och kvantkommunikation mellan två noder där mer av kvantfysiken behövs för att förklara fenomenen.

Mer avancerade kvanttekniker, där kvantfysik används i större utsträckning, som kvantdatorer och kvantmekaniskt sammanflätade sensorsystem, ligger längre bort tidsmässigt, men innebär än mer fascinerande användningsmöjligheter. I dagsläget investerar den civila sektorn globalt stora summor på forskning och utveckling inom kvantteknikområdet. Inom den militära sektorn satsas det också ordentligt, främst i de större länderna, även om inte summorna kan mäta sig med det som satsas civilt. Följaktligen är potentialen stor att helt nya tekniker och användningsområden som bygger på kvantteknik kommer att utvecklas de närmaste 25 åren. Vilka dessa kommer att bli, och vilka konsekvenserna blir för försvar och säkerhet, är svåra att förutse. Nedan diskuteras de områden som forskarvärlden fokuserar på idag och som antas vara av intresse för Försvarsmakten.

## Trender och exempel

Kvanttekniker har potential att påverka många teknikområden. Här fokuserar vi på de kvanttekniker där det idag bedrivs aktiv forskning, men som ännu inte kommersialiserats. Extra viktiga är de kvanttekniker där militära aktörer finansierar forskning och utveckling. Risken att halka efter bedöms vara störst där, vilket kan leda till relativa förmågegap inom berörda områden.

De flesta kvanttekniker har civila tillämpningar. Där civila aktörer driver utvecklingen utvecklas tekniken ofta snabbare. Om det finns kunskap och produkter tillgängliga på den öppna marknaden går det också ofta snabbare att ta ikapp ett förmågegap.

Såväl Försvarsmakten som Nato har pekat ut kvanttekniker som en viktig framväxande och omvälvande teknik. *NATO Science and Technology Organization* (STO) har arbetsgrupper, där FOI deltar, som utvärderar de kvanttekniker som bedöms komma att påverka militära teknik- och förmågeområden. Kvanttekniker kan delas in i fyra områden:

- Kvantdatorer och kvantsimulerare, hårdvara som förväntas vara överlägsen klassiska datorer för vissa typer av beräkningar (se nästa punkt).
- Kvantberäkningar, algoritmer och simuleringar som utförs på kvantdatorer, t.ex. optimeringsproblem och framtagande av material med nya egenskaper. På längre sikt kan kvantberäkningar hota dagens kryptering med asymmetriska nycklar.
- Kvantsensorer och mätteknik, som inkluderar tröghetsnavigeringssystem, atomklockor, accelerometrar, gravitometrar, magnetometrar och elektromagnetiska sensorer som bygger på kvantteknik.
- Kvantkommunikation över såväl som under vattenytan och med kvantnyckeldistribution, kryptering och dekryptering.

Intressanta områden där försvarsaktörer är med och driver utvecklingen inkluderar främst sensorutveckling, primärt för förbättrad detektion och förbättrad navigering i miljöer utan tillgång till extern positionering som GNSS. Kvanttekniker kan förbättra navigeringsmöjligheterna dels genom signifikant minskade fel i accelerations- och vinkelaccelerationsbestämningen i tröghetsnavigeringssystem, dels genom noggrannare sensorer för fixpunktsnavigering. Anomalier i jordskorpans magnetfält respektive anomalier i jordskorpans gravitationsfält är två lovande möjligheter för passiv fixpunktsnavigering. För detektion lovar nya sensortekniker större noggrannhet och högre känslighet. Det högre signal-brus-förhållandet gör att det går att mäta på större avstånd och därmed få en mer översiktlig bild. Det forskas på nya kvanttekniker för de flesta signaturer som Försvarsmakten är intresserade av idag och därutöver kan den nya tekniken göra att ytterligare signaturer blir intressanta. Ett exempel är anomalier i gravitationsfältet, som skulle kunna användas för detektion

av begravda objekt, som landminor och oexploderad ammunition, underjordisk byggnation, som tunnlar och fortifikation, samt ubåtar i undervattensläge. Ett relaterat område som kommer påverkas är signaturreduktion. Detektionsavstånden för dagens smyg- och störningstekniker riskerar att öka markant.

Utvecklingen inom kvantdatorer och kvantkommunikation drivs främst av kommersiella aktörer. Kvantdatorer bedöms i framtiden kunna köpas på en öppen marknad, på liknande sätt som ett beräkningskluster köps in idag. Kompetent personal som kan utföra simuleringar på kvantdatorer kommer troligtvis behövas, åtminstone inledningsvis. Intressanta problem är optimeringsproblem och kvantfysikaliska problem. Ett lovande exempel på det förstnämnda är logistikproblem. Det sistnämnda inkluderar molekyl- och materialberäkningar och skulle t.ex. kunna användas för att ta fram nya sprängmedel. Det är ett aktivt och öppet forskningsområde idag att identifiera de problem en kvantdator kommer att kunna lösa bättre än en klassisk dator. Kvantkommunikations främsta användningsområde för Försvarsmakten bedöms vara mellan utspridda sensorer om de kan sammanflätas kvantmekaniskt. Detta ligger en bit fram i tiden men skulle markant ändra vad som kan mätas och detekteras. Flertalet signaturreducerande åtgärder kommer i detta fall troligen bli verkningslösa.

## Särskilda delområden

2018 gjorde Nato en avskanning av kvanttekniker, *von Kármán Horizon Scanning on Quantum Capabilities for Sensing and Communications*[63], där experter från forskningsinstitut, industrin och militären bedömde kvantteknikernas inverkan för Nato. I denna studie ingick inte kvantdatorer och kvantberäkningar. Mycket av det studien kom fram till om teknikerna och tillämpningarna stämmer fortfarande väl, även om tidsuppskattningarna behövt modifieras. Idag börjar kvantsensorer nå den prestanda som behövs för militära tillämpningar, medan nyttan av kvantkommunikation, kvantdatorer och kvantberäkningar ligger längre fram i tiden.

### Kvantsensorer och mätteknik

Idag bedrivs mycket forskning inom mätning och sensorer som bygger på kvantfysikaliska fenomen. Stora framsteg har gjorts de senaste åren och fler förväntas komma på kort såväl som lite längre sikt.[64] Tidigare sågs ofta kvantfysikaliska fenomen som en begränsning för tekniken, t.ex. sätter de en brusgräns för hur noggranna klassiska sensorer kan bli. Idag har synsättet förändrats och istället för att se dessa fenomen som en begränsning kan de med rätt konstruktion användas för att nå precisioner man tidigare bara kunnat drömma om. Nämnas bör att sensorer som bygger på

63 "von Kármán Horizon Scanning on Quantum Capabilities for Sensing and Communications – Summary Report", Nato, 2018.

64 K. Bongs, S. Bennett, A. Lohmann, "Quantum sensors will start a revolution – if we deploy them right," Nature, 617, 672–675, (2023). doi: 10.1038/d41586-023-01663-0.

kvantfysik, exempelvis supraledande kvantinterferensenhet (SQUID) och kärnmagnetisk resonans (NMR), har funnits i ett antal år. Dessa behandlas inte vidare här.

En av de nya kvantsensorerna som bedöms vara mest intressant är kvävevakanscenter i diamant. Dessa kan exempelvis användas för mätning av magnetiska fält, elektriska fält och tryck. Utöver den förväntade höga noggrannheten finns flera fördelar hos dessa sensorer. Sensorerna kan användas i rumstemperatur, i starka magnetfält som jordens, mätpunktens dimensioner är under en millimeter och dessutom sträcker sig frekvensintervallet som kan undersökas från statik till många GHz.

Två andra exempel på intressanta kvanttekniker som kan användas till sensorer är Rydbergatomer och atominterferometri. En Rydbergsensor kan detektera elektriska fält från statik upp till många GHz. En annan stor fördel med dem är att sensorn är mycket liten i förhållande till de antennstorlekar som används idag. Atominterferometrar kan mäta acceleration, vinkelaccelaretion och gravitation noggrant. Ovan nämnda sensorer har i många fall passerat de brusgränser som finns i deras klassiska motsvarigheter. Detta innebär att vi på kort sikt kan mäta signaturer med större noggrannhet och signaturer som idag ligger i brusnivån. Det betyder även att nya signaturer som gravitation kommer att kunna mätas med tillräcklig noggrannhet för att bli intressanta. I dagsläget är det främst underjordiska hålrum som kan hittas, men framgent finns möjlighet att detektera nedgrävda minor och större undervattensobjekt, med inhomogen massfördelning, såsom ubåtar.[65] På lång sikt kommer sensorerna att ha mångfalt bättre känslighet. I takt med allt bättre sensorer blir det följaktligen viktigare att känna till bakgrundsmiljön de mäter i. Även där snabbar förbättrade sensorer på kartläggningsarbetet. På medellång sikt är det möjligt att tänka sig kvantfysikaliskt sammanflätade sensorsystem, vilka med större precision kan detektera objekt i en flera nivåer högre brusbakgrund.

Inom kvantavbildning, som utnyttjar den elektromagnetiska strålningens kvantegenskaper, har det varit svårt att hitta praktiska tillämpningar som nyttjar egenskaper mer än vad som kan förklaras med semi-klassisk teori. Ett exempel är kvantradar, som var ett aktivt forskningsområde för några år sedan när de första experimentella försöken i mikrovågsområdet med sammanflätade pulser precis hade genomförts i

65 V. Ménoret et al.: “Gravity measurements below 10−9 g with a transportable absolute quantum gravimeter”, Nature Scientific Reports 8, 12300 (2018). doi: 10.1038/s41598-018-30608-1.

laboratoriemiljö.[66] Även om fysiken var intressant visade det sig ganska snabbt att det inte fanns någon praktisk militär nytta.[67]

Därutöver finns ett antal mättekniker som utnyttjar komponenter utvecklade inom kvantteknikområdet, såsom fotonräknande detektorer och källor för sammanflätade fotonpar. En etablerad teknik är fotonräknande lidar.[68] Lidar är ett system där laserstrålar pulsas ut och reflekterade strålar samlas in. Fotonräknande lidar utnyttjar detektorer som kan detektera enskilda fotoner, dvs. elektromagnetisk strålnings minsta beståndsdel. Med dessa känsliga sensorer kan svagare belysning (laserstråle) användas, vilket gör att dessa aktiva system är svårare att upptäcka än klassiska typer av lidarsystem. Fler typer av så kallade kvantinspirerade tekniker, dvs. tekniker som endast använder kvantkomponenter men som kan förklaras semi-klassiskt, finns redovisade i Militärteknik 2045.[69]

### Kvantkommunikation och kryptering

Idag görs stora ansträngningar för att utveckla kvantsäkra krypton. Krypton som utvecklas idag behöver framtidssäkras för att informationen som krypteras inte ska gå att dekryptera under den tidshorisont som informationen bedöms vara känslig. Försvarsmaktens bedömning är att de ligger väl till i detta arbete, merparten av krypton de använder idag bedöms även vara säkra för de generella kvantdatorer som är under utveckling. Bland företag och i andra delar av myndighetssfären finns det däremot större utmaningar då de i hög utsträckning använder äldre asymmetriska krypton som en kompetent kvantdator kommer kunna knäcka.

Idag satsas det stort på forskning inom kvantkommunikation där man kodar informationen i kvanttillstånd.[70,71] Forskningen sker både på universitet och i kommersiella företag. Den teknik som kommit längst är kvantnyckelöverföring.[72]

66 D. Luong et al. "Receiver Operating Characteristics for a Prototype Quantum Two-Mode Squeezing Radar," IEEE Transactions on Aerospace and Electronic Systems, pp. 1-1 (2019), doi: 10.1109/TAES.2019.2951213.

S. Barzanjeh et al. "Microwave quantum illumination using a digital receiver," Science Advances, 6(19), eabb0451 (2020). doi: 10.1126/sciadv.abb0451.

M. Höijer, T Hult, P. Jonsson, "Quantum Radar – A survey of the science, technology and literature," FOI-R--4854--SE (2019).

T Hult, P. Jonsson, M. Höijer "Quantum Radar – The follow-up story," FOI-R--5014--SE (2020).

67 J. H. Shapiro. "The Quantum Illumination Story". IEEE Aerospace and Electronic Systems Magazine 35(4), 8–20 (2020).

68 Light Detection and Ranging.

69 Kindvall, G. och Lindberg, A. (red.), Militärteknik 2045: Ett underlag till Försvarsmaktens perspektivstudie, FOI-R--4985--SE, 2020.

70 N. Gisin et. Al, "Quantum cryptography," Reviews of Modern Physics 74(1), 145–195 (2002), doi: 10.1103/RevModPhys.74.145.

71 Shenoy-Hejamadi et al. "Quantum Cryptography: Key Distribution and Beyond," Quanta 6, 1–47 (2017) doi: 10.12743/quanta.v6i1.57.

72 Vid kvantnyckelöverföring (eng. Quantum Key Distribution) överförs en slumpmässig nyckel mellan två parter.

I kvantnyckelöverföring överförs fotoner mellan två kommunikatörer. Endast kommunikatörerna kan tillgodogöra sig informationen, eftersom den alltid förstörs vid utläsandet. Följaktligen märks det direkt om en tredje part försöker avlyssna. Det medger att de kommunicerande parterna då kan avsluta eller ändra kommunikationen eller kommunikationssättet. Lokala nät som kan kommunicera en bit över 100 km har byggts eller håller på att byggas på flera ställen, t.ex. i EU och Kina. Kvantkommunikation via satellit har visats av Kina. På lång sikt kan ett allmänt tillgängligt kvantinternet finnas.

Kvantnyckelöverföring har föreslagits som en lösning för kvantdatorhotet mot asymmetriska krypton. Dock gör flertalet västländer, inklusive den svenska Försvarsmakten, bedömningen att kvantnyckelöverföring inte är lösningen för att kvantsäkra krypton.[73] På lång sikt finns däremot intressanta tillämpningar inom kvantkommunikation för Försvarsmakten där utspridda sensorer kan sammanflätas och kommunicera kvantmekaniskt. I dagsläget är bedömningen att det är tillräckligt att följa utvecklingen.

### Kvantdatorer och kvantberäkningar

Kvantdatorer bygger på förhoppningen att kunna nyttja den ofantliga parallellism som finns i stora kvantsystem. Idag forskas det på flera olika typer av kvantfysikaliska system, som supraledande kretsar, kvantprickar och joner i magnetooptiska fällor för att nämna några. De har alla sina styrkor och svagheter, men generellt gäller att de, för att kunna bidra till kvantdatorer, behöver vara lätta att skala till större system, med bra kontroll över både de individuella och de sammanflätade kvantbitarna. Därutöver måste dekoherens undvikas så länge som möjligt. Kvantsystemet behöver vara så isolerat som möjligt för att undvika informationstapp genom påverkan från yttre faktorer.

Ett viktigt men svårt steg är att implementera kvantfelrättning, dvs. kod som rättar till de fel som ofrånkomligen kommer att inträffa (eftersom systemet inte kommer att vara helt isolerat). Dagens största kvantdatorer består av flera hundra kvantbitar. Dessa är inte felkorrigerande, vilket gör att de initialt bara kan användas i tillämpningar som är mindre känsliga för beräkningsfel. Det nuvarande forskningsfokuset ligger därför främst på felreduktion, felhantering och antalet tillgängliga grindar. Idag går det att bygga kvantdatorer med nästan lika många felkorrigerade kvantbitar som kan simuleras på en vanlig dator. Vissa beräkningar, som inte kan replikeras på en klassisk dator och som inte kräver universell felkorrigering, kan redan idag utföras på en kvantdator. Vad vi känner till finns det dock idag inget exempel på ett faktiskt problem som en kvantdator löst som inte en klassisk dator kan lösa.

73 French Cybersecurity Agency (ANSSI), Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), Swedish National Communications Security Authority, Swedish Armed Forces "Position Paper on Quantum Key Distribution," https://www.forsvarsmakten.se/contentassets/f7199ed1b90f41529b76970bdb5fce1c/position-paper-on-quantum-key-distribution.pdf, 2024.

Detta förväntas dock ske vilken dag som helst. När man pratar om fungerande kvantdatorer, menas egentligen sådana som kan utföra generella kvantberäkningar som inte en klassisk dator kan utföra under rimlig beräkningstid.

Vidare skiljs det på om kvantdatorn använder generella kvantbitar eller inte. De senare kallas ibland kvantsimulatorer och de kan bara simulera ett eller ett fåtal specifika problem medan en komplett kvantdator är betydligt mer generell. Användbara kvantsimulatorer kommer troligen att finnas i närtid, medan experternas uppskattning för generella kvantdatorer som kan lösa olika problemtyper ligger 5–20 år framåt i tiden. Författarnas uppfattning är att den senare tiden – dvs. närmare 20 år – är det mer troliga.

## Samverkande och förutsättande teknikområden

Det finns några grundläggande och förutsättande teknikområden för de flesta kvantteknikerna. Nanoteknik, dvs. att skapa komponenter med strukturer ner mot atomnivå, används i många kvanttekniker. Dessa nanokomponenter tillverkas ofta med halvledarteknik. Även materialteknik är viktigt eftersom speciella material används inom många tillämpningar av kvantteknik. För att göra system av grundkomponenterna behövs flera olika tekniker för att bevara, manipulera, kontrollera och läsa ut information från kvantteknikerna. Detta inkluderar bland annat kryoteknik och vakuumteknik för att isolera komponenterna från omgivningen, laserteknik, optik och elektronik för att manipulera, kontrollera och för utläsning. I en rapport inom *NATO Transatlantic Quantum Community* (TQC) har en analys gjorts om leveranskedjan för kritiska komponenter för kvantdatorer.[74] Där listas en stor del av de nyckeltekniker och material som krävs för olika typer av kvantdatorer. Detta ger en bra bild av behovet även inom de andra kvantteknikerna (sensorer och kommunikation) då grundteknikerna ofta är gemensamma.

En viktig förutsättning för kvanttekniker och eventuella framtida genombrott är grundforskningen som sker inom den akademiska världen. Då kvantfysik oftast inte är intuitiv, krävs en djup förståelse och flera års erfarenhet för att kunna utveckla befintliga kvanttekniker och tillämpningar samt att kunna komma på nya. Dagen då tekniken börjar bemästras för militära tillämpningar kommer utvecklingen mest troligt att ske utan att information om den delges, liksom inom många andra militärt relevanta teknikområden. Det finns tecken som tyder på att vi kan vara där idag för vissa av teknikerna, exempelvis kvantsensorer inom tröghetsnavigering. Därför kan det i närtid behövas kunskap och verksamhet inom försvarssektorn för att bättre kunna bedöma kommande hot och möjligheter.

74 L. Kingma, F. Heijman, C. Williams, "Critical Vulnerabilities in the Quantum Computing Supply Chain within the NATO Alliance," Nato, 2025.

## Påverkan på militär förmåga

Kvanttekniker innebär både möjligheter och hot och kan påverka förutsättningarna för att skapa och utveckla förmåga. Tidpunkten för när olika tillämpningar av kvantteknik är tillräckligt mogna för användning är svår att förutse, men för framtida förmågeutveckling, materielanskaffning och planering behöver möjligheterna och riskerna beaktas.

Kompetens är en förutsättning för att kunna hantera den kommande teknikutvecklingen. Forskning och utveckling av kvantteknik och dess tillämpningar är än så länge relativt tillgängliga och publiceras normalt öppet. När tekniken börjar bemästras och där militära tillämpningar finns kommer kunskapen enligt ovan troligen inte göras allmänt tillgänglig längre. Nationell kompetens och verksamhet inom kvantområdet kan därför behövas.

En användare av system som nyttjar kvantteknik kommer normalt inte behöva kunna kvantfysik, men en bra allmän teknisk skolning är viktig och kommer bli allt viktigare med tiden. Detta gäller naturligtvis inte bara kvanttekniker utan även andra teknikområden. Den alltmer avancerade tekniken kommer kunna ge kompetenta användare stora fördelar.

### Kryptering och konsekvens för dagens informationshantering

En viktig förändring som kvanttekniken kan medföra är att dagens kryptering blir otillräcklig. Om en tillräckligt kraftfull kvantdator kan byggas kommer dagens kryptering som bygger på publika asymmetriska nycklar att kunna knäckas. Även om det antagligen är ett eller några årtionden kvar tills en sådan kvantdator finns kan det redan idag finnas information som behöver hållas hemlig med kryptering en lång tid framöver. En motståndare skulle kunna spara krypterade meddelanden idag och dekryptera dem när kvantdatorn kommer. Därför menar Försvarsmakten att vi redan idag behöver använda kvantdatorsäkra krypteringsmetoder.[75] Sådana metoder finns tillgängliga men kräver en mer komplicerad nyckelhantering och säker överföring av hemliga nycklar mellan kommunicerande parter. De grundläggande förmågorna ledning och underrättelse påverkas därför stort av utvecklingen.

Civilt förlitar man sig ofta på publika nycklar eftersom hanteringen av dessa nycklar är så mycket enklare. Dessa metoder anses säkra för en konventionell dator, men en kvantdator kan enligt ovan snabbt knäcka denna typ av kryptering. För att samhället i stort inte ska skadas behövs nya metoder för kryptering som inte kan knäckas av en framtida kvantdator.

75 M. Ekerå, Swedish NCSA, Swedish Armed Forces, "The quantum threat to cryptography, our mitigation strategy, and our stance on quantum key distribution", keynote at the NATO IST-SET-198 Symposium, Amsterdam, the Netherlands, October 3–4, 2023.

En viktig aktör för att ta fram nya krypteringsmetoder – så kallad kvantsäker kryptering eller postkvantkryptering – är NIST (*National Institute of Standards and Technology*) i USA, som har föreslagit en lösning som studeras för tillfället.

### Positionering, navigering och tid (PNT)

Inom området positionering, navigering och tid (PNT) finns flera möjligheter att utnyttja kvantteknik för att minska beroendet av GNSS. I närtid möjliggör ny kvantteknik noggrannare tröghetsnavigering[76,77] som bör kunna få plats i ett 1–2 m³ stort utrymme. Bättre atomklockor och atominterferometri för noggrannare bestämning av acceleration och vinkelacceleration förutses kunna öka noggrannheten med en faktor 10–100. Dessa noggrannare system kan följaktligen användas under en längre tid i en GNSS-fri miljö än nu existerande tröghetsnavigeringssystem. Tekniska utmaningar verkar vara minskad noggrannhet vid större kursändringar och viss uppstartstid för de fångade atomerna. Båda problemen kan initialt avhjälpas med parallellkörning med ett traditionellt tröghetsnavigeringssystem. Initialt är tekniken lämpad för större och relativt långsamma farkoster, såsom fartyg och ubåtar. I takt med att tekniken blir mindre och billigare kommer andra typer av plattformar bli aktuella.

En annan navigeringsteknik som kan användas om GNSS inte är tillgängligt är fixpunktsnavigering. Idag utförs passiva test av denna navigeringsteknik exempelvis med hjälp av magnet- och/eller gravitationsanomalikartor. Kvaliteten på kartunderlagen, hur noggranna de är, samt den geografiska täckningen är viktiga. Här finns även stora mättekniska utmaningar som måste övervinnas. Signalerna som behöver subtraheras bort är jordens fält, plattformens signatur, miljöbrus samt plattformens acceleration. Ovanstående gör att det är oklart vilken sensorprestanda som behövs och utvecklingstiden tills den kan finnas. Eventuellt skulle dagens magnetometrar kunna vara tillräckligt bra. Fördelar jämfört med dagens tekniker för ytavskanning är att ovanstående tekniker är passiva samt att det kan finnas detekterbar struktur under platta ytor. En kombination av förbättrad tröghetsnavigering och fixpunktsnavigering ger en betydande förbättring av egenpositionering och navigering i GNSS-fri miljö.

På lång sikt, 2050, förutspås att navigeringssystemen kan göras så små och billiga att de kan användas brett på exempelvis stridsflygplan, stridsfordon, mindre båtar, robotar och drönare. Det är inte otänkbart att de så småningom blir bärbara och kan användas av enskilda soldater.

En lokal noggrann tidsreferens öppnar även nya möjligheter att operera med system som kräver noggrann tid även i GNSS-störd miljö. Kvanttekniken skulle därför kunna användas för att minska beroendet av GNSS när det gäller positionering,

76 E. Amselem et al., "Atom interferometry for high precision navigation", FOI-R--4015--SE (2014).

77 P. Cheiney et al., "Navigation-Compatible Hybrid Quantum Accelerometer Using a Kalman Filter", Phys. Rev. App. 10, 034030 (2018).

navigering och som tidsreferens och denna utveckling har redan börjat. Detta ger effekter för den grundläggande förmågan rörlighet.

### Kvantdatorn för specifika problem och optimeringsproblem

En kvantdator har en mängd tillämpningar, men kommer på inga sätt att ersätta ”vanliga” datorer.[78] Kvantdatorer kommer att användas till en begränsad typ av problem. Att kunna avkryptera meddelanden används ofta populärvetenskapligt för att motivera framtagandet av en kvantdator, men utvecklandet av kvantsäkra krypton ger som konsekvens att just användningen av kvantdatorer för att avkryptera meddelanden minskar i betydelse. Framtagna kvantalgoritmer som däremot förväntas få stor påverkan inom försvarssektorn finns exempelvis inom optimering och kvantberäkningar.

Svåra optimeringsproblem, exempelvis kombinatoriska sådana, bedöms vara den problemtyp som kommer ge kvantdatorn dess stora genombrott. Militära användningsexempel inkluderar ruttoptimering, resursallokering och logistikkedjor. En kvantdator förväntas kunna lösa dessa problem bättre än vad som är möjligt idag redan inom några år och signifikant bättre om 10–20 år.

På sikt, minst 10 år, bedöms kvantdatorns viktigaste användningsområde att bli kvantfysikaliska och kvantkemiska beräkningar, dvs. att kunna simulera material och molekyler bättre. Detta kommer att innebära snabba framsteg inom en mängd områden och förmodas ge bättre mediciner, effektivare elektronik och sprängmedel, samt tåligare material för att bara nämna några exempel. Kvantdatorn kommer påverka både Försvarsmaktens grundläggande förmågor och förutsättningar för att producera förmågor.

### Sensorer och signaturer

Sensorer baserade på kvantteknik med högre känslighet än klassiska sensorer kan ge nya möjligheter att detektera elektromagnetiska vågor i telekrigstillämpningar, magnetiska fält för t.ex. ubåtsdetektion samt lokala gravitationsvariationer för till exempel tunneldetektion. På längre sikt kommer det att bli möjligt att koppla ihop sensorer kvantmekaniskt vilket gör att noggrannheten ökar med en faktor N, där N är antalet sensorer, istället för kvadratroten ur N som är det den klassiska fysiken medger. Aktivt avbildande system som radar, lidar och sonar kan med kvantteknik använda så låga uteffekter att de blir svåra att upptäcka. De kan även få ökad känslighet som gör att farkoster som idag anses vara smyganpassade (*stealth*) blir möjliga att detektera. De grundläggande förmågorna skydd och verkan påverkas därför genom att känsligare kvantmättekniker gör det möjligt att detektera signaturer från objekt som idag betraktas som svåra eller omöjliga att upptäcka, till exempel stealthflygplan och ubåtar. Även ledning och underrättelse påverkas genom att

78 O. Ezratty, Understanding Quantum Technologies (2024).

kvantteknik kan göra aktiva system (radar, kommunikation etc.) ännu svårare att upptäcka, avlyssna och störa.

### Kommunikation

Inom kommunikation kan kvantteknik användas för säker nyckelöverföring men även för att upptäcka avlyssning. Det går också att utnyttja kvantfysiken för att gömma den utsända signalen i bakgrundsbruset. Stora framsteg har de senaste åren skett inom kvantkommunikation. Det finns fungerande optiska fibersystem och kvantkommunikation med och mellan satelliter har testats. Kvantkommunikation i luft eller vatten med sammanflätade tillstånd är dock störningskänslig, både naturligt och från en aktiv motståndare. Även om en motståndare inte aktivt kan avlyssna, kan en kompetent motståndare sannolikt störa ut kommunikationen så att ingen får informationen, vilket kan vara nästan lika allvarligt för vissa tillämpningar. Tidskritisk kommunikation som stridsledning bör därför inte initialt förlita sig på kvantkommunikation.

### Taktik och materiel

Ett exempel på hur taktik och materiel kan påverkas är effekten av kvantgravitometrar. Kvantgravitometrar ger en ny möjlighet att upptäcka till exempel tunnlar, nedgrävda föremål och ubåtar. För att minska risken för upptäckt av de egna ubåtarna eller andra undervattensfarkoster kan man arbeta med signaturbegränsande åtgärder, till exempel eftersträva en så jämn massfördelning som möjligt. Taktiskt och uppförandemässigt kan man gömma sig där bakgrunden är extra besvärlig för upptäckt. Detta kräver dock god information om, och en god kartläggning av, den lokala gravitationen.

### Begränsande faktorer

Den största begränsande faktorn för kvanttekniker är att kvanttillstånden man försöker nyttja är känsliga för omgivningen. Kvantsystem fungerar (bäst) som avgränsade system. För att kunna föra in och plocka ut information krävs dock interaktion med systemet vilket introducerar störningar. En konsekvens av denna nödvändiga interaktion, och typ av störning, är dekoherens av kvanttillstånden, till exempel minskande grad av sammanflätning, vilket försämrar prestandan. För sammanflätade fotoner leder transmission genom atmosfären till dekoherens. I en kvantdator behöver vissa komponenter kylas ner till strax över den absoluta nollpunkten för att fungera. För att kunna läsa av resultatet från komponenterna behöver man dock koppla ut systemet till rumstempereratur, vilket också introducerar dekoherens. För atominterferometrar är ofta vibrationer ett problem som degraderar prestandan. Även om man börjar kunna bemästra åtminstone delar av dekoherensproblemen i laboratoriemiljöer är det ett stort steg att få tekniken att fungera i en operativ miljö.

En viktig slutsats från *von Kármán Horizon Scanning*-studien[79] är att länder behöver samverka för att få kvanttekniken att fungera i den militära kontexten och miljön. Militära systemaspekter måste beaktas vid design av utrustningen. Detta är något som ofta negligeras i forskningen vid universitet och högskolor.

## Aktörer

I rapporten Militärteknik 2045[80] uppskattades olika aktörers monetära satsningar till cirka 1,5 miljarder euro år 2015.[81] Numera gör Qureca regelbundna uppskattningar av kvanttekniksatsningar globalt. 2025 uppskattar de satsningarna till 55,7 miljarder USD, se figur 3. Vi bedömer att deras uppskattning är en underskattning då de privata teknikjättarnas kvantdatorsatsningar inte tycks ingå i beräkningarna. Det betyder att satsningarna har ökat mer än 30 gånger under de senaste 10 åren.

Det land som satsar mest enligt Qurecas sammanställning är Kina med 15,3 miljarder USD vilket nästan är en hundrafaldig ökning jämfört med uppskattningen 2015. USA är det land som satsar näst mest med 7,7 miljarder USD. Notera dock att de privata kvantdatorsatsningarna inte tycks ingå i uppskattningen, så förmodligen satsar de totalt minst lika mycket som Kina. Trea på listan är Storbritannien med 4,7 miljarder USD. Totalt satsar EU och dess medlemsländer cirka 10,4 miljarder USD. Ryssland som nästan saknades i sammanställningen 2015 har initierat flera kvanttekniksatsningar om totalt 1,8 miljarder USD.

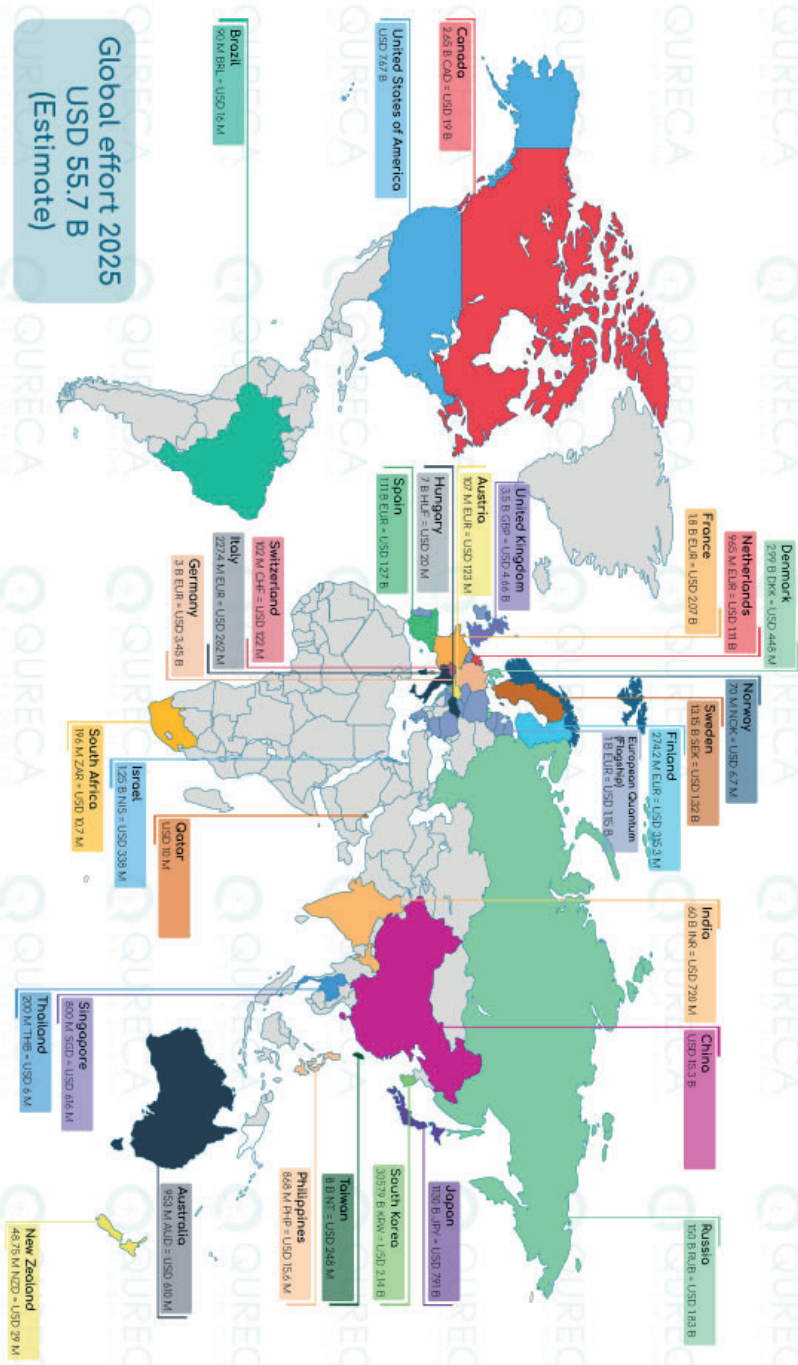
Den största delen av forskningen inom området kvanttekniker bedrivs vid universitet, men en allt större del sker i samverkan med andra aktörer, främst civila företag. Den främsta utvecklingen inom kvantdatorer sker i USA, främst genom stora satsningar från civila informations- och datorföretag som Microsoft, IBM, Google, Intel med flera. Även många nya företag har startats inom området.

Vad gäller militärt styrd forskning är USA störst, tätt följt av Kina. Dessa två är tillräckligt stora för att kunna satsa på alla kvanttekniker de tror kan vara relevanta. I USA finns flera program från DARPA och försvarsdepartementet (DoD) inom området. Även Nato, som har utpekat kvanttekniker som en viktig framväxande och omvälvande teknik, har satsningar. Under 2024 startade *NATO Transatlantic Quantum Community* (TQC) för att stärka och samordna alliansens satsningar inom området. Även *NATO Science and Technology Organization* (STO) har startat ett antal forskningsgrupper inom kvantteknikområdet.

79 "von Kármán Horizon Scanning on Quantum Capabilities for Sensing and Communications – Summary Report", Nato, 2018.

80 Kindvall, G. och Lindberg, A. (red), Militärteknik 2045: Ett underlag till Försvarsmaktens perspektivstudie, FOI-R--4985--SE, 2020.

81 "Technology quarterly–Quantum devices", The Economist, March 11th 2017, pp. 3-12.




**Figur 3** Qureca sammanställer kontinuerligt satsningar inom kvanttekniker globalt i världen. (https://www.qureca.com/quantum-initiatives-worldwide/ (besökt 2025-09-03)).

Kina har satsat stort inom kvantkommunikation och kvantnyckelöverföring. De har fungerande optiska fibersystem och har testat kvantkommunikation med satellit.[82] Kina verkar ligga i framkant inom detta. Till del kan det förklaras av att västvärldens säkerhetstjänster har nedvärderat nyttan av kvantnyckelöverföring.[83] USA och Europa tycks snarare satsa sin forskning på framtidens kvantinternet med fler tillämpningar än bara nyckelöverföring. Kina satsar även stort inom andra kvantområden,[84,85] och det kommer med jämna mellanrum uppgifter om stora framsteg t.ex. inom mätning och sensorer[86,87] men de bedöms som relativt överdrivna.[88] Vår bedömning är att Kina fortfarande ligger efter västvärlden men med tanke på satsningarnas storlek är det inte otänkbart att de snart kan vara ikapp eller rent av förbi.

Ryssland har de senaste åren presenterat flera kvanttekniksatsningar. Dessa satsningar inkluderar aktiviteter inom datorer, beräkningar, kommunikation samt sensorer och mätteknik.[89] Tidigare saknades större kvanttekniksatsningar i Ryssland, åtminstone i öppna källor. FOI:s bedömning är att Ryssland fortsatt kommer ligga efter USA, Kina och Europa de närmaste åren inom de flesta kvanttekniker.

Inom Europa sker stora satsningar och många länder har eller håller på att skaffa kvantstrategier. Dessa är främst fokuserade på forskning och innovation civilt, men satsningarna kommer även få konsekvenser på den militära arenan. Ett exempel är NATO TQC där man bland annat försöker hitta företag med teknik med dubbla användningsområden för att anpassa tekniken för Natos behov.

Den främsta satsningen i Sverige sker vid akademiska institut med finansiella medel från en Wallenbergstiftelse. Tyngdpunkten för satsningen, som är på en miljard SEK för 2018–2030, ligger i Göteborg och går under namnet *Wallenberg Centre*

82 Y.-A. Chen et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," Nature, 589, 214-219, 2012. doi: 10.1038/s41586-020-03093-8.

83 French Cybersecurity Agency (ANSSI), Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), Swedish National Communications Security Authority, Swedish Armed Forces "Position Paper on Quantum Key Distribution," https://www.forsvarsmakten.se/contentassets/f7199ed1b90f41529b76970bdb5fce1c/position-paper-on-quantum-key-distribution.pdf, 2024.

84 E. Kania and J. Costello, "Quantum Leap (Part 1): China's Advances in Quantum Information Science," China Brief, 16(18), 11-16, 2016. E. Kania and J. Costello, "Quantum Leap (Part 2): The Strategic Implications of Quantum Technologies for the PLA," China Brief, 16(19), 22-27, 2016. E. B. Kania and S. Armitage, "Disruption Under the Radar: Chinese Advances in Quantum Sensing," China Brief, 17(11), 15-21, 2017.

85 Q. Zhang et al., "Quantum information research in China" Quantum Sci. Technol. 4 040503, 2019.

86 D. Hambling, "China's quantum submarine detector could seal South China Sea," New Scientist 2017-08-22, https://www.newscientist.com/article/2144721-chinas-quantum-submarine-detector-could-seal-south-china-sea/.

87 M. Giles, "The US and China are in a quantum arms race that will transform warfare", MIT Technology Review 3 January 2019. Se: https://www.technologyreview.com/s/612421/us-china-quantum-arms-race/.

88 J. Haystead, "Quantum Radar Sees the Light," The Journal of Electronic Defense, 2019, July pp. 23-31.

89 A. K. Fedorov et al., "Quantum technologies in Russia," Quantum Sci. Technol. 4, 040501, 2019.

*for Quantum Technology* (WACQT). Utöver det bidrar bland annat ABB, Astra Zeneca, Ericsson, Jeppesen, SAAB, SEB och Volvo med medel och kompetens. Huvudsatsningen sker på kvantdatorer, men det ingår även en satsning på vissa kvantsensorer och kvantkommunikation med forskare från flera större universitet och högskolor i Sverige. Utöver detta är Sverige också representerat i EU:s flaggskeppssatsning på kvantdatorer på totalt 1 miljard euro.

Kvanttekniker är ett stort område, som drar nytta av grundläggande forskningsframsteg från universitet över hela världen, vilket gör det svårt att förutse när genombrotten kommer att ske. Det förekommer ibland också en stor hajp inom kvanttekniker, där man lovar mer än tekniken tillåter. Ett exempel är kvantradar som först utlovade stora möjligheter, men som sedan visade sig inte fungera för praktiska tillämningar.

För en liten aktör som Sverige är det omöjligt att satsa på allt. En noggrann övervägning behövs av vilka kvanttekniker det skall satsas på och framförallt när. Vad gäller kvantdatorns utveckling ses ingen anledning till att försvarsmyndigheterna engagerar sig i dagsläget. Det finns ingen möjlighet att konkurrera med de stora företagen och allt tyder på att kommersiella produkter kommer att finnas tillgängliga. Dessa kommer troligen relativt enkelt kunna anpassas för försvarets behov. Däremot bör Försvarsmakten undersöka hur kvantberäkningar (algoritmer och simuleringar) kan användas inom försvar och säkerhet och bygga upp kompetens inom dessa områden.

För andra kvanttekniker, som kvantkommunikation och flertalet kvantsensorer, finns det också stora civila behov som antagligen kommer att driva utvecklingen, men då tillämpningarna ibland skiljer sig en del åt är det viktigt att aktivt delta på den nivå som behövs för att tekniken ska kunna anpassas för försvarets behov.

För kvanttillämpningar inom PNT, t.ex. tröghetsnavigering och vissa typer av detektion, bedöms de civila behoven idag vara betydligt mindre än de militära behoven. Detta innebär troligen att utvecklingen åtminstone till en början kommer att behöva drivas av militära aktörer. Vill Försvarsmakten dra nytta av den teknik som håller på att växa fram behöver de troligen själva investera i forskning och utveckling i samarbete med lämpliga aktörer.

## Lästips

Teknisk prognos Rapport Nr 1 2023, Tema Kvant, FMV dokumentbeteckning: 22FMV1402-25, https://www.fmv.se/globalassets/dokument/om-fmv/teknisk-prognos-nr-1_20232.pdf.

https://www.chalmers.se/centrum/wacqt/upptack-kvantteknologi/.

S. Charpentier (red.) Framtida utveckling inom Kvantteknologi, 2022-11-24.

J. Kjäll, P. Jonsson, Kvantteknologier-2019, FOI Memo 7034, 2020.

von Kármán Horizon Scanning on Quantum Capabilities for Sensing and Communications – Summary Report, Nato, 2018.

K. Bongs, S. Bennett, A. Lohmann, Quantum sensors will start a revolution – if we deploy them right, Nature, 617, 672–675, (2023). doi: 10.1038/d41586-023-01663-0.

Kindvall, G. och Lindberg, A. (red), Militärteknik 2045: Ett underlag till Försvarsmaktens perspektivstudie, FOI-R--4985--SE, 2020.

N. Gisin et. Al, Quantum cryptography, Reviews of Modern Physics 74(1), 145–195 (2002), doi: 10.1103/RevModPhys.74.145.

Shenoy-Hejamadi et al. Quantum Cryptography: Key Distribution and Beyond, Quanta 6, 1–47 (2017) doi: 10.12743/quanta.v6i1.57.

French Cybersecurity Agency (ANSSI), Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), Swedish National Communications Security Authority, Swedish Armed Forces Position Paper on Quantum Key Distribution, https://www.forsvarsmakten.se/contentassets/f7199ed1b90f41529b76970bdb5fce1c/position-paper-on-quantum-key-distribution.pdf, 2024.

E. Amselem et al., Atom interferometry for high precision navigation, FOI-R--4015--SE (2014).

P. Cheiney et al., Navigation-Compatible Hybrid Quantum Accelerometer Using a Kalman Filter, Phys. Rev. App. 10, 034030 (2018).

O. Ezratty, Understanding Quantum Technologies (2024).

Y.-A. Chen et al., An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature, 589, 214-219, 2012. doi: 10.1038/s41586-020-03093-8.

Q. Zhang et al., Quantum information research in China Quantum Sci. Technol. 4 040503, 2019.

A. K. Fedorov et al., Quantum technologies in Russia, Quantum Sci. Technol. 4, 040501, 2019.

# Bioteknik

*Petrus Hemström och Anna Lindberg*

## Inledande beskrivning

Bioteknik, i samspel med andra teknologiområden, spås av många revolutionera den globala utvecklingen mot 2050. Hur och vad som kan komma att förändras är dock svårare att förutspå. Detta kapitel är skrivet utifrån antagandet att ett paradigmskifte inom biotekniken har skett och att detta fått ett reellt genomslag till 2050. Steve Jobs, som var med och lade grunden till AI och digitaliseringen av samhället har uttalat sig om bioteknik: *"I think the biggest innovations of the 21st Century will be at the intersection of biology and technology – A new era is beginning"*.

Blir revolutionen att flytta kemiindustrin från dyra katalysatorer och energi till designade enzymer och biomassa? Eller blir det bioprintade cybernetiska tillbehör på soldater med hjärn-dator-koppling (eng. *brain computer interface*) i symbios med bioelektroniska drönarsvärmar?

I en rapport från USA:s nationella säkerhetskommitté för framväxande bioteknik (eng. *National Security commission on emerging biotechnology*) beskrivs en framtid där soldater får mat, energi, utrustning, skydd och sjukvård vid fronten tack vare bioteknik.

Men vad är bioteknik? Enligt IUPAC[90] definition är det fritt översatt att "Med hjälp av naturvetenskap och ingenjörskonst använda organismer, delar av organismer eller biologiskt härledda molekyler för produkter eller tjänster".

Bioteknik handlar om att använda, modifiera och utveckla biologiska och biokemiska system. Tillämpningar finns inom diverse områden och omfattningen är så stor att begreppet bioekonomi (eng. *bioeconomy*) används på global nivå för att beskriva bioteknikens ekonomiska inverkan och potential. Läkemedel och medicin, drivmedel och energi, industriprodukter och syntetiska material, livsmedel, jord- och vattenbruk, modifierade växter och djur samt materialdesign är exempel på tillämpningsområden. Selektion och avel har funnits genom historien, men modern bioteknik ger möjlighet till produkter och tjänster som var omöjliga för bara tjugo år sedan. Bioteknik kan ge helt nya biologiska system, tjänster och kemiska komponenter samt sådana som inte finns naturligt. Detta beskrivs ofta som syntetisk biologi.

Grunden i bioteknik är kunskap om livets byggstenar och hur dessa samverkar. Denna förståelse kan utnyttjas i en rad vitt skilda applikationsområden. Många bioteknikområden framstår idag som science fiction. Men, kunskap om proteinreaktioner och -interaktioner, cellvidhäftning, förståelse för neuroners och hjärnans

90 International Union of Pure and Applied Chemistry.

funktion, kan i förlängningen leda till allt från specifika biosensorer till direkt dator-hjärna-koppling eller kanske i slutändan cyborger med sömlöst kopplade biologiska och elektromekaniska delar.

Ett annat centralt begrepp är teknisk biologi (eng. *bioengineering*), där den biologiska och biotekniska utvecklingen bedrivs med ett ingenjörsmässigt tillvägagångssätt. Detta utgör grunden för den revolution inom bioteknik som förutspås och förklaras enklast genom att teknikutvecklingen ger möjlighet till ny försöksdesign där man följer en *design-build-test-learn*-loop (DBTL). Designsteget utnyttjar de stora informationsmängder som byggts upp under årtionden av grundforskning i kombination med nya AI-verktyg, till exempel det Nobelprisbelönade AlphaFold. Det andra steget, build, bygger på sekvensering, editering och syntes av DNA och har dragit nytta av den enorma utvecklingen som skett inom dessa områden. Så kallade *biofoundries* är faciliteter där hela DBTL-cykeln automatiseras, vilket markant förbättrar möjligheterna att accelerera såväl DBTL som det traditionellt försöksbaserade arbetet där de första stegen genomförs i våtlabb och i djur. DBTL ger enorma mervärden och kommer öppna dörren för såväl avsevärt förbättrade befintliga som helt nya och innovativa lösningar. Att det är ett samspel visas genom att förståelse för hur den mänskliga hjärnans neurala nätverk fungerar möjliggjort de senaste tekniksprången inom artificiell intelligens som GPT-4 eller Google DeepMind som i sin tur är hörnstenar i utvecklingen av den nya biotekniken.

Bioteknikområdet innefattar en rad etiska knäckfrågor och dilemman. Detta gäller inte enbart synsätt om hur biologiska system kan och bör förändras och ekologiska risker, utan även tillgänglighet till teknikerna och produkterna.

## Trender och exempel

Bioteknik bedöms på sikt komma att påverka majoriteten av aspekterna av militär konflikt och försvarsförmåga, men det kommer med några undantag att vara en indirekt påverkan. Med det avses att majoriteten av produkter och tillämpningar hittas inom civil forskning och utveckling, eller att civila produkter används som underlag in mot andra materiel-, förmåge- och systemlösningar. Det finns också områden som är av rent försvarsmässig forsknings- och tillämpningskaraktär, där flertalet omfattas av reglering eller större etiska dilemman.

### Strategiskt område och kunskapsrace

Biotekniken lyfts fram som ett nyckelområde av samtliga tunga aktörer i den globala teknikkapprustningen; USA, Kina och EU. Det rör sig i första hand om ekonomiska drivkrafter (bioekonomi), men även strategiska drivkrafter påtalas som att minska beroenden i värdekedjor. Massiva satsningar har länge pågått i Kina med målsättning att bli en världsledande aktör inom området. Den amerikanska kongressens nationella säkerhetskommitté för framväxande bioteknik förespråkar

anslag till biotekniksatsningar, både infrastruktur och forskning, på 15 miljarder USD över de kommande fem åren.[91] Även EU fokuserar på bioteknik, det är ett av tre investeringsområden i *The Strategic Technologies for Europe Platform* (STEP)[92].

Dessa satsningar förväntas leverera tekniska genombrott inom ett antal områden. Ofta fokuseras på medicinska områden, men sammantaget kommer förutsättningarna och maktförhållandena kunna ändras i grunden av andra framsteg. Ett sådant är om bioproduktion gör att behov av t.ex. kritiska råvaror (olja och mineraler) drastiskt minskar.

Biotekniken är en av huvudbärarna i den generella teknologikonvergensen som enligt World Economic Forums analys för oss allt närmare en femte industriell revolution.[93] Man ser att framsteg inom stora teknikdomäner som AI, kvantberäkningar, bioteknik, AR och VR, robotik, avancerade material och nästa generations energilösningar konvergerar med stora teknologihopp som följd.

Bioteknik är en strategiskt viktig teknik för Sverige, vilket konstateras i Vinnovas rapport ”Strategiska tekniker för Sverige”.[94] Rapporten skrevs som ett kunskapsunderlag för regeringens strategiska inriktning av framtida insatser för att gynna:

- Svensk ekonomi och konkurrenskraft
- Nationell säkerhet och försörjningstrygghet
- Miljömässig och hållbar omställning

Utmaningarna är stora i den snabbt eskalerande tekniska och industriella kapprustningen. I det nya geopolitiska läget är det tydligt att biologiska data är en strategisk resurs som måste omhändertas och nyttjas, men även skyddas från konkurrenter.

### Ökat militärt engagemang

När Natos avgående chefsforskare Bryan Wells i sitt avskedstal ska peka på områden som kommer att revolutionera framtida militär förmåga är svaret bioteknik.[95] Ingen kan dock förutspå vad den revolutionen kommer att innehålla eller hur den kommer att påverka oss. Osäkerheten sammanfattas bra av Drew Endy, professor i syntetisk biologi vid Stanford som, vid en amerikansk kongressutfrågning om strategiska prioriteringar inom biotekniken,[96] sa att biotekniken är där datavetenskapen var 1975. Då, 1975, fanns det ingen möjlighet att förutse att handel i framtiden

91 https://www.biotech.senate.gov/final-report/chapters/.

92 https://strategic-technologies.europa.eu/index_en.

93 https://www.weforum.org/stories/2025/01/technology-convergence-is-leading-the-way-for-accelerated-innovation-in-emerging-technology-areas/.

94 Strander et al., 2024.

95 https://www.youtube.com/watch?v=X2cHF22utqU.

96 https://democrats-science.house.gov/hearings/pursuing-the-golden-age-of-innovation-strategic-priorities-in-biotechnology.

skulle ske på internet, att det skulle vara möjligt att försörja sig som influencer eller andra konsekvenser av digitaliseringen. På samma sätt är det idag omöjligt att förutse hur biotekniken kan ha förändrat världen 2075. Att biotekniken kommer att ha en enorm påverkan på vårt samhälle och därmed även på vår framtida försvarsförmåga verkar dock alla överens om. Den amerikanska kongressens nationella säkerhetskommitté för framväxande bioteknik[97] slog till exempel fast att de ser en framtid där "*Warfighters are fed, fueled, equipped, protected and healed on the battlefield by biotechnology*", dvs. att soldater får mat, energi, utrustning, skydd och sjukvård vid fronten tack vare bioteknik.

Bioteknikens påverkan på militär verksamhet är långt ifrån ny. Under första världskriget användes bioteknik för att producera en kritisk råvara som gav möjlighet till större produktion av granater. 1916 behövdes enorma mängder aceton för att producera drivladdningen (kordit) till artillerigranater. I Storbritannien löstes bristen genom att jäsa stärkelse till aceton med en bakterie, *clostridium acetobutylicum*, som isolerades och odlades för ändamålet.[98]

Redan idag påverkar biotekniken vår försvarsförmåga då många läkemedel och råvaror redan tillverkas genom biotillverkning. I takt med att mängden användbara biologiska flöden i celler (eng. *pathways*) ökar kommer en växande andel av (försvars)industrins insatsvaror att tillverkas i bioreaktorer. NATO STO har skapat ett tidsbegränsat forskningsprojekt HFM-391 (så kallad *Research Task Group* i panelen *Human Factors and Medicine*) för biotillverkning av material av vikt för nationell säkerhet, dock utan svenskt deltagande.

### Lösning på globala utmaningar och problem

Världen står inför omfattande utmaningar mot 2050. Det gäller bland annat att uppnå en hållbarare och grönare ekonomi, att råda bot på brist på råvaror och livsmedel, energitillgång och att främja hälsa, åldrande och välmående. Men även att möjliggöra längre rymdresor eller att leva på ogästvänliga platser genom att modifiera miljön eller organismer så att de kan leva i dessa miljöer. Biotekniken målas ofta upp som lösningen på dessa globala utmaningar. Behoven, och nya tekniska möjligheter, driver gemensamt bioekonomin. Forskning och framsteg inom bioteknikområdet har under en längre tid gått mycket fort framåt. Den utvecklingen verkar inte avta utan snarare accelerera genom interaktion mellan olika teknikområden och mängden tillgänglig biodata.

Det är långt ifrån säkert att tillgången till resultat och möjligheterna med bioteknik och teknisk biologi blir allmänt tillgängliga. Etik- och rättvisefrågor är en inneboende del av teknikområdet. Ofta lyfts medicin, genetisk behandling och förbättring

97 https://www.biotech.senate.gov/press-releases/interim-report/.

98 Bunch, A. W. (2014). How Biotechnology Helped Maintain the Supply of Acetone for the Manufacture of Cordite During World War I. International Journal for the History of Engineering & Technology, 84(2), 211-226. https://doi.org/10.1179/1758120614z.00000000043.

av människan som system, men rättviseaspekter handlar även om tillgänglighet till tekniken, tjänsterna och kunskapen. Därtill finns en rad ekologiska frågeställningar i och med introduktion av nya arter och ämnen i miljön. Redan idag finns stora olikheter globalt i hur tjänster och produkter används och kommersialiseras.

## Särskilda delområden

Utvecklingen inom bioteknikområdet påverkar och behöver omhändertas i militär kontext även i Sverige. Majoriteten av forskningen och utvecklingen kommer att drivas civilt. Försvarsmakten och andra försvarsaktörer kommer själva att behöva identifiera och utveckla de militära applikationerna. Försvarsorganisationer behöver därför följa och merunyttja den civila utvecklingen och vid behov påverka utvecklingen för bidrag till önskad militär förmåga. Detta behöver genomföras i kombination med egen forskning och utveckling inom specifika försvarsrelevanta områden, såsom skydd inom CB-området, viss materialutveckling, sensor- och signaturforskning och mänsklig förstärkning respektive degradering.

Bioelektronik[99], ett tvärvetenskapligt område i gränslandet mellan biologi och elektronik, är kanske det område som har störst disruptiv potential i det längre perspektivet, mot 2050 och därefter. Området innehåller många delar med direkt koppling till identifierade militära behov som ökad kognitiv förmåga, snabbare och bättre bearbetning och spridning av data samt bättre och snabbare interaktioner mellan människa och maskin. Det har även koppling till sensor- och signaturområdena och kan tänkas ha tillämpningar i relation till autonoma farkoster och system. Flera av applikationerna omgärdas av svåra etiska överväganden och är starkt integritetskritiska men har potentialen att ge disruptiva fördelar för tidiga användare. En möjliggörare är den allt bättre förståelsen av hjärnans funktioner.

System som består av både biologiska och elektroniska delar har dock funnits länge. Biosensorer består till exempel av en biologisk del som känner igen en signal (som en molekyl). Därefter omvandlas den biologiska signalen till en elektrisk signal som kan förstärkas och avläsas. Det är även möjligt att omvandla elektriska signaler till nervimpulser. Ett exempel som funnits länge är cochleaimplantat där en mikrofon uppfångar ljud som omvandlas till elektriska signaler som överförs till elektroder som ligger nära hörselnerven. Denna reagerar på de elektriska signalerna så att patienten ”hör” ljudet. Tillsammans med elektroder som kan detektera elektriska signaler i neuroner finns möjligheterna för tvåvägskommunikation mellan neuroner och elektroniska enheter. Elektromekaniska proteser kan redan idag styras via elektrisk koppling till nerver i extremiteterna och även direkt från elektroder i patientens hjärna via en dator-hjärna-koppling (BCI, *eng. Brain Computer Interface*).

BCI är ett forskningsområde som attraherar mycket intresse. I mars 2025 röstades det med överlägsen majoritet fram som läsarnas val till *MIT Technology Reveiw's*

99 https://en.wikipedia.org/wiki/Bioelectronics.

årliga lista med omvälvande teknologier (eng. *breakthrough technologies*).[100] BCI har länge dominerats av ett fåtal högprofilerade start-up-bolag med Neuralink i spetsen. Det är även ett aktivt forskningsområde i Sverige med forskargrupper vid ett antal universitet, bl.a. Linköping, Lund, KI och Chalmers. Ett närbesläktat område som redan används för behandling av patienter är neuromodulation, som till exempel används vid smärtbehandling[101], mot Parkinsons sjukdom, epilepsi, depression och andra tillstånd.[102]

Inom bioelektronik finns även annan forskning, som datalagring och beräkning samt biobränsleceller där mikrober eller enzym alstrar elektricitet (eller vätgas) vid nedbrytning av biologiskt material.

Den framtida militära energiförsörjningen ses som en utmaning. Om civila transporter och fordon främst drivs med el eller andra energikällor kan produktion av drivmedel till förbränningsmotorer bli en allt större militär angelägenhet. Bioteknik kan eventuellt ge möjlighet till utlokaliserad produktion av energislag såsom drivmedel till förbränningsmotorer och elektricitet. Bioraffinaderier för omvandling av biomaterial till koldioxidneutrala drivmedel är redan en realitet och biobränsleceller för produktion av elektricitet direkt från biologiskt material kan komma att bli möjligt.[103]

Ett nytt forskningsfält[104] som längre in i framtiden kan komma att påverka energiförsörjningsmöjligheterna är biohybrida framdrivningssystem där muskelcellers lättillgängliga energikälla (glukos), höga effektgrad, tysta gång och höga anpassningsbarhet utnyttjas. Forskningen är i ett mycket tidigt stadium där i första hand encelliga organismer, bakterier, alger och spermier utnyttjas som mikroskopiska ”pumpar” eller simmande bärare av last. Även muskler skördade från däggdjur och insekter alternativt odlade från stamceller har använts för att driva ”gående” eller ”krypande” mjuka nanorobotar. Uppskalning till gående bärare av last ligger mycket längre in i framtiden (efter 2050) då större ”muskler” kräver kontinuerlig tillförsel av syre och glukos via ett ”blodomlopp”, något som inte är möjligt idag men som det forskas mycket på främst inom regenerativ medicin och utformning av vävnader (eng. *tissue engineering*). Det tros vara möjligt att till 2050 skapa nya

100 https://www.technologyreview.com/2025/04/01/1114009/brain-computer-interfaces-10-breakthrough-technologies-2025/.

101 https://www.akademiska.se/for-vardgivare/sektioner/smartcentrum/vardgivarinformation-neuromodulation/.

102 https://www.merckgroup.com/en/research/science-space/envisioning-tomorrow/precision-medicine/bioelectronics.html.

103 Choi, S. (2023). Biofuel Cells and Biobatteries: Misconceptions, Opportunities, and Challenges. Batteries-Basel, 9(2), Article 119. https://doi.org/10.3390/batteries9020119.

104 Pinzger, B. (2024). Biohybrid Robotics. Fraunhofer Institute Rapport till FMV.

vävnader och skriva ut användbara strukturer och organ (eng. *bioprinting*).[105] Detta kommer att ha en omvälvande effekt på militärmedicin och traumavård. När nya organ kan printas vid behov för transplantation, utgående från stamceller hämtade från patienten själv, kan nya kroppsdelar, bioprintade och/eller elektromekaniska, ersätta förlorade kroppsdelar med bibehållna eller förbättrade egenskaper, med högre tillgänglighet och med mycket mindre risk att stötas bort än idag.

Realtidshälsoövervakning med sensorer (burna och/eller inopererade), individanpassad medicin och genterapibehandlingar kommer primärt att utvecklas för civil användning men har även stor nytta för försvarsverksamhet. Diagnos, optimering av träning och näringsintag eller medicinsk behandling baserad på (bio)sensordata skulle i framtiden kunna förutsäga behov av vila eller tillägg i nutrition, förhindra skador och förutse och förebygga smittspridning och sjukdomsutbrott. Genom kännedom om fysisk och mental status i vardag och under träning kan personalen i krig följas upp på distans. Vid behov, såsom utmattning, skada eller trauma, kan medicinering utföras endera automatiserat eller via självmedicinering. I den framtida operationsmiljön kommer möjligheterna för, men också kraven på och värdet av, den militära personalen att öka. Möjligheter att veta i vilket skick både enskilda soldater och enheter befinner sig kommer att öka, och därmed anpassning för uppgifter.

Även hotaspekten från kemiska och biologiska ämnen breddas och kompliceras med biotekniska möjligheter. Ökad kunskap om biologiska system ger möjligheter att utveckla nya mer raffinerade sätt att slå mot exempelvis människor och djur. Detta omfattar allt från nya verksamma substanser och produktions- och distributionsmetoder, till potentiella nya genetiskt modifierade organismer. Detta kan utgöra ett reellt hot inom den nära framtiden. Biotekniska framsteg medger även nya typer av motmedel och är därför en viktig aspekt att omhänderta. Skyddet inkluderar reglering, motmedel, indikering, sanering men även vaccinutveckling och framställning samt tillgänglighet och responstid. Ett exempel, m-RNA vaccin, visade sig under pandemin vara helt avgörande för befolkningsskyddet och därmed också för försvarsförmågan.

Hur ser framtiden ut? Det enda vi vet är att den kommer och att den kommer att bära med sig överraskningar. Om mat, energi och kanske byggmaterial kunde tillverkas av befintliga råmaterial i fält, vid fronten eller på skyddad plats skulle logistikbehov, rörlighet och basering påverkas. Sensorer med automatisk respons, bättre nutrition och kroppsegna reservdelsorgan bidrar till ökad uthållighet och överlevnad. Biomaterial kan ge biolika robotar av helt ny, icke-maskinliknande karaktär

105 Bliley, J. M., Shiwarski, D. J., & Feinberg, A. W. (2022). 3D-bioprinted human tissue and the path toward clinical translation. Science Translational Medicine, 14(666), Article eabo7047. https://doi.org/10.1126/scitranslmed.abo7047.
Wang, X., Zhang, D., Singh, Y. P., Yeo, M. J., Deng, G. T., Lai, J. Q., Chen, F., Ozbolat, I. T., & Yu, Y. (2024). Progress in Organ Bioprinting for Regenerative Medicine. Engineering, 42, 121-142. https://doi.org/10.1016/j.eng.2024.04.023.

och rörelse, samt material med en ny möjlighet till skydd och vilseledning på ett transparent slagfält. Flera av exemplen kommer inte att infrias, men andra kan komma i deras ställe. Vi kommer att bli överraskade och kanske överväldigade om delar av paradigmskiftet inom bioteknik slår igenom, och om teknikområden som fältet beror av utvecklas som förväntat.

## Samverkande och förutsättande teknikområden

### Genetik och genteknik

Bioteknikens grund rör informationsbärarna DNA och RNA och andra molekyler samt deras interaktioner. Området behandlar flera olika nivåer av komplexitet där förändringar i DNA och RNA styr celler att producera önskade tjänster.

I grunden ligger de molekyler som bygger upp informationsbärarna, som kan liknas med bokstäver i en bok. DNA-sekvenser, det vill säga gener, transkriberas och translateras till peptidsekvenser. Peptidsekvenserna, det vill säga proteiner, formas och omformas beroende på omständigheter. De veckas och modifieras för att utföra olika uppgifter i celler. Alla dessa steg, som är intrikata samspel mellan proteiner och andra molekyler, kan modifieras med hjälp av bioteknik. DNA och RNA kan förändras i små enskilda delar, helt nya sekvenser kan tillföras och befintliga tas bort. Även artificiella informationsbärare kan byggas upp för att skapa helt nya typer av strukturer som inte finns naturligt.

Biotekniken omfattar även reglering av cellers mognadsprocess, till exempel att styra hur stamceller stannar eller fortsätter i sin utveckling mot alla de olika specifika celltyper som bygger upp en biologisk organism och människa. Differentierade celler kan omprogrammeras till stamceller som i sin tur kan förökas, differentieras och 3D-skrivas till mänskliga vävnader och organ som sedan kan användas för transplantation i den ursprungliga donatorn. Det handlar om att skapa tjänster och produkter genom att göra förändringar i biologiska system, eller skapa helt nya sådana.

### DNA-tekniker

DNA-sekvensering, förmågan att läsa den primära genetiska koden i organismer, är en grundpelare i biotekniken. Teoretiskt finns här nästintill all information som behövs för att förstå hur en organism är uppbyggd. Det gäller bara att avkoda informationen. Hastigheten med vilken DNA kan sekvenseras har ökat oerhört snabbt de senaste 20–30 åren. Bioinformatik är området för informationshantering av exempelvis DNA.

Geneditering är genteknik som möjliggör specifika, riktade förändringar i DNA-sekvensen hos levande organismer genom användning av enzymer. Målet med geneditering är att införa förändringar i genuttrycket genom att ändra, ta bort, lägga till gener eller påverka transkriptionen av generna. Förändringarna i DNA-sekvensen

kan även påverka translationen till proteiner, dvs. proteinets aminosyrasekvens, och därigenom proteinets struktur och funktion. Den mest använda tekniken för geneditering är CRISPR/CAS som belönades med Nobelpris 2020.

DNA-syntes har varit möjligt länge, men möjligheten att skapa syntetiska, långa DNA-sekvenser har utvecklats de senaste åren. Hastigheten och skalan, men framför allt priset på syntetiserat DNA, möjliggör nu att hela DNA-uppsättningar för t.ex. virus görs genom syntes. Enklare organismers informationsbärande delar kan således skapas helt artificiellt i labb.

Syntetisk biologi är bioteknik som använder de ovan listade teknikerna för att göra förändringar i organismer, men med en mer ingenjörsmässig approach än den klassiska. Grundtanken är att designa organismer som är gjorda enbart för att utföra en uppgift, eller att modifiera en existerande organism så att den utför den uppgiften. I området ingår även att föra in informationsbärande element som inte finns naturligt.

### Neurovetenskaper och -teknologier

Bioteknik är tvärvetenskapligt och BCI ligger forskningsmässigt inom eller nära neuroteknologi. Såväl sekvensering av organismers och människans arvsmassa som studier av den mänskliga hjärnan har finansierats genom större forskningssatsningar som troligen lett till dagens upptäckter och utveckling.

År 2013 startades ett omfattande arbete med att kartlägga och bättre förstå hjärnans funktioner i USA. Det så kallade *Brain Initative* (*Brain Research Through Advancing Innovative Neurotechnologies*® Initiative) startades i syfte att revolutionera förståelsen om den mänskliga hjärnan.[106] Under åren 2013-2023 drevs i EU *The Human Brain Project* som ett *European Future and Emerging Technologies (FET) Flagship project*. Konvergens mellan områden och tvärvetenskap betonas, liksom är fallet för bioteknik och teknisk biologi. Målet med arbetet var, som det skrevs år 2012:[107]

> *"The Human Brain Project should lay the technical foundation for a new model of ICT-based brain research, driving integration between data and knowledge from different disciplines, and catalysing a community effort to achieve a new understanding of the brain, new treatments for brain disease and new brain-like computing technologies."*

### Systemövergripande forsknings- och tillämpningsområden

Regenerativ medicin och stamcellsforskning är grundläggande forskningsområden. Stamceller är celler som inte är fullt ut differentierade utan som kan ge upphov till ett antal olika celltyper. Förståelse för stamceller och differentieringsprocesserna används bl.a. i regenerativ medicin. Möjligheter att artificiellt skapa organ och reservdelar till människan är inte enbart av betydelse för vård. Det ger nya möjligheter

106 Home | BRAIN Initiative, https://braininitiative.nih.gov/.

107 Human Brain Project, https://www.humanbrainproject.eu/en/.

för kontrollerade kliniska tester och förståelse för interaktioner och effekter på en övergripande strukturnivå, innan tester i djur och människa.

Omics-fälten (*metabolomics, proteomics, genomics, transcriptomics, epigenomics*) ger förståelse för hur delar av organismer, organismer och system fungerar. Dessa områden utvecklas också med hög hastighet och analyserna får högre upplösning genom förbättrade analysmetoder, sensorer och databehandling. Datamängderna från omics-fälten kommer att bidra till ökad förståelse och nya tillämpningar som att anpassa lösningar till specifika behov, t.ex. individualiserad medicin. Sammantaget ger detta möjlighet att följa den enskilda organismen och gruppen som på så vis blir analyserbar, optimerbar, behandlingsbar etc. på en helt ny nivå.

Ett annat relaterat fält är samspelet mellan organismer och deras betydelse för varandra. Ett exempel är människans mikrobiom, dvs. de bakterier som finns i och utanpå våra kroppar. Betydelsen av det mänskliga mikrobiomet för allt från mental hälsa[108] till vikt[109] och infektionskänslighet är ett växande forskningsfält som kommer att utvecklas tack vare framsteg inom de olika omics-fälten.

### Bioinformatik och konvergens med informationsteknik

Redan nu är synergierna mellan bioteknik- och AI/ML-utvecklingen markanta där Googles DeepMind är det mest slående exemplet. Förståelsen för hur den mänskliga hjärnans korttidsminne fungerar användes som inspiration för programmering av neurala nätverk. 2024 tilldelades Demis Hassabis vid Google Deepmind Nobelpriset i kemi för de genombrott som möjliggjorts av användning av de nya bioinspirerade AI-möjligheterna för att beräkna hur proteiner veckar sig och antar sin funktionella form.

AI/ML ger en ökad möjlighet att modellera och simulera effekter av förändringar i biologiska system även utan en laborativt bevisad och perfekt teoretisk förståelse för systemen. Utförandet kommer att bedrivas alltmer ingenjörsmässigt och automatiserat i specifikt utformade forsknings- och tillverkningsanläggningar stöttat av allt större datamängder och förfinade beräkningsmöjligheter. En stor del av modelleringen är av optimerande karaktär, något en framtida utveckling av kvantberäkningar kommer att bidra till. Detta har tidigare i kapitlet exemplifierats genom DBTL-cykeln och *biofoundries*.

Ett ytterligare forskningsområde i gränslandet mellan biologi, bioelektronik, neuroteknologi och AI är biologiska datorer där neuroner används i stället för kiselhalvledare, ett slags *brain on a chip*.[110] Fördelarna med ett biologiskt system är minskad energiåtgång (och uppvärmning) med upp till en miljon gånger, men även datasäkerhet då döda celler förmodligen är mycket svåra att extrahera data

108 J. Am. Chem. Soc. 2025, 147, 4, 2998–3002.

109 Heliyon Volume 10, Issue 17, 15 September 2024, e37609.

110 https://www.nationalgeographic.com/science/article/brain-cells-organoids-computers-ai-energy.

ifrån. Området är dock i ett oerhört tidigt stadium och om exemplet någonsin blir verklighet så är det förmodligen långt efter 2050.

### Bioprinting och material med nya egenskaper

Kopplingen mellan additiv tillverkning, bioteknik och regenerativ medicin syns redan idag som 3D-bioprinting av vävnader och som stödstrukturer för tillväxt av celler, men även för tillverkning av medicintekniska produkter. Det ligger inte alltför långt borta att gissa att här finns ett mycket stort utrymme för tekniska genombrott, inte enbart för att printa ersättningsvävnader utan även helt nya biologiska system med helt andra egenskaper än dagens, för helt andra applikationer. Exempelvis kan kanske material med nya signaturegenskaper utvecklas.

Materialområdet är i vissa delar integrerat med bioteknik, då bägge områdena hanterar organiska strukturer på olika nivåer samt tillverkningssätt. Bioteknik kan ge nya sätt att framställa polymerer och andra typer av material med önskade egenskaper, där det biologiska kan gälla både framställningen och typen av produkt. Detta beskrivs kort i kapitlet om material. Bioteknik kopplar även till nanoteknikområdet.

## Påverkan på militär förmåga

Som tidigare beskrivits i kapitlet, exempelvis i stycken om särskilda delområden, kan bioteknik korskopplas med elektronik, robotik och autonoma system. Sensorer kan vara uppbyggda av biologiska element men även utvecklas med hjälp av bioteknik för en precisare upptäckt av skadliga ämnen och hälsoövervakning i eller utanpå biologiska system.

Bioelektronik skulle kunna användas till nya typer av gränssnitt och kopplingar till maskiner. Tänk om en drönarpilot kunde styra och koordinera flera semiautonoma system och deras funktioner enbart via hjärnan. Eller att de kontrolleras av biologiska datorer baserade på nervceller, artificiella hjärnor. Dessa skulle även kunna lösa problem med behov av beräkningskraft vid framskjutna noder. Analyser från Georgetownuniversitetets centrum för säkerhet och framväxande teknologier (CSET) pekar ut ökad kognitiv förmåga, ökad stridskapacitet (eng. *warfighting ability*) och artificiell hybrid superintelligens (biologisk och artificiell) som drivkrafterna bakom de stora kinesiska sattsningarna på *brain computer interfaces*.

Farkosters signaturer och signaturanpassning kan finna nya former genom biomimetiska robotar eller nya typer av biokamouflage och framdrivningsmekanismer.

Förmodligen är det effekterna inom områden som inte traditionellt förknippas med bioteknik som kan bidra med störst försvarsnytta. Listan på möjliga tillämpningar är lång. Biotekniska produkter och tjänster kommer att bidra till framtidens plattformar och system, energiförsörjning, miljöåtgärder, sensorer och signaturer,

material, databearbetning, integrering av människa och elektroniska system, logistik, underhåll och livsmedel, men givetvis även till sjukvården.

Däremot är de områden inom vilka försvarssektorn bör bedriva integritetskritisk forskning långt färre. En utmaning är bioteknikens bidrag in till andra försvarsrelevanta forskningsområden. Det kommer mot 2050 krävas att biotekniska områden bättre omhändertas i forsknings- och förmågeutvecklingsverksamheten än vad som är fallet idag. Förbättrade möjligheter till produktion och tillgång till energi och material har betydelse för allt från självbestämmande till uthållighet. En stor del av Försvarsmaktens materiel, system och förmågor kan påverkas. En utmaning med främst icke medicinsk bioteknologi är bristen på upparbetade komunikations- och samarbetsformer mellan de som identifierar problemen och de som förstår de biotekniska lösningarna.

Försvarsmässigt ses idag stora möjligheter inom medicin och rehabilitering samt hur människan kan förändras och stärkas. Utvecklingen av soldatsystemet samt mänsklig förstärkning och optimering omhändertas i denna antologi i separata kapitel. Bioteknik är ett medel för att förbättra, förstärka, degradera och återställa mänsklig förmåga. I de fall där syftet är illegitimt, exempelvis att degradera, finns överlapp med farhågor om framtida utveckling inom de biologiska och kemiska hotområdena.

Inom områdena kemiska och biologiska hot syns nya, och möjligen omfattande, typer av hot som inte hör samman med sedan länge reglerade agens och ämnen. Ökade kemiska och biologiska hot leder till ökade krav på skydd, profylax och motmedel. Biotekniken kommer även ge möjlighet till nya typer av skydd, diagnos och behandling.

Den framtida bioteknikutvecklingen kommer sannolikt att påverka balansen mellan offensivt användande av och försvar mot kemiska och biologiska hot. Denna balans, eller obalans, är i dagsläget starkt förskjuten till fördel för offensiv användning. Det finns möjlighet att bioteknikutvecklingen kommer erbjuda ökade möjligheter till försvar mot B- och C-hot. En förutsättning är dock att befintliga angreppssätt för att utveckla och använda motmedel utvecklas, därutöver att forskning kring hot avsevärt breddas till att omfatta risker med bioteknikens möjlighet att skapa helt nya typer av hot för militär verksamhet och samhället i stort.

Resultat från bioteknik används redan idag för att förutse och optimera hälsa och prestation hos individer. Detta kopplar an till mätning, sensorer, individanpassad vård och individualiserade upplägg för personal. Försvarets verksamhet pågår under mer eller mindre extrema förhållanden och här kan biotekniken underlätta för individens uppgift och överlevnad. Ett specifikt sätt att återställa, förändra eller förbättra människan är genom reversibel eller irreversibel påverkan på gener, så kallad genterapi.

Hjärnans funktion och mekanismer har beforskats länge. Mot 2050 kommer omfattande framsteg inom såväl neurovetenskaper, elektronik, materialteknik och datalogi leda till nya möjligheter för kognition och koppling till beslutsstödsystem. Begrepp som förstärkt och virituell verklighet (AR/VR) kan få helt nya innebörder, och styrning av proteser eller exoskelett kan ske på nya sätt.

Det finns relativt okontroversiella tillämpningar där organismers, växters och djurs genetiska material förändras, särskilt om de avser medicinsk behandling och även viss förädling av växter och djur. Gällande modifiering av grödor och djur råder dock ingen global konsensus. Redan idag finns stora skillnader i synsätt om ELSI (eng. *ethical, legal and social issues*) mellan till exempel EU och USA. Detsamma gäller specifika typer av förändringar i mänsklig arvsmassa, där både embryo och född individ kan ändras genetiskt. Inom militärt framåtblickande litteratur beskrivs supersoldater med övermänskliga egenskaper. Farhågan är att människan som system kan förändras, individuellt och som grupp, till att bli fysiskt och kognitivt överlägsen. Men även att individer och grupper kan bli alltmer sårbara. I och med de omfattande möjligheter biotekniken ger, finns otaliga etiska och legala utmaningar att ta ställning till. Civila aktörer driver en stor del av utvecklingen och mänskligheten kommer framöver fortsatt efterfråga bättre behandling av svåra genetiska sjukdomar och nedärvda drag, hälsosammare mat, en planet det fortfarande går att leva på och gröna lösningar på dagens klimat- och miljörelaterade utmaningar. Utvecklingen i stort kommer att påverka försvarets verksamhet och det samhälle försvaret verkar i.

## Aktörer

### Sverige

Sverige har en stark position inom bioteknik. Vi har världsledande företag i AstraZeneca och avknoppningar från Pharmacia. Vi har även internationellt ledande forskningsmiljöer som Karolinska Institutet. Utöver dessa finns ett antal mindre forskningsmiljöer där mycket intressant forskning bedrivs, t.ex. Umeå universitet, där Emmanuelle Charpentier arbetade med gensaxen CRISPR/CAS, och laboratoriet för organisk elektronik vid Linköpings universitet. Sverige har för att vara ett litet land en imponerade bredd i bioteknikforskning, detta syns bl.a. i det stora svenska bioteknikdeltagandet i EU:s ramprogram. Sverige har dessutom ett antal viktiga infrastrukturer för bioteknisk forskning, som SciLife Lab, MaxIV och ESS.

Sveriges största tillgång är, enligt Vinnova[111], ett Life science-block som kombinerar bioteknik, konnektivitet, autonoma system och AI, just den kombination som bör ha störst möjlighet att mynna ut i militärt relevanta genombrott.

111 Strander et al., 2024.

### Europa och EU

Bioteknik är ett fokusområde för EU. Det finns strategier som t.ex. *EU Bioeconomy strategy*[112], *Competiveness Compass*[113] och *Clean Industrial Deal*[114]. Däremot finns inte samma tydliga geopolitiska fokus som i USA och Kina.

Storbritannien och Schweiz är två framstående biotekniknationer utanför EU där speciellt Dstl i Storbritannien gör stora satsningar på det de kallar teknisk biologi (eng. *Engineering Biology*) med försvarsfokus.

### Nato

Natos forskningsorganisation (*Science & Technology Organization*, STO) startade under våren 2025 en ny panel för nya innovativa teknologier. De första två teknikområden som denna panel ska studera är kvantteknik och bioteknik. Sedan tidigare finns även en panel om människa och medicin (*Human Factors and Medicine*, HFM).

Att bioteknik och syntetisk biologi utgör utmaningar är något som Nato länge uppmärksammat. Exempelvis beskrivs detta i *Emerging Threats of Synthetic Biology and Biotechnology*, en publikation från 2021 där *NATO Science for Peace and Security Series C: Environmental Security* redogör för möjliga risker och handlingsstrategier.[115]

### USA

USA har publicerat flera dokument om bioekonomi, syntetisk biologi och bioteknik. År 2020 publicerades ett arbete där strategier för att omhänderta och säkra verksamhet inom *life sciences* presenterades, med fokus på strategisk global och ekonomisk relevans för att bättre omhänderta och fortsätta leda områden viktiga för bioekonomin.[116] Biden-administrationen hade ett stort fokus på bioteknik och

112 https://environment.ec.europa.eu/strategy/bioeconomy-strategy_.

113 https://commission.europa.eu/topics/eu-competitiveness/competitiveness-compass_en.

114 https://commission.europa.eu/topics/eu-competitiveness/clean-industrial-deal_en.

115 Trump BD, Florin MV, Perkins E, et al., editors. Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues [Internet]. Dordrecht (DE): Springer; 2021. Available from: https://www.ncbi.nlm.nih.gov/books/NBK584256/ doi: 10.1007/978-94-024-2086-9.

116 National Academies of Sciences, Engineering, and Medicine; Division on Engineering and Physical Sciences; Health and Medicine Division; Policy and Global Affairs; Division on Earth and Life Studies; Forum on Cyber Resilience; Board on Health Sciences Policy; Board on Science, Technology, and Economic Policy; Board on Agriculture and Natural Resources; Board on Life Sciences; Committee on Safeguarding the Bioeconomy: Finding Strategies for Understanding, Evaluating, and Protecting the Bioeconomy While Sustaining Innovation and Growth. Safeguarding the Bioeconomy. Washington (DC): National Academies Press (US); 2020 Jan 14. Available from: https://www.ncbi.nlm.nih.gov/books/NBK556429/ doi: 10.17226/25525.

bioekonomi med *Executive orders* inom området.[117,118] Vidare tillsatte administrationen en nationell säkerhetskommitté för framväxande bioteknik för att utreda hur landets nationella säkerhet kan komma att påverkas av utvecklingen inom biotekniken. USA är den klart starkaste aktören inom bioteknikområdet och satsar målmedvetet på att behålla den positionen.

### Kina

Kina satsar stort på forskning och utveckling inom många områden och bioteknik är ett av dem. I Kinas tolfte femårsplan (2010–2015) pekades bioteknik ut som en av de ”nya pelarna” i det industriella systemet. Insatserna har höjts i de följande femårsplanerna och i den senaste (14:e) pekas bioteknik ut specifikt som en nationell forskningsprioritet där investeringarna skall öka med mer är 10% årligen till 2035.[119] Satsningarna på bioteknik har gett resultat. I NSCEB-rapporten[120] beskrivs hur kinesiska företag som Wuxi AppTec köper upp mängder av innovativa företag i väst och på så sätt blir marknadsledande och med statliga pengar monopoliserar marknaden (så kallad *Brute force economics*). Ett annat företag som har byggt upp en ledande ställning på ett liknande sätt är BGI (Beijing Genomics Institute) som är störst i världen på gensekvensering. Kinesiska bolag har idag i stort sett hela världsmarknaden för gentester. Det har ifrågasatts huruvida det är klokt att ge Kina tillgång till så pass mycket genetiska data.

Den kinesiska strategin är hittills mycket lyckad och börsvärdet på kinesiska bioteknikbolag har de senaste fem åren ökat med 100 gånger.

### Kommersiella aktörer

De största aktörerna på bioteknikmarknaden är företag. Vi har avgränsat till läkemedelsbolag som utvecklar biologiska läkemedel eller som utnyttjar bioreaktorer för tillverkning av läkemedelssubstanser. Företag som AstraZeneca, Novartis, Roche, Johnson & Johnson och Merck & Co. satsade under 2023 tillsammans över 80 miljarder USD på forskning och utveckling inom bioteknikområdet, främst läkemedelsutveckling.[121]

117 https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/09/12/executive-order-on-advancing-biotechnology-and-biomanufacturing-innovation-for-a-sustainable-safe-and-secure-american-bioeconomy/.

118 https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/10/18/national-security-memorandum-on-countering-biological-threats-enhancing-pandemic-preparedness-and-achieving-global-health-security/.

119 https://www.fdd.org/analysis/2025/01/15/biotech-battlefield/.

120 https://www.biotech.senate.gov/final-report/chapters/.

121 https://www.fiercebiotech.com/biotech/top-10-pharma-rd-budgets-2023.

## Lästips

The Future of Biotech, National intelligence Council, 2021, NIC-2021-02494.

En populärvetenskaplig sammanställning om möjligheter med bioteknik för försvar 2050. https://www.nationaldefensemagazine.org/articles/2022/8/1/study-predicts-biotechs-long-term-impact-on-defense.

Strander, Y., Marklund, G., Zika, A., Stenberg, L., Lundin, N., Johansson, D., & Hallding, K. (2024). Strategiska tekniker för Sverige (2024-01501). Vinnova. https://www.vinnova.se/globalassets/publikationer/2024/rapport-ru-strategiska-teknikomraden_ver-01.0-final-1.pdf?cb=20241030174857.

Bliley, J. M., Shiwarski, D. J., & Feinberg, A. W. (2022). 3D-bioprinted human tissue and the path toward clinical translation. Science Translational Medicine, 14(666), Article eabo7047. https://doi.org/10.1126/scitranslmed.abo7047 .

Bunch, A. W. (2014). How Biotechnology Helped Maintain the Supply of Acetone for the Manufacture of Cordite During World War I. International Journal for the History of Engineering & Technology, 84(2), 211-226. https://doi.org/10.1179/1758120614z.00000000043 .

Choi, S. (2023). Biofuel Cells and Biobatteries: Misconceptions, Opportunities, and Challenges. Batteries-Basel, 9(2), Article 119. https://doi.org/10.3390/batteries9020119.

Pinzger, B. (2024). Biohybrid Robotics. Fraunhofer Institute Rapport till FMV.

Stenberg, L. (2024). Globalt perspektiv på kritiska tekniker (2024-01501). Vinnova. https://www.vinnova.se/globalassets/publikationer/2024/globalt-perspektiv-pa-kritiska-tekniker.pdf?cb=20241002125122.

Strander, Y., Marklund, G., Zika, A., Stenberg, L., Lundin, N., Johansson, D., & Hallding, K. (2024). Strategiska tekniker för Sverige (2024-01501). Vinnova. https://www.vinnova.se/globalassets/publikationer/2024/rapport-ru-strategiska-teknikomraden_ver-01.0-final-1.pdf?cb=20241030174857

Valdes, J. J., Chambers, J. P., & Kotras, D. M. (2024). Biological Electronics. Military Reveiw, March-April 2024.

Wang, X., Zhang, D., Singh, Y. P., Yeo, M. J., Deng, G. T., Lai, J. Q., Chen, F., Ozbolat, I. T., & Yu, Y. (2024). Progress in Organ Bioprinting for Regenerative Medicine. Engineering, 42, 121-142. https://doi.org/10.1016/j.eng.2024.04.023.

# Material

*Linda H Karlsson*

## Inledande beskrivning

Vår civilisations utveckling är tätt kopplad till människans förmåga att framställa, förädla och använda material. Våra första tidsåldrar är döpta efter de material vi lärde oss framställa och använda: stenåldern, bronsåldern och järnåldern. I samband med upptäckter av nya material och nya sätt att använda dem har civilisationen ofta tagit stora steg framåt. Utvecklingen av material och tillhörande tillverkningsprocesser har i stor utsträckning format den tekniska utveckling vi ser idag och som är en förutsättning för den militära utvecklingen genom historien och mot framtiden.

Forskning och utveckling inom materialteknik syftar till att upptäcka helt nya, eller kombinationer av redan kända, egenskaper hos material. Grafen är ett bra exempel, då det trots att det bara består av grundämnet kol har en rad intressanta kvaliteter såsom hög hållfasthet, temperaturtålighet, böjbarhet, elektrisk ledningsförmåga och värmeledningsförmåga. Inget annat känt material uppvisar enskilt samtliga dessa egenskaper.

Inom forskning och teknikutveckling testas material och deras egenskaper i olika steg: initialt i simuleringar och laboratorier, därefter i olika prototyper för att förhoppningsvis till sist kunna användas i en produkt. Tack vare framsteg inom avancerade beräkningar och analysmetoder, inkluderande AI, finns möjlighet att effektivisera denna process och att modellera snarare än experimentera i laboratorier som första steg. Allt tyder på att utvecklingen av material och de produktionstekniker dessa är beroende av kommer fortsätta att accelerera, mycket tack vare digitalisering, möjligheter till design inför experimentella tester, och bättre interaktion och utveckling med samverkande vetenskapsområden såsom bioteknik, nanoteknik och kvantteknik.

Materialforskningen drivs idag främst av civila aktörer, i form av kommersiella aktörer och akademi. Detta gäller i stort sett all materialutveckling i Sverige liksom i resten av världen. Det förändrade världsläget har ökat den militära sektorns intresse och år 2050 kommer troligen den militära och den civila sektorn att samverka för att ta fram material och tillverkningsprocesser som passar både för militära och civila användningsområden.

Idag ligger fokus inom den militära materialforskningen på avancerade material och produktionstekniker som kan ge upphov till material (och därmed produkter) som kan ge förbättrad eller till och med disruptiv effekt för militär verksamhet, såsom hypersoniska farkoster och adaptiv signaturanpassning, vilka potentiellt kan ge asymmetriska fördelar gentemot en motpart.

Materialutvecklingen idag kan skapa förutsättningar för disruptiva tekniska genombrott till år 2050. Om 20–30 år kan det finnas produkter med funktioner som inte existerar idag. Vi kommer kunna skapa olika typer av produkter specialanpassade för ett eller flera uppdrag, komponenter som tål extrem värme (över 1600 grader Celsius) och större påfrestningar samt sensorer som är försvinnande små och kan användas för att se i flera våglängder samtidigt, men även adaptivt kamouflage.

## Trender och exempel

Det är idag möjligt att manipulera material och materia ända ner på atomnivå och även att bygga upp och kombinera molekyler för att generera egenskaper som inte förekommer naturligt. Framväxten av kvantberäkningar och vidareutveckling av nanoteknologier ger förutsättningar för att skapa framtidens nanomaterial, biomaterial, energikällor och energilagringssystem samt mikrochip, för att bara nämna några exempel. Inom den militära sektorn kan nya material i förlängningen ge upphov till förbättrad effekt inom många tillämpningsområden. Exempel på sådana är vapen och sensorer som kan röra sig i hypersonisk fart, tysta och nästan osynliga vapen med högre verkan, mer effektiva skydd, adaptiva kamouflage och sensorer för flera våglängdsområden samtidigt, tysta ledningsplatser, bättre kommunikation samt telekrigsförmåga.

Nya tillverkningsmetoder såsom additiv tillverkning ger möjligheter att tillverka reservdelar och materiel där det behövs och när det krävs. Detta kan innebära minskat behov av lagerhållning givet att nödvändiga förutsättningar i form av råvara, energi, ritning, skrivare och tid samt rätt placering är uppfyllda. Användning av additiv tillverkning kan bli ett komplement till att reservdelar finns i centrala lager och transporteras därifrån vid behov och kan också ge Försvarsmakten tillgång till reservdelar som inte längre tillverkas. Effekten kan bli ett minskat logistikbehov för enskilda materielsystem men även krav på att nya logistiklösningar för produktion tas fram. Additiv tillverkning har visat sig kunna skapa strukturer som är omöjliga eller ytterst svåra att skapa med traditionella tillverkningsmetoder. Detta kan också möjliggöra produkter med bättre egenskaper, till exempel lägre vikt vid bibehållen (eller förbättrad) hållfasthet.

## Särskilda delområden

De militära domänerna är beroende av materiel och därigenom av materialutvecklingen. Med hjälp av artificiell intelligens och avancerade beräkningar kan ledtiderna för upptäckt av nya material minskas kraftigt. Det kan innebära att fler nya material upptäcks och kan studeras. Dock kommer det fortfarande ta tid att verifiera material för olika materielsystem, eftersom kraven ofta är hårt ställda och kräver många, långa och tidskrävande undersökningar och tester för att kunna verifiera materialets egenskaper. Normalt tar det ca 20 år från det att ett material

skapas i ett laboratorium till dess att det är implementerat i en kommersiell produkt. Samtidigt förväntas utvecklingen gå snabbare när den understöds av AI och i rådande världsläge med behov av snabbare ledtider. De mest lämpade nya material och materialkombinationer vi hör om från grundforskningen idag kan därmed ha hunnit implementeras i militära system redan innan år 2050.

Resultat från forskning och utveckling inom materialvetenskaperna är allmänt användbar. Nya material med stor genomslagskraft inom den civila sektorn kan troligen nyttjas även militärt. Det är därför av vikt att militär forskning och utveckling följer vad som sker på den civila sidan och tar hem det som kan vara militärt användbart.

Nedan beskrivs några särskilt intressanta materialområden med potential att bidra till nya och potentiellt banbrytande militära tillämpningar inom perioden fram till år 2050.

### Multifunktionella material

Multifunktionella material är ett samlingsbegrepp för material som har fler än en egenskap. Till exempel skulle ett material i en bärande struktur också kunna fånga in energi, lagra energi och/eller fungera som sensor för att mäta skador, temperatur eller tryck. Denna typ av material kan utöver sitt utökade antal egenskaper även ge ökad funktionalitet för de produkter som de ingår i. Exempelvis är vikt och volym konstanta utmaningar för många militära system.

Multifunktionella material skulle också kunna användas för så kallat dynamiskt underhåll, där materialet och därmed produkten själv signalerar behovet istället för att det som idag upptäcks av personal vid regelbundet underhåll.

### Avancerade material

Avancerade material är ett samlingsbegrepp för framforskade material med en eller flera egenskaper som är avsevärt bättre än de i naturen naturligt förekommande. Avancerade material designas för att förstärka specifika egenskaper för tilltänkta tillämpningar, vilket gör dem högst intressanta för framtida försvarsmateriel. Ofta designas dessa nya material på atomnivå, där kombinationer av flera olika grundämnen ger önskade egenskaper. Denna forskning är starkt beroende av kvalificerade beräkningsmodeller och datacenter med stor beräkningskraft, men också av nya mät- och verifieringsmetoder.

### Tvådimensionella material

Andra material som anses intressanta är tvådimensionella material som med sitt höga förhållande mellan materialens yta och volym, har extrema egenskaper och är väl lämpade för t.ex. gassensorer, katalysatorer och som dopämnen[122] i andra

122 Ämnen som tillförs till en struktur för att ändra någon egenskap hos denna.

material för att förstärka dessas egenskaper. Grafen[123], det första och mest kända tvådimensionella materialet, har undersökts för många tillämpningar både civilt och militärt. Det finns indikationer på att det redan implementerats i produkter. Grafen kan användas för dämpning av radarsignaturer vilket undersökts i prototyper för kamouflagenät av SAAB Barracuda och SmartIR.[124] SmartIR använder även grafen som signaturdämpande material för termiska och synliga våglängder. Tillsatsen av grafen gör också att signaturen kan bli adaptiv, det vill säga justeras.

Grafen kan användas i elektrooptiska sensorer för att minska behovet av kylning. För värmekameror är detta extra intressant då de ofta behöver kylas. Sensorerna blir därmed mindre, lättare och får bättre upplösning. Grafen kan även användas som gassensorer för t.ex. identifiering av CB-ämnen och explosivämnen. Grafen används i civila produkter som tillsatsämne i metaller såsom titan och koppar samt olika former av plaster (polymerer) för att minska vikt men bibehålla prestanda. Detta kommer med största sannolikhet också att användas militärt.

Eftersom grafen kan tillverkas av nästan allt kolbaserat material, är det intressant som ersättningsmaterial för miljöfarligare och klimatpåverkande material. Bland annat skulle grafenbaserade smörjmedel kunna ersätta oljebaserade smörjmedel med minskad klimatpåverkan och sannolikt lägre underhållsbehov som följd.

Andra tvådimensionella material såsom MXener används t.ex. som elektromagnetiska sköldar eftersom de är lätta och tunna och kan absorbera elektromagnetisk strålning.[125]

### Metamaterial

Metamaterial är syntetiskt skapade material med egenskaper som inte förekommer naturligt. Inom den militära forskningen utvecklas de för signaturdämpande tillämpningar, såväl elektrooptiska och magnetiska som akustiska. De kan skräddarsys för att bryta radarstrålning, värmestrålning och synligt ljus i bestämda riktningar och bryta och (omin)rikta akustiska ekon.

### Extremt värmetåliga material

Inom många olika militära tillämpningar utsätts material för extrem värme. Exempel är eldrör, robotar, motorer, förbränningsmotorer och efterbrännkammare, där temperaturer lokalt kan överstiga tusen grader Celsius. Dessutom har rymden blivit aktuell som en militär domän, vilket ökar behovet av uppskjutningar. Uppskjutna och nedstigande material utsätts för mycket höga temperaturer när de färdas

123 Se till exempel A.K. Geim och K.S. Novoselov, The Rise of Graphene, Nature Material 6, sida 183–191, 2007.

124 SmartIR.co.UK.

125 Iqbal et al, MXenes for multispectral electromagnetic shielding, Nature Reviews Electrical Engineering, 1, sida 180-198, 2024, https://www.nature.com/articles/s44287-024-00024-x.

genom atmosfären. Hotet från kraftiga laservapen gör också att behovet av värmetåliga material ökar.

Sammantaget har denna utveckling ökat intresset för värmetåliga material. Ett aktuellt exempel är högentropiska material som tål extrema temperaturer (över 2000 grader Celsius) samtidigt som de bibehåller sina egenskaper.[126] Utvecklingen av liknande material kommer att fortsätta fram till år 2050.

### Biomaterial

Biomaterial kallas de material som antingen härrör från naturen eller som har naturen som inspiration. De brukar delas in i biomimetiska, biokompatibla, biosyntetiska och biobaserade material. Intresset för dessa ökar på grund av behovet av miljövänliga och klimatvänliga material samt den snabba utvecklingen av nya avancerade verktyg. Biomaterial som kan fästas på eller opereras in i kroppen är till exempel av stort intresse.

Biomimetiska material är ingenjörsmässiga försök att härma djurs och växters anpassningar i naturen och på så sätt lösa olika tekniska problem. Ett exempel är hur kardborrars små krokar på sina taggar med sin envisa fästförmåga inspirerat till tillämpningar inom textil- och skoindustrin.

Inom bland annat signaturanpassning kan inspiration hämtas från hur kulörer byggs upp i naturen. Hos exempelvis skalbaggar och fåglar är det inte pigment utan strukturen på nanometernivå som ger upphov till färgen. Bläckfisken kan ändra både form och färg. I dess hud finns små färgpigment som kan förflyttas vilket gör att bläckfisken kan ändra färg. Forskning inom området kommer med största sannolikhet att öka, eftersom biomimetiska material bland annat kan användas för att kontrollera signaturer.

Biobaserade material inkluderar bland annat nanocellulosa och lignin, en rest som utvinns från skogsindustrin. Nanocellulosa är en form av polymer som utvinns från cellulosa eller framställs bakteriellt. Ofta är den nedbrytbar, ibland ätbar, och forskning pågår för användning vid svårläkta sår eller medicinering när biokompatibilitet är viktigt, dvs. inom medicin och vård för att möjliggöra att material kan användas i kroppen eller på huden utan att stötas bort.

### Nya polymerer

Polymerer, ofta kallade plaster i dagligt tal, är material som består av mycket långa molekylkedjor och som i industriella tillämpningar ofta är baserade på olja. Plaster är vitt spridda och har stor miljöpåverkan då de bryts ned mycket långsamt och

126 Karlsson, L.H, Dalberg, E, Andersson, P., Dalenbring, M. och Parmhed, O., Extremt värmetåliga material – Avskanning av forskningsfronten, FOI Memo 8675, december 2024. I detta memo är extremt värmetåliga material ett samlingsbegrepp för material som bibehåller sina önskvärda egenskaper vid temperaturer över 1600°C.

därmed stannar kvar i naturen länge. Forskning pågår för att ersätta dessa material med återvinningsbara eller miljövänligare polymerer, t.ex. nya avancerade, multifunktionella termoplaster som går att smälta och härda flera gånger, eller snabbt nedbrytbara biopolymerer baserade på naturligt förekommande material. Exempel på dessa är nanocellulosa, spindelsilke och lignin.

## Samverkande och förutsättande teknikområden

Material och materialutveckling är såväl beroende av som möjliggörande för forskning och utveckling inom många andra områden. En förutsättning för utveckling av framtidens avancerade material är framtagandet av nya tillverkningstekniker och analystekniker samt metoder kring dessa.

### Avancerad tillverkning

Med avancerad tillverkning menas idag förekommande men även framtida tillverkningsmetoder där material och materialstrukturer kan skräddarsys efter tillämpning. Dessa metoder används vanligen inom forskning och har inte tagit sig till industriell tillverkning än.

### Additiv tillverkning

Additiv tillverkning är en av de metoder som anses ha störst potential för att skapa strukturer och material med disruptiva kvaliteter. Additiv tillverkning är ett samlingsbegrepp för olika tekniker där strukturer byggs upp lager för lager genom tillsättning av material utgående från CAD-modeller.[127] Liksom traditionella tillverkningsmetoder kräver additiv tillverkning ibland efterbearbetning, som till exempel uppvärmning av strukturerna, eftersom hålrum och defekter kan uppkomma under tillverkningen. Temperatur och utrustning som behövs för uppvärmningen varierar kraftigt beroende på material och krav på slutstrukturen.

Forskning kring additiv tillverkning innefattar bland annat undersökningar av om det är möjligt att variera materialsammansättningen för att få så kallade gradienta material. Sådana material skulle kunna användas istället för färg eller andra skyddande lager som riskerar att släppa från underlaget vid upprepad användning av föremålet.

### Nanotillverkning

Nanotillverkning (*nanofabrication*) innebär att strukturer och material tillverkas i nanometerskala. Det är en grundläggande och viktig teknik för dagens elektronik där komponenter har ingående element i nanometerstorlek. Metoderna ger stor kontroll ned på atomskala vilket innebär att material (och delar till produkter) kan

127 Klassiska tillverkningsmetoder såsom slipning och svarvning kallas subtraktiva tillverkningsmetoder eftersom material tas bort för att skapa en struktur.

skräddarsys. Genom att göra komponenterna mindre kan fler och mer komplexa egenskaper tillföras till materiel.

Denna utveckling har accelererat på senare tid och kommer fortsätta förbättras i och med användning av artificiell intelligens och biomolekylära processer. Robotar i nanometerstorlek skulle till exempel kunna användas för att precisionsleverera mediciner i specifika organ och celler i människor och andra organismer.

### Biotillverkning

Biotillverkning (*biomanufacturing*) innebär tillverkning genom biologiskt baserade metoder eller med biologiskt baserade material. Denna typ av tillverkning kan möjliggöra produktion av avancerade farmakologiska molekyler men också av andra molekyler, polymerer och material som baseras på eller drar nytta av biologiska system. Tillämpningsområdena är många och beskrivs utförligare i kapitlet om bioteknik. Liksom för materialområdet ges nya förutsättningar till att hitta och tillverka biosystem och bioprodukter med hjälp av bland annat AI. En ingenjörsmässig *Design-Build-Test-Learn-approach* och automation ger nya förutsättningar för biotillverkning.

### Artificiell intelligens

Artificiell intelligens och avancerade beräkningsmetoder är viktiga för materialutvecklingen genom att de kan användas för att hitta nya material med önskade egenskaper. Utvecklingen drivs i dagsläget främst av forskning vid universitet och högskolor.

AI för utveckling av nya material har redan startat och kommer med stor sannolikhet att vara en disruptiv teknologi. Den som har tillgång till en stor databas med material med egenskaper som är väl anpassade för t.ex. avancerade flygtillämpningar, signaturanpassning etc. kommer att få en enorm fördel gentemot andra. Här gör t.ex. Google ett stort arbete med att identifiera nya material med hjälp av AI[128] och UC Berkeley leder ett projekt som samlar materialdata från experiment och simuleringar för att skapa en databas med alla material.[129] Dessa databaser kan användas för att söka efter ämnen med vissa egenskaper och även beskriva hur sådana material ska kunna skapas.

### Halvledare och mikroelektronik

Moderna mikrochip kallas halvledare då de till största delen innehåller halvledarmaterial. Dessa chip är en förutsättning för det moderna, digitaliserade samhället och kommer fortsätta att vara ytterst viktiga för att den tekniska utvecklingen ska

128 Millions of new materials discovered with deep learning, https://deepmind.google/discover/blog/millions-of-new-materials-discovered-with-deep-learning/.

129 https://next-gen.materialsproject.org/.

kunna fortsätta. Detta gäller även för militär materiel som i allt högre grad blir digitaliserad och där utvecklingen troligen inte kommer att bromsas i framtiden. Därmed kommer forskningen och utvecklingen av dessa material och tekniker att fortsätta vara av yttersta vikt för Sverige och vår försvarsförmåga.

## Påverkan på militär förmåga

Då material och produktionsteknik är grundbultar i det mesta omkring oss kommer förändringar av dessa med största sannolikhet att inverka även på framtida militär förmåga. Hur stor effekten kommer bli och inom vilka områden som förändringen kommer vara störst beror på många omständigheter. Nedan följer en sammanfattning av de faktorer som bedöms ha störst påverkan om utvecklingen fortsätter som idag.

Avancerade material och strukturer framtagna med artificiell intelligens, samt nya tillverkningsmetoder som additiv tillverkning, kan komma att få en oöverskådlig påverkan inom försvaret.

Tvådimensionella och andra avancerade material kommer att kunna öka sensorers känslighet och snabbhet samt möjliggöra minskad sensorstorlek. Detta tillsammans med samhällsutvecklingen, med ökad övervakning och tillgänglighet av kameror, kommer att förändra lägesbilden för Försvarsmakten såväl som för våra eventuella motparter. Man talar om det transparenta slagfältet, där det blir svårare att undgå upptäckt.

Detta ökar behovet av signaturanpassning på olika sätt, bland annat nya material som kan imitera omgivningen statiskt eller adaptivt. Här kan till exempel biobaserade material och biomimetiska material spela en viktig roll. Soldatutrustning som ändrar färg och skenbar temperatur kommer att finnas. Även annan form av signaturanpassning, såsom akustisk, kan påverkas starkt av den pågående materialutvecklingen.

Idag finns stort forskningsfokus på lättare och mer värmetåliga material, bland annat nya kompositer, för att minska flygets påverkan på klimatet. Detta kan få en stor påverkan på framtida flygförmåga då dessa material skulle kunna användas för lättare och mer lastbärande flygande farkoster.

## Aktörer

Materialteknik och forskning kring avancerade material har av många aktörer, bland annat länder som USA, Ryssland[130] och Kina, samt internationella organisationer som Nato och EU, identifierats som kritiskt för att behålla och uppgradera militära förmågor. Även betydelsen av material för det civila samhället och

130 Thematic Intelligence: Aerospace, Defense & Security, Advanced Materials in Defense, Global Data, 16 januari 2023, GDDEF-TR-S062.

totalförsvarsförmågan har framhållits. I Sverige har behovet av avancerad materialteknik lyfts i flera strategier.[131]

### Sverige

Traditionellt har Sverige varit starkt inom materialforskning och -utveckling. Vi har en industri baserad på järn och stål och svenska universitet har framstående, inom vissa områden världsledande, materialforskning.

Sverige har också rika tillgångar på sällsynta jordartsmetaller. Tidigare har man inte utvunnit dessa då det inte varit ekonomiskt lönsamt och inte heller funnits tillräckligt med incitament för att påbörja gruvdrift. I och med det ökade behovet av sällsynta jordartsmetaller, som ett resultat av elektrifieringen av samhället, kan detta komma att omvärderas. Detta särskilt mot bakgrund av planerna på att öka graden av självförsörjning av kritiska råmaterial inom EU.

Wallenbergs initiativ gällande material för framtiden (*Wallenberg Initiative Materials Science for Sustainability,* WISE) är en av de större satsningarna i modern tid inom material med stort fokus på klimatpåverkan. Den kommer med största sannolikhet även att påverka utveckling av material för militära tillämpningar.

Inom svensk innovation har det militära materialområdet fått ett uppsving de senaste åren med bland annat företag som Grafren, som modifierar grafen för militära tillämpningar och Amexci som tillverkar militär materiel med additiv tillverkning.

### Europa och EU

Inom Europa och EU, bland annat inom *Europan Defence Agency* (EDA), pågår arbete med att identifiera kritiska material och infrastruktur samt att bygga upp infrastruktur för kritiska material och relaterade produktionstekniker. Detta för att göra Europa mindre beroende av andra länder. Utlysningar inom EDF och *Horizon Europe* stöttar forskningen inom den militära respektive civila sektorn, till exempel *The Innovative Advanced Materials Initiative* (IMI4EU). Samtidigt kräver den typ av satsningar som diskuteras mycket pengar över lång tid.

Fabriker för så kallade halvledare, dvs. mikrochip, planeras inom EU och kommer troligen i framtiden att byggas upp i något eller några EU-länder. Hela kedjan från gruva till förädling till processering och tillverkning av mikrochip kommer att behövas. Detta är en stor omställning för EU som hittills köpt materialen från andra länder. Vi har dock en stark forskning inom EU och Sverige kring dessa material, så förhoppningen finns att vi kommer ha den kompetens som behövs. På grund av den avancerade tillverkningen kommer inte mikrochip kunna tillverkas i fält

131 Coming together to lead the way, A Swedish research and innovation within additive manufacturing and 3D printing. Umeå universitet 2017, https://www.vinnova.se/m/strategiska-innovationsprogram/agendor/additiv-tillverkning-och-3d-printing/. Datum: 2024-11-14.

fram till år 2050, utan kommer att behöva tillverkas på specifika platser med rätt material och utrustning för att sedan transporteras ut i fält.

EU och Europa arbetar även med cirkularitet inom både den civila och militära sektorn, dvs. att byta ut miljöfarliga material mot miljövänligare.[132]

### Nato

Nato har identifierat material och materialutvecklingen som ett prioriterat forskningsområde. Även tillgången till kritiska råmaterial för militär materiel är något som Nato lyfter fram liksom säkerställd tillverkning inom alliansen och fungerande försörjningskedjor.

### USA

USA har en traditionellt stark materialforskning inom både den civila och den militära sektorn. Likt EU arbetar USA med att skapa egna värdekedjor för kritiska råmaterial. De har stark forskning inom många materialområden, elektronik samt artificiell intelligens. På universitet som MIT och Stanford pågår materialforskning i världsklass.

### Kina

Kina lägger stora resurser på forskning och utveckling inom materialområdet. Enligt *Australian Strategic Policy Institute* (ASPI) är kinesiska institut ledande inom forskning inom stora delar av materialområdet.[133] Detta ligger helt i linje med Kinas mål att bli ledande inom allt fler teknikområden och utmana resten av världen, speciellt USA, om att vara starkast inom forskning och teknikutveckling både civilt och militärt.

### Kommersiella aktörer

Stora företag som Google lägger ned stora pengar på materialforskning och tillhörande industri. Civila aktörer har redan stor betydelse och kommer förmodligen att få en än större betydelse i framtiden.

## Lästips

Karlsson, L.H, Dalberg, E, Andersson, P., Dalenbring, M. och Parmhed, O., Extremt värmetåliga material – Avskanning av forskningsfronten, FOI Memo 8675, december 2024.

132 Det sker idag ofta genom att man ersätter med en molekyl/struktur som är näraliggande men som ännu inte visat sig ha skadliga effekter.

133 https://www.aspi.org.au/programs/critical-technology-tracker/.

Thematic Intelligence: Aerospace, Defense & Security, Advanced Materials in Defense, Global Data, 16 januari 2023, GDDEF-TR-S062.

# Energi

*Wilhelm Sahlén, Mattias Elfsberg och Niklas Zettervall*

## Inledande beskrivning

Energi betraktat som teknik- och forskningsområde innefattar allt från batterier och bränslen till försörjningskedjor, logistiska utmaningar och geopolitik.[134] Energiområdet kan, för både stora och små system, betraktas från produktions-, distributions-, lagrings- och konsumtionsperspektiv, dvs. det omfattar:

- Omvandling av energi från källor som sol, vind, kärnbränsle eller fossila källor till mer användbara former där elektricitet och bränslen är två exempel.
- Distribution av producerad energi, som elektricitet över kraftnät eller som flytande eller gasformigt bränsle via fartyg, tankbilar eller olje- och gasledningar. Distributionen sker ofta via någon form av lagring, kanske framförallt när det handlar om bränslen.
- Lagring av energi. Detta är centralt då tillgång och produktion måste balanseras med efterfrågan och förbrukning. Exempel på lagring är allt från stora bränslelager i bergrum till energi lagrad i en elbil eller mobiltelefon.
- Nyttiggörande av energi i tillämpningar. Exemplen på där energi konsumeras är i princip oändliga med allt från framdrift av fordon, fartyg och flygplan, till IT-system och uppvärmning och drift av anläggningar.

För en robust, ekonomiskt hållbar och välfungerande energiförsörjning är respektive perspektiv beroende av varandra och utformning av energisystem måste utgå från relationen mellan perspektiven.

Forskning och teknikutveckling inom energiområdet drivs främst på av samhällets energiomställning och utfasningen av fossila energikällor. Att ersätta system som är beroende av fossila energikällor och energieffektivisering är två centrala frågor. Energiomställning är inte bara en utmaning för försvarsmakter utan kan möjliggöra förmågeförhöjning och ökad resiliens om tekniker som utvecklas tillvaratas. En viktig fråga för Försvarsmakten är förmåga i kallt klimat, vilket ställer specifika krav på energisystem. Militära tillämpningar har av sin natur höga krav på robusthet och säkerhet.

134 W. Sahlén, M. Elfsberg, J. Enström, M. Karlsmo, M. Karlsson Hagnell, E. Lallo, A. Odell, R. Stappe Renner och N. Zettervall, ”Förstudie för FoT område Energiförsörjning,” FOI-R--5705--SE, 2024.

## Trender och exempel

Utvecklingen av nya energitekniker innebär att omställningen från fossila bränslen inte enbart medför hinder[135] – den öppnar också nya möjligheter. Tekniker som utvecklas har bred påverkan och driver förändring inom både stora och små industrier. Exempelvis har SSAB för avsikt att ställa om sin produktion genom det fossilfria stålsamarbetet Hybrit[136], samtidigt som intresset för kärnkraft växer och innovativa batterilösningar integreras i en rad olika system.

Samhällets utfasning av fossila bränslen påverkar försvarsmakter och militära system som förlitar sig på civila försörjningskedjor. Utfasningen kommer fortsätta mot 2050, där omfattningen kan vara svårbedömd. Elektrifieringen av personbilsflottan kommer mycket sannolikt fortsätta där utbyggnad av infrastruktur för laddning och tillgång till el är förutsättningskapande. Några trender kopplat till elektrifiering av fordonsflottan är önskan om batterier med högre energitäthet för ökad räckvidd samt att korta ner laddningstiderna, vilket i sin tur ställer högre krav på både batterier och laddningsinfrastruktur med krav på tillgänglig effekt vid laddningstillfället.

När det kommer till den militära fordonsflottan kan det vara svårare att byta ut drivlinor till helt elektriska då det finns krav på fordonen som inte uppfylls med nuvarande energilagringstekniker, till exempel avseende räckvidd och fältmässig möjlighet till laddning. Det finns däremot plattformar som kan gynnas av att hybridiseras. En hybridisering kan medföra bränslebesparing genom att den traditionella förbränningsmotorn kan arbeta mer effektivt då den stöttas av en elektrisk motor. Exempel på andra fördelar är att markfordon eller fartyg med en hybridiserad drivlina kan övervaka områden tyst utan att behöva starta en förbränningsmotor. En hybridiserad drivlina med elmotorer får en annorlunda effekt- och vridmomentskurva jämfört med traditionella förbränningsmotorer vilket kan medföra bättre manövrerbarhet för plattformen.

Mot 2050 kommer sannolikt de flesta militära plattformar vara hybridiserade men man kommer fortfarande behöva förlita sig på flytande bränslen framförallt för tunga markfordon, fartyg och flyg där kraven på energitäthet och räckvidd är höga.

En majoritet av alla transporter använder idag flytande fossila bränslen och samhället vilar i grunden på en infrastruktur kring dessa bränslen. Det betyder att om de fossila bränslena till sin huvuddel kan bytas mot likvärdiga bio- eller elektrobränslen innebär det en enorm besparing då ingen ny infrastruktur kommer behövas. Även om det i teorin skulle kunna gå att ersätta det mesta av de fossila bränslena med dessa alternativ är det i praktiken behäftat med en mängd potentiella försvårande omständigheter, där ekonomi, politik samt tillgång på insatsvaror (biobränslen) och elektricitet (elektrobränslen) kommer att sätta gränserna. Likt för batterier drivs

135 J.Enström, K. Danel, E. Lallo, S. Munktell, W. Sahlén, M.Tynnhammar, ”Omvärldsanalys – Energitekniker”, FOI-R--5606--SE, 2024.

136 https://www.hybritdevelopment.se/.

omställningen från den civila sidan, ofta med liten insikt kring de militärspecifika krav som försvarsmakter kommer behöva.

Ett område som arbetar mot en omställning är det civila flyget. Till exempel är det redan från 2025 ett krav att allt flyg inom EU tankas med minst 2% *Drop-In Sustainable Aviation Fuel*, SAF, en siffra som dock kan vara så hög som 50% på enskilda flygningar. EU:s mål på 70% SAF år 2050 kommer ställa stora krav på produktion men även på en större bränsleflexibilitet. Begränsningar i tillgänglig instatsråvara för produktionen av dessa SAF-bränslen kommer kräva större bredd vad gäller vilka bränslen som kommer vara godkända att flyga på. De idag elva godkända processvägarna för produktion av SAF kommer att behöva bli fler.

För elektrobränslen är målen lägre satta på grund av större utmaningar kring produktionsekonomi och en ännu omogen teknik. Här har EU satt målet till 1,2 % inblandning år 2030 och 35 % år 2050.[137] Vi bedömer dock att osäkerheten i dessa siffror är betydande. Noterbart är att flyg, både civilt och militärt, är väldigt viktkänslig och kräver en energibärare med hög energitäthet. Förutsatt att ingen revolutionerande teknik kommer att öka energitätheten hos batterier radikalt, kommer allt flyg fortfarande vara beroende av flytande jetbränslen 2050. Även om en revolutionerande batteriteknik, med tillräckligt hög energitäthet, skulle finnas på plats innan 2050 är ledtiden för att utveckla och certifiera nya flygplan så pass lång att dagens flygteknik fortfarande kommer vara den dominerande.

För fordonstrafiken är situationen en annan. Här genomgår personbilstrafiken ett skifte mot elektrifiering och bedömningen är att denna andel kommer att öka fram till 2050, vilket innebär att behovet av alternativa flytande bränslen är begränsad. För lastbilstrafiken kan dock situationen vara en annan och det kan finnas en stor marknad för både bio- och elektrobränslen.

Det område som är mest eftersatt och som ligger längst ifrån att byta de fossila bränslena mot alternativa är den storskaliga fartygstrafiken där till exempel containerfartyg och tankfartyg inkluderas. Det finns dock gemensamma intresseområden mellan fartygsdieslar och fordonsdieslar och eventuellt kan dessa två områden tillsammans driva utvecklingen. För mer småskaliga fartygstyper med kortare transportsträcka finns det redan idag exempel på eldrift och andra alternativa framdrivningslösningar.

Behoven och (säkerhets)kraven på bränslen för flyget, och för fartyg och lastbilstrafik, skiljer sig åt radikalt och utvecklingen inom dessa två kategorier sker i det närmaste separat. Eftersom flygtrafiken har mycket hårt ställda krav på densitet, förångningsegenskaper, inblandning av aromater med mera har dieselmotorer lägre satta krav och kan använda bränslen med mindre hårt definierad specifikation. Som exempel är både RME (rapsmetylester) och HVO (hydrerad vegetabilisk olja) godkända redan idag för fordonstrafik men skulle aldrig kunna användas i dagens flygplansmotorer.

137 https://transport.ec.europa.eu/transport-modes/air/environment/refueleu-aviation_en.

Vätgas är ett annat omtalat bränsle. Vätgasen har flera attraktiva egenskaper såsom förmåga att brinna vid ett bredare blandningsförhållande än kolväten, hög viktmässig energitäthet och koldioxidfritt utsläpp samt förmåga att användas i bränsleceller. Dock finns en kaskad av potentiella egenskaper som kraftigt kan reducera dess användning. Vätgas är flyktig och kräver väldigt specialiserad lagringsinfrastruktur som kraftigt försvårar dess användning. Dess explosiva natur och en potentiellt hög andel kväveoxider (NOx) i förbränningsprodukterna är två andra negativa aspekter, liksom försprödning av (metall)material och en infrastruktur som i dagsläget inte är i närheten av att vara komplett nog för att vätgasen ska kunna ersätta flytande bränslen i närtid. Att binda vätgasen i andra större molekyler, så kallade vätebärare, är ett alternativ som lyfts fram. Där talas det i huvudsak om ammoniak (NH3) men då det är giftigt, brandfarligt och potentiellt korrosivt kommer sannolikt det inte bli ett huvudsakligt bränsle i framtiden. En rimlig bedömning är att ammoniak även i framtiden i huvudsak kommer användas som konstgödsel.

### Reservkraft/ödrift

Försvarsmakter är generellt beroende av det civila samhället för energiproduktion och bränslen, vilket kan medföra sårbarheter vid konflikter. Vilket inte minst har visats under Rysslands anfallskrig mot Ukraina.[138] Energiförsörjningssystemet är ett attraktivt mål för fienden att sabotera eller slå ut. För att öka motståndskraften och minimera risken för energibortfall kan elnät decentraliseras med flera militära mikronät som kan byggas upp som redundans för det civila elnätet. Idén att decentralisera elnätet är inte på något sätt ny men har fått ett uppsving i samband med ny teknik som möjliggör enklare självförsörjning av energi. Exempel på detta är lokal produktion av elektrisk energi med förnybara energikällor som sol, vind och vatten där energilagring blir viktigt då solen inte alltid skiner eller att det inte alltid blåser. Det finns därmed ett behov av att lagra effektöverskott, dock inte nödvändigtvis bara i batterier. Konceptet för detta kallas *Power to X* och går ut på att nyttja överskott av energi till att producera vätgas, metanol eller andra fossilfria bränslen.[139] Försvarsmakten och även andra organisationer (till exempel sjukvård, polis och brandkår) som behöver ha elektricitet eller drivmedel vid kris kommer sannolikt att satsa på mikronät och bli mer självförsörjande. Exempel på detta tas upp i klimatstrategin för USA:s armé från 2022 där de ska öka andelen militära anläggningar med mikronät med 30 % jämfört med 2021.[140] För att lagra energin kan olika metoder nyttjas, där batterier är ett enkelt sätt att både lagra och nyttja elektrisk energi men kan ha begränsningar på grund av lägre energitäthet jämfört med andra lagringstekniker. Det kan därmed vara fördelaktigt att kombinera olika

138 A. Odell, A. Lioufas, M. Olsén, K. Mossberg Sonnek, F. Welander och A. Hörnedal, ”Russian attacks on the Ukrainian power system,” FOI-R--5596--SE, Stockholm, 2024.

139 https://www.ri.se/en/from-electricity-to-x-for-the-climate.

140 https://www.army.mil/e2/downloads/rv7/about/2022_Army_Climate_Strategy_Implementation_Plan_FY23-FY27.pdf.

typer av tekniker som tillsammans skapar ett robust och effektivt energilagringssystem. Ett exempel på fördelaktig kombination är hybriddrift med batteri och förbränningsmotor. En förbränningsmotor har bäst verkningsgrad vid ett optimalt varvtal. Vid en varierad last kommer varvtalet att variera och därmed även verkningsgraden. Kombineras förbränningsmotorn med ett batteri tillåts den att ständigt gå vid sitt optimala varvtal medan batteriet hanterar variationen av lasten. Systemet kommer därmed få en bättre verkningsgrad än vid nyttjandet av enbart en förbränningsmotor.

En annan teknik för energilagring är metaller. Metaller kommer med flera fördelar, där hög energitäthet och enkel hantering är två av de mest attraktiva. De huvudsakliga hindren kring metallförbränning för energiproduktion är att det är en ny oprövad teknik, utan egentlig infrastruktur samt att frågor såsom slitage vid kraftverk är ett stort frågetecken idag. Nya tekniker likt denna har förmodligen långt kvar innan de är redo för storskaligt användande. Det finns dock en potential att använda lätt ombyggda kolkraftverk där kolpulvret byts mot metallpulver. Redan idag finns forskningsprojekt för detta i Europa.[141] Om metallförbränning realiseras finns potential att nyttja denna typ av energilagring i olika typer av fartyg, militära och civila, men även anläggningar. Främst gäller det tillämpningar där vikt inte är en kritisk parameter.

Vissa länder genomför även studier av moderna kärnkraftreaktorer som är små och modulära, på engelska benämnt *Small Modular Reactor* (SMR). Bland annat utvecklar USA en SMR som dessutom ska vara lätt att utplacera och driftsätta[142] och i Estland utvecklar företaget Fermi Energia en mer stationär SMR.[143]

## Särskilda delområden

Lagring av energi är centralt vid utformningen av ett tillfredsställande energiförsörjningssystem. En förutsättning för att energilagringsteknikerna får relevans är att det finns tillgänglig energi att lagra. Energi kan genereras på en mängd olika sätt. För det civila elnätet i Sverige dominerar vattenkraft och kärnkraft, följt av vindkraft, värmekraftverk och solkraft.[144]

Val av energilagringsteknik kan se olika ut beroende på vilka krav en tillämpning ställer. Energilagringstekniker som bedöms spela en betydande roll för militära system och plattformar är batterier och bränslen i form av fossila bränslen, biobränslen, elektrobränslen, vätgas och metall. Vilken energilagringsteknik som är bäst bestäms helt utifrån vilka krav som tillämpningen ställer. Energilagringsteknikerna

141 https://www.metalot.org/.

142 https://www.cto.mil/pele_eis/.

143 https://fermi.ee/en/fermi-energia-chooses-ge-hitachis-bwrx-300-as-the-technology-for-planned-smr-nuclear-power-plant-in-estonia/.

144 https://www.vattenfall.se/fokus/hallbarhet/sveriges-elproduktion/.

har olika för- och nackdelar där vissa har högre energitäthet men kanske svårigheter i form av att de är mindre flexibla i effektuttag medan motsatsen gäller för andra tekniker. I vissa fall finns det goda skäl att kombinera olika energilagringstekniker för att uppnå ett tillfredställande energiförsörjningssystem.

Ett annat delområde som är intressant är energiskörd[145] (eng. *energy harvesting*), där energi skördas från olika naturfenomen och lagras för att kunna nyttjas av elektronisk utrusning. Det som är utmärkande är att det generellt handlar om icke konventionella energikällor med oftast mycket låga effekter. Exempel på källor kan vara sol, vind, termiska källor, vatten, piezoelektricitet, elektromagnetiska generatorer och biobatterier.

### Batterier

Batterier är viktiga som energilager på grund av deras frekventa förekomst samt deras näst intill unika förmåga att lagra elektrisk energi. Batterier kan delas in i primära (ej uppladdningsbara) eller sekundära (uppladdningsbara) batterier, där majoriteten av utvecklingen sker på sekundära batterier så som litiumjonbatterier. Litiumjonbatterier har en mycket hög energitäthet jämfört med andra batterikemier, vilket har gjort att de finns i nästan all modern elektronisk utrustning, såväl för civil som militär användning. De används även nästan uteslutande i el- och hybridfordon som energilager. Näst mest mogen av batteritekniker som bygger på metalljonbatterier är natriumjonbatterier, som på 70- och 80-talet studerades parallellt med de nu marknadsledande litiumjonbatterierna. Natriumjonbatterier är också kommersialiserade och används i en rad olika tillämpningar globalt. En stor fördel med dessa är att de inte är beroende av dyra och sällsynta material. Natriumjonbatterier kan just nu ses som komplement snarare än ersättare för litiumjonbatterier då de har betydligt lägre energitäthet än litiumjonbatterier.

Globalt är den akademiska forskningen och industrins utvecklingsverksamhet omfattande med en tillväxt som fortsätter accelerera. Denna drivs i hög grad av politisk styrning med högt uppsatta mål om elektrifiering och omställning till en fossilfri energiinfrastruktur, vilket kommer kräva en stor mängd batterikapacitet. Inom Europa finns ambitioner att expandera batterisektorn och bli självförsörjande. Många aktörer får stöd genom stimulansåtgärder från både privata och offentliga aktörer. Bland annat satsas det på natriumjonbatterier av företag som det svenska Altris men även Tiamat, CATL, Novasis Energies och Natron Energy. För de redan väletablerade litiumjonbatterierna är kostnad och prestanda de stora forsknings- och utvecklingsfrågorna, där det finns många förslag på vidareutveckling.

Eftersom natriumjonbatterier inte har utvecklats lika intensivt som litiumjonbatterier finns det teoretiskt sett stora möjligheter till förbättringar. Skulle

145 Bhatt K., Kumar S., Kumar S., Sharma S., Singh V., ”A review on energy harvesting technologies: Comparison between non-conventional and conceptual approaches”, Energy Reports, 12, pp. 4717 – 4740, 2024, DOI: 10.1016/j.egyr.2024.10.019.

natriumjonbatterierna väsentligt förbättras med avseende på bland annat energitäthet skulle detta kunna vara ett stort framsteg för naturresursproblematiken och de skulle kunna vara ett bra alternativ för högeffektstillämpningar.

Ett flertal olika batterikemier bubblar upp med förhoppningar om att göra banbrytande framsteg inom batteriforskning. Sannolikheten för revolutionerande genombrott anses vara låg och litiumjonbatterier förväntas fortsätta dominera marknaden under de kommande 10–20 åren, dock med stöd av andra batterityper som komplement.

En utmaning för batterier som i någon mening är specifik för försvarstillämpningar med hårda krav på robusthet är funktion i kallt klimat där en del forskning och utveckling pågår där man framför allt studerar olika elektrolyter.

### Bio- och elektrobränslen

Utvecklingen av bio- och elektrobränslen drivs av den civila sidan. Det gör också att flertalet av försvarets specifika behov kan glömmas bort. När man fokuserar på bränslen för flyget (SAF[146] och elektrobränslen) är det centralt att komma ihåg att militära system nästan alltid är operativa under mycket längre tid än civilt flyg. Två exempel på detta är amerikanska Boeing B-52 och europeiska Panavia Tornado, där den förstnämnda togs i bruk redan 1955 och först nu får en kraftig uppdatering av motorerna. Längre operativ tid betyder att systemen inte nödvändigtvis enkelt kan anpassas till nya krav, speciellt inte för en så central del som bränsle och bränslesystem. Här kan det bli så att vissa specifika krav kommer att behöva tas hänsyn till när den civila sidan går mot mer och mer SAF-inblandning. Det är inte omöjligt att militärt flyg kan behöva begränsa mängden SAF-inblandning under en tidsperiod, alternativt behöva inblandning av olika ämnen för att klara sin specifika specifikation.

Även för fordonssidan har den militära sidan specifika krav som inte nödvändigtvis kan mötas av de bränslen som finns inom den civila trafiken. Militära fordon har ett stort behov av lagringsstabila bränslen då dessa fordon har en mycket kortare och mindre frekvent körsträcka. Civila fordon har en kort omsättningstid på bränslen, vilket betyder att relativt instabila bränslen såsom RME aldrig hinner degraderas så pass att det påverkar motortillförlitlighet eller motorprestanda. Kort omsättningstid betyder också att fuktnivåer aldrig hinner bli ett problem i bränsletankar. Inget av detta gäller nödvändigtvis för de militära fordonen eller fartygen som kommer kräva mer stabila bränslen. Här är HVO en potentiell kandidat även om tillgång och mängd av insatsråvara är stora frågetecken.

En potentiell utveckling som kan öka bränsleflexibiliteten, mest lämpat för tyngre fordon såsom stridsfordon, är att ersätta dieselmotorn med en mindre gasturbin

146 Sustainable Aviation Fuel, biobränsle för flyg.

som sedan kopplas till ett hybridsystem. Allt detta har dock lång väg från utveckling till färdig produkt.

Det är inte enbart fordon inom Försvarsmakten som kommer kräva bränslen som kan lagras under lång tid utan detta gäller även i högsta grad elproducerande dieselaggregat till bergrum, sjukhus och andra kritiska funktioner. I sådana tillämpningar kan bränslet behöva lagras under mycket lång tid och här kan det visa sig att de dyrare processerna för elektrobränslen kommer att passa bättre då dessa kan ta fram mer stabila bränslemolekyler med längre lagringsbeständighet. Detta är dock en fråga som kommer behöva omfattande forskning och utveckling.

Ett annat specifikt exempel på områden där bio- och elektrobränslen kan ha svårt att möta kraven är för de fåtal tillämpningar som använder högspecialiserade fossila bränslen där det idag inte finns andra alternativ, såsom JP-10 i RBS 15.

Vad gäller produktionen av alternativa bränslen finns redan idag en omfattande sådan för RME och HVO, samt distribution av dessa till bensinstationer runtom i landet. För SAF är situationen en annan och den lilla kapacitet som finns kommer behöva byggas ut, samt att fler aktörer och framförallt fler insatsvaror behöver komma in i produktion. Produktionen av elektrobränslen är idag än mindre utbyggd än den för SAF och kan komma att spela en central roll för specifika applikationer såsom långtidslagrade bränslen.

### Vätgas

Även utvecklingen inom vätgasen drivs av den civila sidan, och även här kan Försvarsmakten komma att ha specifika krav. Även om vätgasen har en bra lagringsbeständighet så har den ofta problem med läckage, samtidigt som dess explosiva natur och krav på specifik infrastruktur förmodligen kommer att begränsa dess användning till ledningsplatser, energilagring i bergrum samt eventuellt som bränsle till bränsleceller.

En fördel med vätgas är dess möjlighet att produceras lokalt, med endast vatten som insatsvara och elektrisk energi. Det finns således en möjlighet till lokal produktion och konsumtion, och där det vid ett sådant läge inte heller kommer att ställas stora krav på långtidslagring då kedjan av produktion och konsumtion sker inom en kort tidrymd. Detta kräver dock god tillgång till elektrisk energi.

I sammanhanget är bränsleceller högst relevanta då de flesta bränslecellerna använder vätgas som bränsle.

### Metall

Metallförbränning är en teknik som inte ännu är kommersialiserad. Det bedrivs forskning vid ett antal universitet och högskolor, bland annat Eindhoven University of Technology (TU/e), McGill University och Lunds Tekniska Högskola.

Vid förbränning av metaller avges en stor mängd energi i form av värme som kan nyttjas för att driva en stirlingmotor eller ångturbin som i sin tur kan generera elektricitet. Förbränningen resulterar inte i några växthusgaser, men beroende på vilken media som metallen förbränns i produceras olika restprodukter. Metallen reagerar med syre och bildar metalloxid. Metalloxiden kan samlas upp och med hjälp av tillförsel av energi återställas till ren metall för att möjliggöra upprepad användning. Lagring av energi i metaller lämpar sig i huvudsak för användning till större anläggningar. Likt för vätgasen finns möjlighet till lokal produktion och konsumtion förutsatt att det från början har funnits ett lager av metall på platsen. Som nämnts ovan är det största hindret för denna teknik dess omogna tillstånd och avsaknad av infrastruktur. Elproducerande kraftverk som använder metallpulver kommer generellt sett att vara i större skala och med största sannolikhet inget som lämpar sig för mindre ledningsplatser eller liknande. Fördelar med metall är hög energitäthet, enkel hantering, enkel uppsamling av restprodukter (metalloxider, ofta i pulverform) och, som tidigare nämnts, inga utsläpp av växthusgaser. Om metallerna börjar brinna oönskat kan det dock vara svårt att släcka branden. Metallförbränning kan också använda en rad olika oxidatorer, från aluminium till vattenånga, och kommer att både kunna producera värme och användas för produktion av vätgas. Metallerna man i huvudsak fokuserar på för energilagring är järn och aluminium, två metaller som finns i enorm mängd på jorden. Nackdelar är att det är en komplex process som krävs för att bränna metallerna och det är förmodligen långt kvar tills kommersiella system har lanserats.

## Samverkande och förutsättande teknikområden

I takt med omställningen av energisystemet och införandet av smartare och mer flexibla elnät kommer beroendet av halvledare och kraftelektronik att öka, då många energisystem kopplas samman via just kraftelektronik. Kraftelektronik kommer sannolikt fortsätta utvecklas med lägre interna förluster.

EU har antagit en förordning om halvledare (EU 2023/1781), Chips ACT[147] med syfte att stärka unionens konkurrenskraft och innovationsförmåga inom området.

## Påverkan på militär förmåga

Energiförsörjning är en grundläggande komponent i militär förmåga. Det påverkar allt från operativ kapacitet till strategiska sårbarheter. För att upprätthålla en effektiv militär förmåga krävs robusta och flexibla energiförsörjningssystem, såväl som förmåga att hantera och skydda dessa system vid en eventuell konflikt. Nya typer av produktion, lagring, distribution och förbrukning av energi kan och kommer att ha en betydande roll för hur olika system och plattformar bör nyttjas men även i

147 European Chips Act - European Commission, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en.

större skala för hur olika förband och organisationer verkar i framtiden. Till exempel kan nya typer av verkanssystem nyttjas i högre grad som en följd av elektrifierade system, som laservapen eller HPM-vapen.[148] Fordon eller andra plattformar kan få en lägre signatur då man eventuellt inte behöver ha en förbränningsmotor för att försörja ledningssystem, sensorer eller andra energiförbrukare.

Med fler elektrifierade militära system ställs nya högre krav på energiförsörjningen. Förutom nya system som utvecklas kan befintliga system dra nytta av nya typer av energiförsörjningssystem, framförallt energilagringssystem. Med nya, mer effektiva eller energirika energilagringssystem kan befintlig utrustning nyttjas under längre tider och operationer kräver mindre logistik. Det är inte bara mer och mer energirika energilagringssystem som utvecklas utan även mer effektiva sätt att nyttja den lagrade energin på. Att nyttja den tillgängliga lagrade energin så effektivt som möjligt är alltid fördelaktigt. Mer effektiv lagring eller effektiv förbrukning kommer bidra till att behovet av transporter och distribution av bränsle och annan lagrad energi minskar.

Som tidigare nämnts kommer troligtvis flytande bränslen behövas även år 2050. För fossila bränslen har man tidigare haft synsättet att ett bränsle kan försörja en mängd olika system och plattformar. Detta synsätt kan behöva ändras när det blir fler och fler olika typer av bränslen som kan tillämpas, och där flera av dem dessutom eventuellt kan tillverkas lokalt.

Studier genomförs i dagsläget på att skapa batterier som har god möjlighet att prestera vid kalla klimat. För att ett batteri ska kunna prestera tillfredsställande behöver det kunna leverera en förväntad effekt och kapacitet men även kunna laddas inom rimliga tider, oavsett temperatur. Militära system som kan gynnas av förbättrad batteriprestanda i kallt klimat är allt från mindre soldatburna system till större fordon som stridsfordon. Det kalla klimatet påverkar inte bara batterier specifikt utan även flytande bränslen och andra former av energilagringstekniker. Nya flytande bränslen för militärt bruk behöver vara tåliga mot kyla.

Mot 2050 kommer det däremot fortfarande finnas kvar militära system som nyttjar dagens konventionella energisystem, samtidigt med ett fortlöpande skifte till materiel som nyttjar nyare energitekniker. Troligtvis kommer den totala energianvändningen vid 2050 vara högre än i dagsläget då ny teknik möjliggör nya användningsområden och förmågor.

Energiförsörjningen är ofta ett attraktivt mål för fienden. Genom att slå ut eller skada delar av energiförsörjningen påverkas den militära operativa förmågan avsevärt. Det är därför viktigt att skydda sin energiförsörjning men även utveckla den med fokus på robusthet och dessutom ha alternativa lösningar för att minska beroendet av traditionella energinätverk. Exempel på detta är att tillämpa ö-drift vid förhöjd kris och därmed kunna bli mer självförsörjande och ha en högre robusthet.

148 High Power Microwave, mikrovågsvapen i syfte att störa eller förstöra elektronik.

## Aktörer

I perspektivet 2050 kan man förvänta sig att ett stort urval av aktörer är involverade i utveckling och användning av energiförsörjningssystem. Området är mycket brett och innefattar en mängd olika användare och teknikområden. En utvecklingstrend kan vara att fler aktörer utvecklar och nyttjar miljövänliga och robusta energilösningar och energiproducenter som sneglar på ö-drift och mikronät. För Försvarsmakten är det av särskilt intresse att följa energiverksamhet som bedrivs inom Nato och EU, men även att dra lärdomar från hur andra försvarsmakter löser sina uppgifter kopplat till energiförsörjning.

## Lästips

Enström, J., m. fl., Omvärldsanalys - Energitekniker för ett framtida försvar, FOI-R--5606--SE, 2024.

Melin, T., m. fl., Energikällor, framdrivning och klimatneutralitet - Frågeställningar för Försvarsmaktens framtida flygsystem 2045, FOI Memo 7503, 2021.

Nykvist, B., m. fl., Klimatneutral Försvarsmakt - Analys av fossilfria vägval för försvarsgrenarna. Möjliga åtgärder på kort sikt, FOI-R--5201--SE, 2021.

Odell, A., m. fl., Russian attacks on the Ukrainian power system, FOI-R--5596--SE, 2024.

Oßwald, P., m. fl., Combustion kinetics of alternative jet fuels, Part-I: Experimental flow reactor study, Fuel, vol. 302, 2021.

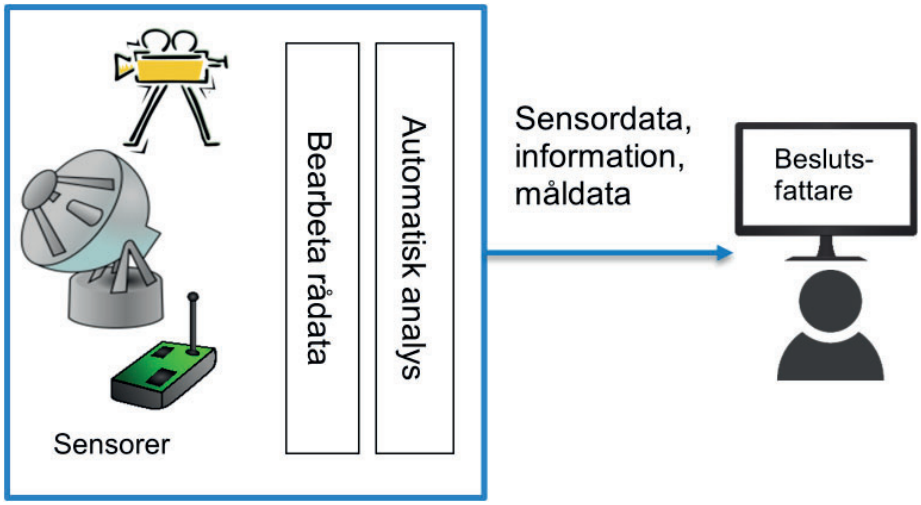
Sahlén, W., m. fl., Förstudie för FoT område Energiförsörjning, FOI-R--5705--SE, 2025.

# Sensorsystem

*Christina Grönwall*

## Inledande beskrivning

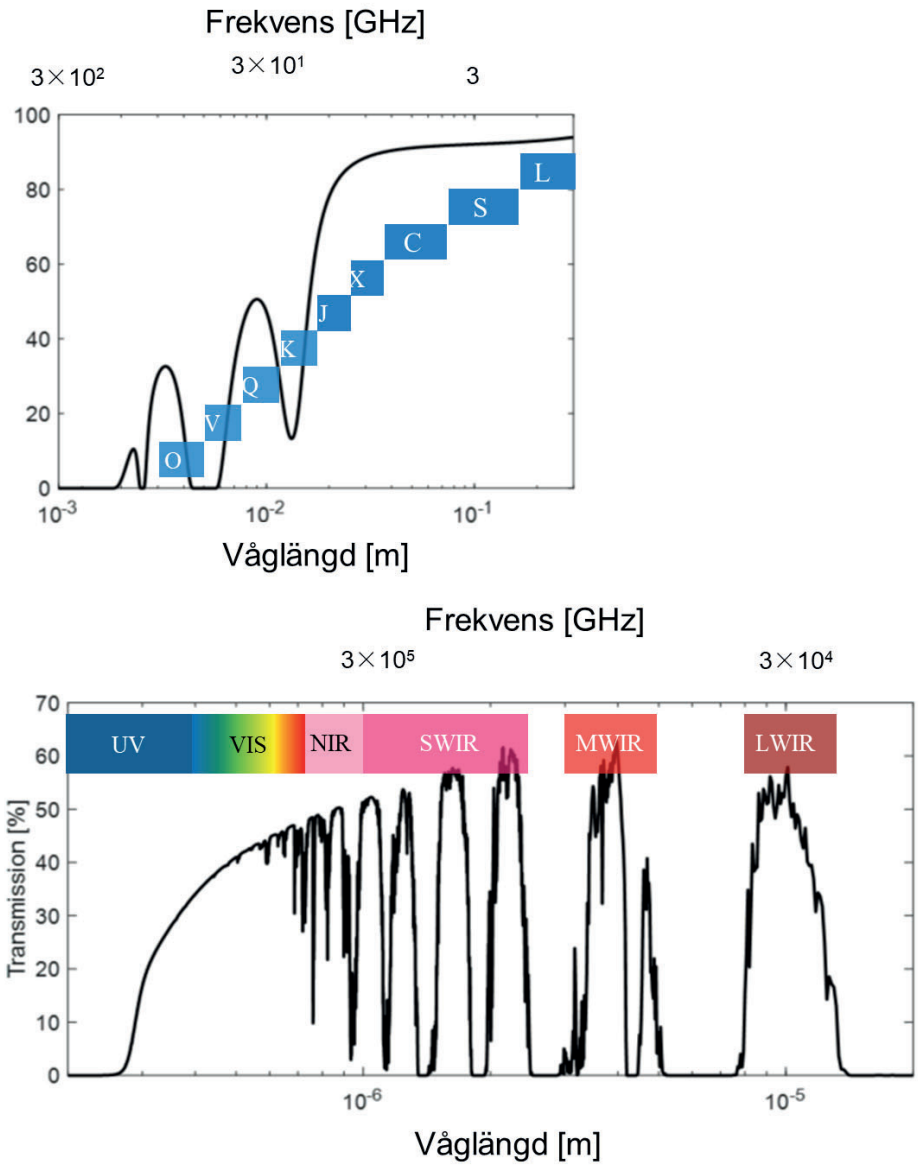
Detta kapitel fokuserar på sensorsystem inom radar, elektrooptik (EO) och infrarött (IR) som används på marken, över vattenytan, i luften och rymden. Ett sensorsystem består av en eller flera sensorer som mäter fenomen inom samma eller olika våglängds- eller frekvensområden. Dessutom ingår en enhet för bearbetning av rådata och någon nivå av automatisk analys av sensordata, se figur 4.




**Figur 4** Ett sensorsystem består av en eller flera sensorer, en enhet för bearbetning av rådata och någon nivå av automatisk analys.

Mängden sensorsystem ökar, både inom försvaret och i samhället i stort. De används i hela bekämpningscykeln, från underrättelseinhämtning till verkansverifiering. Data från sensorsystem är underlag för terrängbeskrivningar, navigeringsstöd, förarstöd, hinderdetektion och automatisk måligenkänning. Det finns idag sensorsystem för de flesta typer av plattformar, från handhållna sensorer och små drönare till stridsvagnar och satelliter. De kan fjärrmanövreras och ha automatiska funktioner. Både antalet typer och numerären av sensorsystem antas öka under prognosperioden. Sensorsystemen kommer oftare bestå av flera olika typer av sensorer, ha avancerad automatik eller vara autonoma. Ett exempel är IR-sensorer, som pga. sin storlek och kostnad tidigare endast fanns på fordon och i målsökare, och nu finns för små drönare, eldhandvapen och som soldatburna. Det finns sensorsystem utvecklade för bilindustrin, hemmalarm eller viltvård som har så bra prestanda att de kan användas för försvar och säkerhet. Figur 5 visar atmosfärens transmission för

olika sensorvåglängder. Där det är hög transmission finns idag sensorsystem eller så pågår FoU för att ta fram sensorsystem som kan utnyttja transmissionsfönstret.




**Figur 5** Atmosfärens transmission för radar (överst) och EO/IR (nederst), med angivna sensorband. (Hallberg m.fl., 2021). IR: infrarött (eng. *infra red*), UV: ultraviolett, VIS: visuellt, NIR: när-IR (eng. *near IR*), SWIR: kortvågs-IR (eng. *short wave IR*), MWIR: mellanvågs-IR (eng. *mid wave IR*), LWIR: långvågs-IR (eng. *long wave IR*).

## Trender och exempel

Trender är fortsatt ökad upplösning, miniatyrisering av sensorsystem, inbyggd elektronik för sensorstyrning och beräkningar, samt energieffektivisering. Under senare delen av prognostiden tillkommer ökat behov av störtålighet och störskydd, samt blandning av fiberoptik och elektronik för parallellisering av beräkningar och utläsning av sensordata.

En drivkraft för utvecklingen av sensorsystem är upptäckt av svåra mål, som döljer sig i sin omgivning, utnyttjar terrängskyl under rörelse eller är maskerade. Sensorsystem utvecklas nu för våglängdsområden där design och kravställning för signaturanpassning hittills varit lägre prioriterat. Exempel på sådana är de med multi-/hyperspektrala sensorer, kombinationer av radar och EO/IR, kombinationer av passiv och aktiv inmätning samt multistatiska mätkonfigurationer. Det är svårt att signaturanpassa sig mot sensorsystem som kan anpassa sin mätmetod i realtid.

En annan drivkraft är att kombinera data och information från sensorsystem med information om terräng och underrättelser för ett transparent slagfält. I detta ingår snabb överföring till rätt beslutsfattare, vilket i sin tur ställer krav på anpassade beslutsstödsystem hos mottagaren.

Sedan länge används flyg- och helikopterburna sensorsystem för spaning och övervakning. Genom miniatyriseringen kan även små drönare, markfarkoster och små satelliter utrustas med högkvalitativa sensorsystem.

Ett tekniksprång pågår på programvarusidan, vilket tillsammans med miniatyriseringen och strömsnåla beräkningsenheter innebär att stora datamängder kan tolkas och hanteras i nära realtid. Det möjliggör att automatisk analys av data i s.k. algoritmer för t.ex. måldetektion och igenkänning integreras i sensorsystemet. Algoritmerna innehåller helt eller delvis AI, främst maskininlärning.

Den civila marknaden driver på utvecklingen av publika, standardiserade gränssnitt mellan sensorsystem, tredje parts algoritmer och kommunikationssystem. Då behövs standardisering på låg logisk och fysisk nivå. Försvarsindustrin ligger efter den civila marknaden men initiativ som SOSA[149] och SAPIENT[150] visar att förändring är på gång. Standarder krävs för att enkelt kunna koppla ihop olika sensorsystem i nätverk. Syftet är att uppnå spanings- och övervakningssystem som kan kopplas ihop sömlöst. Standardisering är en förutsättning för datafusion, generering av lägesbilder och för ISTAR.[151] Den underlättar test av innovativa lösningar och

149 SOSA: Sensor open systems architecture, https://www.opengroup.org/sosa.

150 SAPIENT: Sensing for Asset Protection with Integrated Electronic Networked Technology, https://www.gov.uk/guidance/sapient-autonomous-sensor-system.

151 ISTAR is the process of integrating the intelligence process with surveillance, target acquisition and reconnaissance tasks in order to improve a commander's situational awareness and consequently their decision making Intelligence, surveillance, target acquisition, and reconnaissance - Wikipedia.

integration av ny teknik i befintliga materielsystem och förenklar även integrering av svenska myndigheters skräddarsydda algoritmer i Försvarsmaktens sensorsystem (s.k. GFE, eng. *government furnished equipment*). Standardiseringen kommer införas oavsett vad traditionell försvarsindustri önskar, för det underlättar innovationsarbete med slutanvändare och att snabbt anpassa materiel när svagheter identifierats.[152]

En annan trend är att modifiera befintliga sensorer för att få sensorsystem med nya egenskaper. Ett exempel är kameror med kiselbaserade detektorer som vanligen används inom det visuella området, där man med modifieringar av filter och kamerans inbyggda algoritmer kan utnyttja detektorns känslighet inom UV och NIR. Inom radarområdet används idag SDR (eng. *software defined radio*) för att bygga ihop små, kostnadseffektiva radarsensorer. En annan trend är så kallade passiva radarsystem där man separerar sändare och mottagare och utnyttjar befintliga signaler, till exempel digitala TV-sändningar, som sändare. Då kan sensorsystem användas mer flexibelt och anpassas till rådande situation.

Det utvecklas också nya sensorer som mäter flera typer av fysikaliska fenomen samtidigt. Inom EO/IR-området finns polarisationskänsliga sensorer, där ljusets polarisation underlättar upptäckt av mänskligt tillverkade objekt i en naturlig bakgrund. Hyperspektrala (HS) sensorer mäter i flera smala våglängdsintervall, ibland hundratals. Med ett HS-system erhålls ett ”spektralt fingeravtryck” som särskiljer mänskligt tillverkade objekt från naturliga material. Dessa två typer av sensorsystem finns kommersiellt och utvecklingen kommer främst att vara inom automatisk dataanalys. På radarsidan görs stora forsknings- och utvecklingssatsningar inom gruppantennteknik med *Active Electronically Scanned Array* (AESA). En AESA-radar består av flera elektriskt styrbara radarelement, till skillnad från mekanisk avskanning med en stor radardisk. Man kan rikta radarelementen utan att mekaniskt vrida själva radardisken, vilket ger möjlighet till snabbare avsökning. Under prognosperioden förväntas detta studeras av de nationer som har AESA-teknik.

## Särskilda delområden

Sensorsystem i korta våglängder inom IR, SWIR**,** är relativt nya och används än så länge mest för högprestandatillämpningar. I SWIR kan man utnyttja natthimlens strålning bättre än i NIR (traditionella bildförstärkare) och se genom dimma och rök. Inom SWIR-området finns ögonsäkra lasrar som kan bidra till belysning av scenen. Utvecklingen av SWIR-sensorer är inte lika snabb som i Vis/NIR-området och sensorerna kostar just nu 4-5 gånger mer än motsvarande i Vis/NIR-området. Intresse från bilindustrin och säkerhetsbranschen att använda SWIR-sensorsystem förväntas sänka priserna.

Eventkameran, även kallade neuromorfisk kamera, är en ny typ av sensor där varje pixel enskilt genererar information om förändringar i ljusintensitet. Jämfört med

152 Försvarsmaktens lärdomar från kriget i Ukraina, FM2023:2379-9, 2023.

konventionella kameror har de högre temporal upplösning, lägre latens, högre dynamiskt omfång, lägre bandbredd, samt lägre strömförbrukning. Snabba förlopp som mynningsflammor kan urskiljas och kameran kan användas i låglju förhållanden. Möjliga tillämpningar undersöks just nu i forskningssamarbeten inom EDA och Nato.

Det finns möjlighet att använda AESA-radar för flera uppgifter, dvs. som multifunktionsradar. Mycket arbete återstår vad gäller komponenter och programvara för styrning, men inom en tioårsperiod bör det finnas fullt styrbara radarantenner. Därefter kommer utvecklingen ske inom måligenkänning. En AESA-radar förväntas kunna användas smart, till exempel för samtidig avspaning och ”punktmarkering” (målföljning) av mål. Alternativ är samtidig spaning och telekrigsinsats eller samtidig spaning och kommunikation. Genom att anpassa utsända radarsignaler efter rådande förhållanden möjliggörs minskad risk för röjning. AESA-teknikens flexibilitet gör att radarsystemen även kan användas som syntetisk aperturradar (SAR) för markavbildning eller sjöövervakning och som väderradar. AESA-radarer studeras även för antidrönarsystem (C-UAS, eng. *counter umanned aerial systems*). Vad det innebär taktiskt att kunna styra en antenn på detta sätt är till stora delar outforskat.

En grupp av metoder för automatisk analys av sensordata samlas under begreppet ATR (*Automated or aided Target Recognition*), vilket avser automatisk analys av mål och omfattar algoritmer för upptäckt, klassificering, igenkänning, identifiering, samt teknisk analys av objekt.[153] Idag omfattar ATR-begreppet inte målföljning, men det kan ändras eftersom måldetektion och målföljning allt oftare görs samtidigt. Med ATR möjliggörs tidig upptäckt och karakterisering av hot för att få längsta möjliga tid för beslut om motåtgärder. I ATR jämförs sensordata med målbibliotek. Bibliotekets information om målet baseras på tidigare inmätningar, CAD-modeller eller från underrättelser. Fram mot 2050 kommer ATR utvecklas så att måldetektion är möjlig när det bara finns sensordata på delar av målet eller med ett sensorsystem i en närliggande våglängd eller frekvens. Måligenkänning är idag vanligt för bildalstrande EO/IR-sensorsystem.[154] Inom prognosperioden förväntas måligenkänning bli vanligt även på radarsidan och det är utvecklingen inom AESA- och SAR-teknikerna som möjliggör detta. Inom prognosperioden kommer också effektiva ATR-funktioner finnas i de flesta sikten och sensorsystem, från eldhandvapen till stora plattformar. Funktionerna leder till snabbare, robustare och noggrannare följning och igenkänning av mål.

I takt med utvecklingen av radarsystem ökar kraven på dess komponenter. Fotonik kan på avgörande vis ersätta viss elektronik, till exempel för att kunna integrera

153 FOI:s ATR-forskning använder definitioner enligt STANAG 3769, 2nd ed. ”Minimum resolved object sizes for imagery interpretation”, ibland med tillägg eller modifieringar. Definitionerna används även för icke-bildalstrande sensorer och för nätverk av distribuerade sensorer.

154 Näsström, F., m.fl. Automatisk detektion av markmål, FOI Memo 8663, 2024.

avancerad radarteknik på mindre plattformar med begränsad kraftförsörjning.[155] Fotonikradar omfattar typiskt fiberoptiska komponenter kopplade i nätverk så att olika signalbehandlingsfunktioner kan användas.[156] Potentiella fördelar är hög bandbredd, rak frekvenskarakteristik, låg transmissionsförlust, parallellisering av analog signalbehandling och immunitet mot elektromagnetisk interferens. För närvarande sker en snabb utveckling av fotoniskt integrerade kretsar (PIC, *photonic integrated circuit*), en teknik som förväntas få stor inverkan på både radar- och EO/IR-teknik.

Kvantsensorer är en annan mycket intressant teknik. Tyvärr begränsas mätavstånden idag av höga brusnivåer. Brusproblemet behöver lösas innan tekniken blir militärt intressant. Kvantsensorer beskrivs i kapitlet om kvantteknik.

Maskininlärning (ML) utvecklas för alla typer av sensorsystem. ML-algoritmer integreras idag i EO/IR-system inom Vis, Vis-NIR och LWIR. Civila exempel är åtelkameror och perimeterövervakning. Inom några år finns specialanpassade algoritmer även för HS-, SWIR- och 3D-data. Det pågår utveckling av specialanpassade ML-algoritmer för radardata med fasinformation (komplexa radardata).

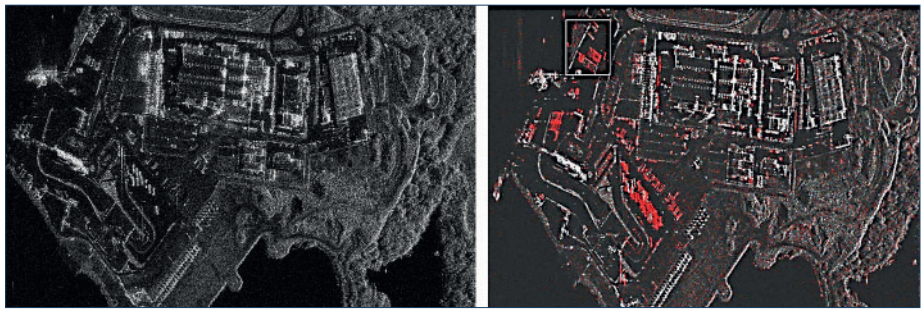
Utvecklingen av ML- och ATR-funktioner är datadriven, dvs. det krävs stora mängder (sensor)data för utveckling, test och verifiering. Datadrivna algoritmer förväntas användas 2050, med tanke på den stora mängd sensorsystem som förväntas finnas då, även om det med stor sannolikhet är andra algoritmer än de som används idag. Bäst prestanda uppnås när sensoranpassade algoritmer tränas på många exempel av varje mål i olika typer av bakgrund. Måldata behöver samlas i skyddade databaser. Det krävs systematik och infrastruktur för att vidmakthålla dessa databaser. Vid utveckling av ML- och ATR-funktioner behöver olika varianter av algoritmer testas på stora mängder sensordata. Detta kräver stora beräkningskluster. Förmodligen har Sverige före 2050 både egna beräkningskluster och databaser som är gemensamma med andra Natoländer.

En annan kraftfull metod för målupptäckt, som idag inte baseras på ML, är förändringsdetektion.[157] I förändringsdetektion analyseras skillnader mellan sensordata från olika tidpunkter. Förändringarnas karaktär analyseras för att avgöra vilka som ev. utgör mål. Förändringsdetektion har visat mycket goda resultat för sensordata insamlat med drönare, markfordon, flyg eller satelliter, se exempel i figur 6. Förändringsdetektion används idag av flera aktörer för att följa Rysslands förstörelse av Ukraina. Förändringsdetektion är en av nyckelteknikerna för att erhålla ett transparent slagfält.

155 Panda, S.S.S., m.fl., Recent advances and future directions of microwave photonic radars: a review, IEEE Sensors Journal, vol. 21, nr. 19, s. 21144-21158, 2021.

156 Yao, J., Microwave photonic system", Journal of Lightwave technology, vol. 40, nr. 20, s. 6595-6607, 2022.

157 Axelsson, M., m.fl., Förändringsdetektion ur ett sensorperspektiv, FOI Memo 8254, 2023.



**Figur 6** Förändringar i en hamn mellan två olika dagar, markerade med rött i den högra bilden. Automatisk analys av SAR-data från ett flygplansburet system (Sjögren m.fl., 2022).

## Samverkande och förutsättande teknikområden

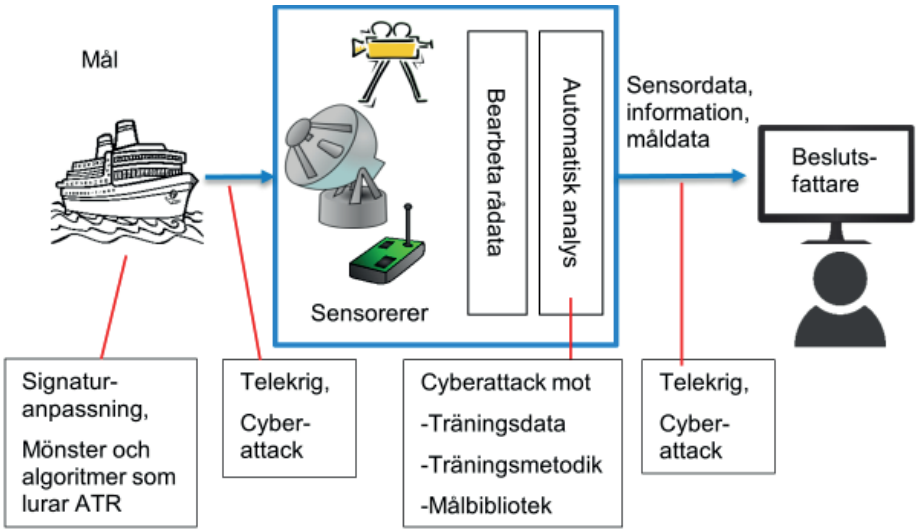
Ett förutsättande teknikområde för sensorsystem är halvledare. Tillverkningen av halvledare sker huvudsakligen i Asien där Taiwan är dominerande. De stora aktörerna har alla tillverkning i Asien vid sidan av USA och Europa. USA har en konkurrensmässig fördel i den globala halvledarindustrin då de i hög grad nyttjar amerikansk teknologi för design och tillverkning av halvledarchip.[158] USA har nyligen infört restriktioner mot kinesiska företag för överföring av avancerad teknologi och ställer dessutom krav på att EU och vissa länder i Asien förhindrar att de överför ny teknik till Kina.[159]

Det finns några teknikområden som utmanar sensorsystem. Till exempel är sensorsystem och signaturanpassning varandras motsatser. Grundläggande tekniker, systemlösningar och handhavande är i en ständig duell. Under flera år framöver förväntas sensorsystemen ha övertaget relativt signaturanpassningstekniken men inte nödvändigtvis mot en aktör som vet sin egensignatur och är skicklig på att hantera sin materiel.

En annan duell är den mellan sensorsystem och telekrig. Det kommer krävas att sensorsystem har störskydd och diagnossystem som detekterar störningar. Därefter behöver det störda sensorsystemet, tillsammans med ev. andra sensorsystem, kunna anpassas och kompensera för databortfallet. Två ytterligare dueller är de mellan sensorsystems algoritmer och tekniker för att lura algoritmer, samt mellan sensorsystem och cyberattacker. Dessa nya typer av hot behöver studeras mycket mer. Problemets omfattning illustreras i figur 7 nedan.

158 Paulander I., Khedri, M., Sammanfattning studie av kritiska delsystemsfunktioner för multifunktionssystem, FOI Memo 8546, 2024.

159 Weidacher Hsiung, m.fl., Strategic outlook 10, China as a global power, FOI-R--5620--SE, 2024.




**Figur 7** Illustration av hot mot sensorsystem.

## Påverkan på militär förmåga

Den ökande användningen av sensorsystem för ATR, lägesbild och ISTAR ger möjlighet till kortare tid från upptäckt till beslut om insats**.** Med anpassade sensorsystem kan man få tidigare förvarning även i mörker, rök och dimma. En skytt kan få specificerade mål markerade direkt i siktet. Nyligen insamlade sensordata kan parallellt genomsökas av ATR- och scenanalysalgoritmer. Då kan hypoteser avseende fiendens organisation, aktivitet och avsikt skapas snabbt. Till exempel om en samling fordon utgör en ledningsplats, en sjukvårdsplats eller en bränsledepå. Det finns algoritmer som automatiskt värderar kvaliteten i insamlade data. Om kvaliteten är låg rapporterar systemet att nya mätningar behöver göras. Då kan satelliten, flygplanet eller drönaren direkt fortsätta att samla in nya data utan att ett nytt uppdrag behöver planeras av en markorganisation.

Datadriven algoritmutveckling innebär att både beräkningskluster och sensordata blir värdefulla resurser som måste skyddas.

Teknikens landvinningar gör att frågor måste ställas om gränsen mellan automatik och människan. Vilka beslut är lämpliga att hantera med automatiska funktioner och vilka ska hanteras av människor? För att svara på detta behöver man koppla teknikens möjligheter mot DOTMLPFI[160], hur Sverige vill uppträda och krigets lagar.

Den tekniska utvecklingen påverkar försvars- och säkerhetspolitiken långsiktigt, eftersom den möjliggör alltmer autonoma sensorsystem. Den globala utvecklingen och spridningen av sensorsystem innebär att många, även fienden, får tillgång till

160 Doktrin, organisation, träning, materiel, ledarskap och utbildning, personal, faciliteter, interoperabilitet.

dem. Man måste anta att fienden också använder tekniken för att korta sin tid för beslut om insats.

I vissa framtidsscenarier tror man att krig i större utsträckning utspelas i städer med miljontals invånare och skyskrapor. Exempel skulle kunna vara fredsframtvingande insats i Ukraina eller stöd till Taiwan. Storstäder av den typen ställer delvis andra krav på sensorsystem och automatisk sensordataanalys.

## Aktörer

Forskning och utveckling av sensorsystem sker internationellt på universitet, institut och företag. Det är civila behov som driver utvecklingen. Exempel på civila branscher som har militärt intressanta tillämpningar är fordonsindustrin och säkerhetsbranschen. Stora aktörer inom sensorsystem är EU, Natoländer och Kina. USA leder utvecklingen och har kraftiga exportrestriktioner för sensorsystem med spetsprestanda.

För svenskt vidkommande behöver man säkra tillgången till tillräckligt bra mörkersensorer för Försvarsmaktens (och blåljusmyndigheternas) behov. Svenskt deltagande i internationella samarbeten är nödvändigt för att få kunskap om hur man kan utnyttja nya sensorförmågor, liksom för att bedöma utvecklingen av hotsensorers prestanda och utveckla skyddstekniker (s.k. *sensor denial*).

Den omfattande sensorforskning som bedrivs i Kina innebär oförutsägbar spridning av ny teknologi. Den globala spridningen av sensorsystem gör att kvaliteten på hotsensorer inte beror på en aktörs teknikmognad, utan på dennes möjligheter att få tillgång till förmågan. Utvecklingen inom data- och informationsbehandling innebär att tekniskt komplexa sensorsystem kan vara relativt lättanvända och leverera lättolkad information. Det möjliggör för proxy-aktörer och organiserad brottslighet att med god förmåga kunna använda avancerade, militära sensorsystem.

## Lästips

Axelsson, M., m.fl., Förändringsdetektion ur ett sensorperspektiv, FOI Memo 8254, 2023.

Försvarsmaktens lärdomar från kriget i Ukraina, FM2023:2379-9, 2023.

Hallberg, T., m.fl., Signaturanpassning och sensorprestanda, FOI Memo 7637, 2021.

Näsström, F., m.fl. Automatisk detektion av markmål, FOI Memo 8663, 2024.

Panda, S.S.S., m.fl., Recent advances and future directions of microwave photonic radars: a review, IEEE Sensors Journal, vol. 21, nr. 19, s. 21144-21158, 2021.

Paulander I., Khedri, M., Sammanfattning studie av kritiska delsystemsfunktioner för multifunktionssystem, FOI Memo 8546, 2024.

Sjögren, T.K., m.fl., Change detection for monostatic pursuit SAR GMTI- Theories and experimental results, IEEE Tr. Geoscience and Remote Sensing, vol. 60, s.1-14, 2022.

Weidacher Hsiung, m.fl., Strategic outlook 10, China as a global power, FOI-R--5620--SE, 2024.

Yao, J., Microwave photonic system, Journal of Lightwave technology, vol. 40, nr. 20, s. 6595-6607, 2022.

# Signaturanpassning

*Hans Kariis*

## Inledande beskrivning

Signaturanpassningsteknik (SAT, *signature management*, *stealth*) handlar om metoder för att minska kontrasten mellan ett objekt och bakgrunden ur alla aspekter som kan detekteras av sensorer. SAT brukar sorteras under begreppet vilseledning och 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 används för att upptäcka objekt. Tekniskt sett handlar det främst 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 (marina tillämpningar som fartyg och ubåtar) eller andra emissioner eller spår som någon sensor detekterar.

SAT är ett övergripande systemområde där det är viktigt att ha kunskap om hela kedjan där hotsensorer, miljö, maskeringssystem, formgivning och materialegenskaper finns med.

Dimensionerande för behovet av signaturanpassning är kapaciteten hos de sensorer som används 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.

Sannolikheten för konflikt med kvalificerade motståndare har ökat. En sådan motståndare har tillgång till avancerade sensorer varför betydelsen av signaturanpassningsteknik ökar.

Signaturer, i betydelsen igenkänning av militära enheter, har länge varit en viktig parameter i militära duellsituationer, såväl på land som till sjöss och i luften. Att kunna kontrollera sin signatur är en förmåga som kan öka chansen till överlevnad.

Fram till första världskriget låg fokus på att markera tillhörighet; för att undvika vådabekämpning på slagfältet var till exempel nationstillhörighet tydligt markerad med starka färger.

Kamouflage, att minimera signaturen för att inte upptäckas, blev prioriterat i samband med första världskriget då gröna, grå och beigea färger började dominera soldaternas uniformer. Dåtidens kamouflage var endast avsett att ha effekt mot

mänskliga observatörer under dagtid. Först med utvecklingen av mer avancerade tekniska sensorer uppkom behovet av multispektralt kamouflage.

Försvarsmaktens fältuniformer var fram till 1990 enfärgade, men med M/90 kom mönster i fyra färger som gav ytterligare frihetsgrader att smälta in i bakgrunden. Det svenska mönstret består, till skillnad från de flesta andra länders, av tämligen stora enfärgade fält, i samma storleksordning som löv på träd. För lägre signatur vintertid kan Snödräkt 90 nyttjas som skyddsplagg. Då fältuniform 90 utvecklades var den dimensionerande motståndaren fortfarande en tekniskt högt kvalificerad stormakt och det tänkta operationsområdet var Sverige.

För flygplan och fartyg är signaturen som uppvisas mot radarsensorer av avgörande betydelse. På 1970-talet började man intressera sig för metoder att reducera radarmålarean för plattformar. Detta kan göras genom en geometrisk utformning som reflekterar bort strålningen från mottagaren, genom val av material som absorberar radarstrålningen eller en kombination av dessa.

Sverige är en viktig aktör på området och en eftertraktad partner i internationella samarbeten. De svenska Visbykorvetterna var tidiga exempel på smygfartyg, som sedan de först sjösattes 2000 har inspirerat andra länder att utveckla liknande koncept. Alltsedan kalla kriget har teknik och taktik för signaturanpassning utvecklats i nära samarbete mellan Försvarsmakten, FOI, FMV och försvarsindustrin, vilket visat sig vara ett framgångsrikt arbetssätt.

## Trender och exempel

I dagens konflikter, bland annat i Ukraina, syns tydligt att slagfältet blir alltmer transparent, vilket innebär att man måste anta att alla objekt och rörelser på slagfältet är kända för alla aktörer. Det möjliggörs bland annat av en mångfald små, billiga drönare försedda med små och billiga men ändå högpresterande sensorer. Även satelliter och lokalbefolkningens medvetna eller omedvetna avslöjanden av militär aktivitet i sociala media bidrar till det transparenta slagfältet. Positionering av mobiltelefoner och annan personlig utrustning, som smartklockor, bidrar till lägesbilden.

Denna trend förväntas fortsätta fram till 2050 med ett accelererande antal sensorer som bevakar alla dimensioner av slagfältet. En utmaning är att kunna sammanställa en stor mängd data med olika format och presentera det för beslutsfattare. I framtiden kan AI-baserade verktyg för insamling och sammanställning av information förväntas spela en större roll. Förändringsdetektion, mönsterigenkänning, fusion av data från flera sensortyper och automatisk spårning av rörliga objekt kan snabbt ge motståndaren en sammanslagen bild av slagfältet vilket skapar nya utmaningar för vår signaturanpassning.

Den operationsmiljö där våra framtida förband ska verka kan bli bredare än traditionell svensk terräng. Militärgeografin i norra och östra Europa är tämligen lik den i Sverige även om en större andel öppna fält, mindre andel skog och tätare placerad bebyggelse kan förväntas. Terrängtyper som berg, öken och djungel kan förväntas prioriteras ner.

Tidsaspekterna i OODA-loopen (observera (O), orientera (O), besluta (D) och handla (A)) blir kortare med tiden allteftersom sensor- och ledningssystem utvecklas. I en duellsituation innebär det att det blir än viktigare att upptäcka motståndaren innan man själv blir upptäckt. Detta kan åstadkommas med bättre sensorer och/eller bättre signaturanpassning.

Den dominerande hotriktningen ändras från horisontell till vertikal. Detta då drönare blir en allt viktigare del av spaningen. Flygplan dyker alltid upp först vid horisonten för att, när de närmar sig, visa sig vid högre aspektvinklar. Små drönare däremot kan upptäckas rakt ovanför våra förband utan föregående varning. Framtidens signaturanpassning måste erbjuda skydd i alla hotriktningar då små drönare kan dyka upp var som helst medan satelliter även i framtiden kommer att vara viktiga för långräckviddig spaning.

Nya sensorteknologier dyker upp i utvecklingslabb och något senare på slagfältet. Signaturanpassningens utveckling måste anpassas till eller ännu hellre föregå dessa. Inom det optiska området utvecklas sensorer känsliga i våglängder där det tidigare inte funnits något hot, såsom *Short Wave Infra Red* (SWIR, 1.1 - 2.5 μm). Signaturanpassningen och vilseledningen måste anpassas både till de metoder som används för att bära och förflytta sensorer och till sensorernas egna tekniska prestanda.

Om man ställs mot en motståndare som använder AI-baserade metoder för måluppträckt och målidentifiering ställer det högre krav på signaturanpassning, men kan också ge nya möjligheter att vilseleda en motståndare. Om målidentifieringsalgoritmerna är kända kan man genom små modifieringar av ett objekts utseende förmå AI-algoritmen att tolka det som något helt annat, till exempel en panda.[161] Detta kan göras genom att lägga på ett s.k. adversiellt mönster på det objekt som ska skyddas. Mönstret kan se ut som brus eller vara helt osynligt för blotta ögat men motståndarens AI-algoritm tolkar det som något annat.

Med automatiserad förändringsdetektion kan tillkomna eller flyttade objekt hittas om samma område genomsöks vid olika tidpunkter. Datainsamlingen kan ske obemärkt från satellit eller från drönare.

161 Claudia Hübner, Alexander Schwegmann, Developing dual attribute adversarial camouflage patterns for counter-AI reconnaissance, Proceedings Volume 13199, Target and Background Signatures X: Traditional Methods and Artificial Intelligence; 1319902 (2024) https://doi.org/10.1117/12.3033819.

De nya sensortrenderna kan motverkas med mer avancerad VSS (Vilseledning, Signaturanpassning, Skenåtgärder), tre begrepp som hänger ihop och kan komplettera varandra.

En annan trend är att hållbarhets- och miljöaspekter kommer in i design av militär materiel, inklusive signaturanpassningsmateriel. Till exempel tittar man på växtbaserade material för maskering.

## Särskilda delområden

### Spektral design

En kombination av material och struktur (metamaterial) kan användas för att skräddarsy en ytas reflektans över ett visst våglängdsområde. Dessa material får skenbara egenskaper utifrån sin struktur, ofta egenskaper som naturliga material inte kan ha. En tillämpning är när man vill styra emission av IR-strålning till våglängdsintervall där hotsensorer inte förekommer, såsom 3-8 µm. I detta spektralområde är inte atmosfären transparent så sensorer skulle vara oanvändbara på avstånd längre än några meter. Eftersom det är en fysikalisk begränsning kommer det att förbli så även efter 2050. Spektralt designade färger och textilbaserade kamouflagesystem finns på hög TRL-nivå och förväntas vara operativa i god tid före 2050. Redan idag finns teknik för att i laboratoriet tillverka små spektralt designade ytor. Tidsaspekten för uppskalning till hela operativa plattformar är bara en fråga om tillförda resurser.

### Adaptivt kamouflage

Kamouflage vars egenskaper kan förändras behövs för att bibehålla en låg signatur vid förändring i bakgrund, väder, ljusförhållanden eller hotbild. Mycket forskning och utveckling sker för att få fram adaptiva kamouflagesystem som i realtid kan ändra färg, mönster, termisk emission eller radarreflektion, men ännu finns inga operativa system. Exempel på utveckling sker inom EDF-projektet ACROSS och inom NATO STO. Målet med dessa verksamheter är att ha färdiga adaptiva system före 2050.

Vid implementering av adaptivt kamouflage måste hänsyn tas till folkrättsliga aspekter. Det är till exempel inte tillåtet att anpassa signaturen hos ett militärt objekt så att det uppfattas som ett civilt objekt. Däremot är det helt legitimt att anpassa signaturen till bakgrunden så att objektet inte alls syns. Det är också tillåtet att förvilla motståndaren genom att få ett högvärdigt militärt objekt, till exempel en stridsvagn, att likna ett militärt objekt av mindre värde, såsom en lastbil.

### Biomimetik

Kamouflage som förekommer hos djur eller växter kan kopieras eller inspirera till militär signaturanpassning. Exempel är bläckfiskar, skalbaggar, påfåglar och kameleonter. Sådant biologiskt kamouflage studeras nu i det elektrooptiska området med målsättning att efterlikna och modifiera materialen för att uppnå bättre skydd mot nya sensortyper. Inom begreppet biomimetik ryms även biologiska material som kan modifieras eller tillverkas i strukturer så att nya förmågor uppnås. Ett exempel är att nyttja cellulosa (från träd) till att framställa extremt värmeisolerande material för IR-signaturanpassning.

### Skenmål

I de fall ett objekt inte går att helt dölja kan motståndaren vilseledas genom användning av skenmål. Dessa är billiga objekt som efterliknar de verkliga målen och kan mätta motståndarens sensor- eller verkanssystem. Skenmål har demonstrerats för både mark-, sjö- och luftbaserade objekt, se figur 8. I flygfallet används sedan länge remsor och facklor för att skydda flygfarkoster mot radar- respektive värmesökande robotar. Detta benämns traditionellt som telekrigsåtgärder i svensk terminologi, men skulle också kunna betraktas som skenmål.

**Figur 8** Exempel på skenmål. Den högra bilden visar exempel på fackelfällning från en flygande plattform.

I framtiden förväntas en ökad användning av skenmål och en intensifierad duell mellan sensorsystem och signaturanpassningsteknik. AI kommer att kunna användas både på sensorsidan för automatisk målidentifiering och på signatursidan genom anpassning av skenmåls utseende och taktiska uppträdande så att de blir mer lika det verkliga objektet.

### Vattendimma

Rök har sedan länge använts för att dölja militära objekt eller aktiviteter. Ett mer miljö- och hälsovänligt alternativ är finfördelad vattendimma, som har visat sig ha goda egenskaper mot flera sensortyper.

## Samverkande och förutsättande 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 förmåga att detektera låg-signaturmål eller hitta maskerade mål i en komplex bakgrund.

SAT kopplar till plattformsområdena för mark, sjö, luft, rymd och soldat. Internationellt pratar man om *integrated survivability* som 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 anpassning i efterhand.

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 plattformssignatur 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. Ett helhetsgrepp bör i framtiden tas på en plattforms skydd och möjlighet till verkan där aspekter som ballistiskt skydd, signaturanpassning, vilseledning, vikt och rörlighet, energiförbrukning och ammunitionshantering kommer in.

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.

## Påverkan på militär förmåga

Signaturanpassning betraktas i första hand som en del i skyddet av våra plattformar och ger därmed förbättrad överlevnad. Förmågan till signaturanpassning måste ständigt utvecklas för att möta utvecklingen av nya och förbättrade sensorsystem.

I kombination med sensorer bidrar signaturanpassning till ett informationsövertag. En sensorbärande plattform med låg signatur kan komma närmare målet som ska observeras vilket ger oss bättre underrättelser. Lägre signatur kan bidra till kortare stridsavstånd genom att en verkansplattform kan komma närmare målet innan eld öppnas vilket ger större sannolikhet att framgångsrikt bekämpa målet.

Taktiskt kan detta sammanfattas: Se men inte synas. Duellen mellan sensor och signatur kan också komma att påverka stridsavstånd och avstånd mellan logistikhubbar

och frontlinjen. Vi ser i Ukraina hur drönares ökande räckvidd tvingar motståndaren att flytta sin logistik bakåt.

God signaturanpassning kan ge bibehållen skyddsnivå med lägre vikt vilket i sin tur kan ge plattformen ökad rörlighet. Detta är särskilt tydligt för avsuttna soldater men är relevant även för markfordon och flygande system.

Genom att kombinera god signaturanpassning på våra plattformar med skenmål, som har något högre signatur än den äkta plattformen, kan en ökad skyddsnivå uppnås även för plattformar som är omöjliga att helt dölja. Skenmål kan även användas för att mätta motståndarens system.

## Aktörer

I Sverige har berörda myndigheter (FM, FMV, FOI, FortV, FHS) ett gott samarbete. Området är kringgärdat av en viss sekretess, men inte så stor att samverkan omöjliggörs.

Viktiga statliga aktörer, som Sverige har ett samarbete med, är:

- Nederländerna (TNO)
- Tyskland (Bundeswehr WTD 52, Fraunhofer IOSB)
- Storbritannien (dstl)
- Tjeckien (VVU)
- Portugal (Cinamil)
- Schweiz (armasuisse)
- Frankrike (Onera, DGA)
- Norge (FFI)
- Finland (FDRA)

Även USA, Ryssland och Kina utvecklar signaturanpassnings- och vilseledningsmateriel men uppgifter i öppna källor är knapphändiga.

Viktiga samarbetsorgan är:

- EU (EDA, EDF)
- Natos organisation för forskning och utveckling (*Science and Technology Organization*, STO)

Viktiga industriaktörer är:

- Sverige (Saab Barracuda, BAE systems, Mimicrys, Saab Kockums m.fl.)

- Tyskland (Rheinmetall, Krauss Maffei m.fl.)
- Storbritannien (QinetiQ, Malvern Optical m.fl.)
- Tjeckien (Inflatech m.fl.)
- Portugal (Citeve m.fl.)
- Schweiz (SSZ)
- Israel (Fibrotex)
- Frankrike (Safran, Thales)
- Norge (Kongsberg)
- Polen (Miranda)
- Grekland (Intermat)
- USA (i2k Defense tillverkar skenmål)
- Kina (Hangzhou Gauss, Shape inflatable Manufacturing, InflWuxi Xibang)

Samverkan inom Sverige:

- Akademisk samverkan med universitet och högskolor sker främst inom optik och materialforskning på låg TRL-nivå.

Samverkan kring frågor rörande materielanskaffning sker mellan statliga aktörer på området, såsom Försvarsmakten, FMV, FOI, FHS, FortV. Samverkan, i den mån LOU tillåter, sker även med svensk industri (Saab Barracuda är en stor internationell aktör).

## Lästips

FOI orienterar om Sensorer, 2004.

Pieter A. Jacobs, Thermal Infrared Characterization of Ground Targets and Backgrounds (ISBN 0-8194-6082-6).

Tim Newark, Camouflage (Thames and Hudson Ltd (February 2, 2009, ISBN 0500287104).

Arméstudie överlevnad MARK192004S, FM 2024.

Fördjupade lärdomar och erfarenheter från kriget i Ukraina av Försvarsmakten på uppdrag av Regeringen, utgiven 27 juni 2024.

Claudia Hübner, Alexander Schwegmann, Developing dual attribute adversarial camouflage patterns for counter-AI reconnaissance, Proceedings Volume 13199, Target and Background Signatures X: Traditional Methods and Artificial Intelligence; 1319902 (2024) https://doi.org/10.1117/12.3033819.

Åkerlind, Christina, Optical Studies of Bio-inspired Materials for Camouflage, Doctoral thesis, 2020, ISSN 0345-7524 ; 2069, Linköping University, Department of Physics, Chemistry and Biology, Thin Film Physics, Faculty of Science & Engineering.

Jennifer Silander, Hans Kariis, Linnea Åberg, Optical and thermal properties of carboxymethylated cellulose aerogels, SPIE Security + Defence (ESI25D), 2025, Paper No. 13673-8.

Försvarsmaktens lärdomar från kriget i Ukraina, FM2023:2379-9.

Jouni Rantakokko Jonas Nygårds, Obemannade farkoster för markstriden - erfarenheter från Ukraina, FOI-R--5723--SE, 2025.

# HPM (High Power Microwave)

*Tomas Hurtig och Mattias Elfsberg*

## Inledande beskrivning

I detta kapitel beskrivs offensiv teknik inom området mikrovågsvapen (eng. *High Power Microwave, HPM*). Ett HPM-vapen skickar ut mycket kraftiga, men kortvariga, pulser i ett pulståg. Toppeffekten kan vara mycket hög, upp mot gigawatt, men medeleffekten är låg. HPM-pulser kan temporärt eller permanent försätta målelektronik ur funktion. Inom HPM-forskningen studeras hur HPM-strålning kan genereras, hur den verkar mot olika typer av elektroniska komponenter och utrustningar samt hur man provar och skyddar utrustning och samhällssystem mot denna typ av elektromagnetisk påverkan.

Mikrovågsvapen möjliggör permanent fysisk förstörelse av elektronisk utrustning. Dessutom finns möjligheten att störa/förstöra även icke kommunicerande elektroniska system genom inkoppling av energi via kablage eller direkt in på kretskort och halvledarkomponenter, så kallad bakvägskoppling. Framvägskoppling är endast aktuell för kommunicerande målobjekt och innebär att energin kopplas in via systemets antenn. Framvägskoppling kan indelas i inombands- och utombandskoppling beroende på om HPM-pulsens frekvens överensstämmer med målsystemets kommunikationsfrekvens (inomband) eller inte (utomband).

Traditionellt bygger de kraftigaste HPM-vapnen på elektronrörsteknik då denna möjliggör generering av mycket höga toppeffekter i relativt kompakt format. Den snabba utvecklingen av transistorer för radarindustrin och digitalt styrda gruppantenner, AESA (eng. *Actively Electronically Scanned Array*), har dock möjliggjort HPM-vapen baserade på halvledarförstärkare.

Det faktum att HPM-tekniken blivit operativ innebär att man börjat kravställa militär materiel med avseende på HPM-hotet.[162] Detta innebär i sin tur att det pågår ett intensivt arbete på flera håll i världen (inklusive Sverige) med att ta fram metoder för att prova elektronisk materiels tålighet mot HPM-bestrålning.

Rysslands invasion av Ukraina har visat att användningen av relativt billiga drönare, även civila sådana, fyller flera mycket viktiga funktioner på båda sidor. De används bland annat för spaning, eldinriktning och direkta attacker. Så länge drönarna flyger med hjälp av pilot och/eller satellitbaserade navigations- och positionsbestämningssystem (GNSS, eng. *Global Navigation Satellite Systems*) går de ofta att bekämpa med telekrigsåtgärder. Redan nu kan dock relativt enkla modeller navigera på geografisk information eller med tröghetsnavigering och blir då betydligt

162 MIL-STD-464C, Department of Defense Interface Standard, Electromagnetic Environmental Effects Require-ments for Systems.

mer svårbekämpade. I Ukraina har man även sett ryska drönare som är styrda via fiber.[163] Det har visat sig att ett effektivt sätt att bekämpa enklare drönare är att använda HPM. Mikrovågseffekten är så pass hög att den effekt som kopplar in i drönarens elektronik via kablar, kretskort och/eller antenner blir så kraftig att elektroniken slutar fungera och drönaren därigenom störtar. Ytterligare fördelar med HPM-vapen är att varje salva är billig, magasinet djupt (så länge det finns elektrisk energi att tillgå fungerar vapnet) och att HPM-vapnet inte behöver riktas in lika noga som till exempel ett kinetiskt vapen eller ett laservapen.

## Trender och exempel

Då militär elektronik kan vara väl skärmad och då HPM-tålighet börjar bli en del av kravställningen vid anskaffning av ny materiel skall man nog inte förvänta sig att HPM-vapen kommer 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, det vill säga där mikrovågsenergin kopplar in i elektroniken via antenner eller sensorer. Även externa sensorer som till exempel kameror, radar och IR-sensorer kan tänkas vara sårbara.

Den starkaste utvecklingstrenden är dock anpassningen av HPM-vapen för att bekämpa mindre drönare (eng. *Counter Unmanned Aerial System*, C-UAS). Många enklare drönare kan naturligtvis bekämpas genom störning av GNSS och/eller störning av kommunikation mellan pilot och drönare. Den mycket snabba utvecklingen av små drönare gör dock att de numera kan flyga på geografisk information eller med hjälp av tröghetsnavigering och alltså inte behöver pilot eller GNSS för att uppfylla sitt uppdrag. Då mikrovågsstrålning alltid utbreder sig i en lob gör det att ett HPM-vapen inte behöver riktas in lika noga som till exempel ett kinetiskt vapen eller ett laservapen. Detta gör det även möjligt att bekämpa en hel eller delar av en svärm utan att behöva rikta om strålningen mot varje enskild individ i svärmen. Det stora behovet av att finna praktiska och ekonomiskt försvarbara sätt att bekämpa drönare har gjort att intresset för HPM-vapen ökat dramatiskt under de senaste åren. När dessa vapen väl kommer ut på förband kommer säkert fler användningsområden upptäckas och behovet av att HPM-härda militär utrustning kommer att öka.

Flera aktörer har tagit fram HPM-system specifikt för bekämpning av små drönare. Bland dessa finns också system som bygger på halvledarförstärkare och gruppantennteknik (AESA). Det är långt kvar innan ett halvledarbaserat system kan generera lika höga toppeffekter som ett elektronrörsbaserat system. Det kommer att dröja åtminstone fem-tio år. Tekniken medför dock många andra fördelar.

163 Russian Fiber Optic Drone Beats Any Jammer (UPDATE: Ukraine Version), https://www.forbes.com/sites/davidhambling/2024/03/08/russian-fiber-optic-drone-can-beat-any-jammer/.

Bland dessa kan nämnas möjligheten att skicka ut pulser med olika frekvens, att rikta strålningen utan att behöva vrida antennen mekaniskt, att skicka pulser med olika pulslängd och olika avstånd i tiden mellan pulser. En ytterligare fördel är att vapnet är helt mjukvarustyrt vilket förenklar integration med annan utrustning som kan finnas i närheten, till exempel radar, telekrigsutrustning och kommunikationsutrustning.

En ytterligare trend är att vissa forskargrupper studerar HPM-vapen för högre frekvenser än vad som är brukligt inom området. De flesta HPM-system genererar strålning någonstans i L- eller S-bandet (1-2 GHz eller 2-4 GHz). Sedan några år tillbaka publiceras dock fler och fler studier av mycket kraftiga strålkällor i X-band (8-12 GHz).[164] Anledningen är inte helt klar men det skulle kunna vara för att det är svårare att skärma mot högre frekvenser och att en kort våglängd kopplar effektivt till små elektriska strukturer.

## Särskilda delområden

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 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. Detta är mycket svårt att realisera med traditionell HPM-teknik som bygger på elektronrör men relativt enkelt om HPM-systemet bygger på halvledarbaserade förstärkare som i ett AESA-system.

För utvecklingen av halvledarbaserade AESA-system är naturligtvis utvecklingen av transistorer till förstärkarna av avgörande betydelse. Radar- och kommunikationsindustrin driver än så länge denna utveckling och användandet av galliumnitrid på kiselkarbid (GaN-SiC) har möjliggjort den snabba ökningen av uteffekt för radarsystem baserade på AESA-teknik. Transistorer för radartillämpningar utvecklas dock mot en kravspecifikation där medeleffekten är ganska hög i jämförelse med toppeffekten, ofta runt 10 %. Detta är inte nödvändigt om transistorn ska användas för HPM-ändamål. För ett HPM-vapen är toppeffekten mycket viktigare än medeleffekten och 0.1-1 % är fullt tillräckligt. En radartransistor utvecklas också för att kunna vara i bruk dygnet runt i flera års tid medan en transistor för HPM-bruk är en del av ett vapen som används då och då och troligen bara under relativt korta tidsperioder. Dessa skillnader i kravställningen gör att det finns en stor potential att öka toppeffekten från AESA-baserade HPM-vapen om och när transistortillverkarna anser det värt att satsa på denna, för dem, nya marknad.

164 Fanzheng Zeng, et al., Investigation of an X-band Cerenkov-type high power microwave oscillator driven by sheet electron beam, AIP Advances, Maj 03, 2021, https://doi.org/10.1063/5.0046206.

En ytterligare ökning av uteffekten från transistorer skulle möjliggöras av helt nya halvledarmaterial. Diamant skulle erbjuda enorma fördelar både med avseende på toppeffekt och medeleffekt då det tål 50 gånger så höga elektriska fält och har 15 gånger högre värmeledningsförmåga jämfört med kisel.[165] Det pågår intensiv forskning kring diamant i dioder och transistorer runt om i världen men ännu finns inga kommersiellt tillgängliga komponenter.

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 plattformsintegrering för fler, och mindre, plattformar och i fler taktiska situationer. Långa pulsserier ökar möjligheterna att täcka ett brett frekvensområde med flera smalbandiga pulser av olika frekvens.

De närmaste tio-femton åren kommer säkert elektronrörstekniken finnas kvar och vidareutvecklas då den erbjuder mycket höga uteffekter i relativt kompakt format. Nya magnetiska material gör att det numera är möjligt att använda permanentmagneter för många olika typer av HPM-strålkällor som bygger på elektronrörsteknik. Fortsatt utveckling av dessa material kan möjliggöra mindre och lättare magnetsystem. Utveckling av material som tål höga elektriska fältstyrkor är ett annat område som har stor betydelse för hur kompakt strålkällan kan bli. I många elektronrör för de högsta uteffekterna slits katoden fort och det begränsar antalet pulser som kan genereras innan förslitningen gör strålkällan obrukbar. Även på detta område är materialutveckling en viktig framgångsfaktor.

## Samverkande och förutsättande teknikområden

Av naturliga skäl ställer användandet av HPM vissa krav på egen utrustning då den behöver vara väl skärmad för att inte skadas av ’egen eld’. Detta kan innebära särskilda krav på skärmningsåtgärder för närbelägen utrustning eller vissa begränsningar i placeringen av sådan utrustning. En mycket kraftig strålkälla på en plattform som även bär kommunikationsutrustning, utrustning för telekrig och radar kräver en fin indelning av både tids- och frekvensspektrum.

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 hel- eller halvautomatiserat inriktningsverktyg. I de fall målobjekten är små eller har liten radarmålarea, som till exempel små drönare, kan radar behöva kompletteras med andra metoder för upptäckt och följning.

Då olika mål, till exempel olika typer av drönare, är sårbara vid olika frekvenser och pulsformer kan en identifiering av målet användas för att söka efter rätt frekvens och

165 Diamond Transistors, https://www.techbriefs.com/component/content/article/47455-diamond-transistors.

pulsform i en databas över tidigare provade eller bekämpade mål. Om målet finns i databasen kan vapnet anpassa frekvens och pulsform för att uppnå maximal verkan.

## Påverkan på militär förmåga

Kraftigare och mer kompakta HPM-system kommer att göra det billigare och enklare att bekämpa enklare drönare, speciellt när dessa flyger med hjälp av geografisk information eller tröghetsnavigering och alltså inte kan bekämpas med traditionell telekrigföring som slår ut GNSS eller radiokommunikation. 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 drönare som genomför en koordinerad attack men med distribuerade uppgifter, det vill säga vissa drönare navigerar, andra bär en verkanslast, andra har som uppgift att störa och förvilla, etc.

Användandet av autonoma eller semiautonoma militära system kommer säkerligen att öka under de närmaste 25 åren och dessa vapen och skyddssystem är beroende av avancerad elektronik för sin funktion. När beroendet av elektronik ökar blir systemen också mer känsliga för HPM-påverkan.

## Aktörer

I USA har *Rapid Capabilities and Critical Technologies Office* (RCCTO) köpt in fyra system från Epirus för utvärdering. Raytheon fick under 2023 ett utvecklingsuppdrag värt 31 miljoner dollar från *Naval Surface Warfare Center Dahlgren Division* för att utveckla ett HPM-vapen.[166] BAE, Leidos och Verus Research vidareutvecklar med hjälp av AFRL HPM-vapnet THOR.[167]

Kina bedriver idag en omfattande forskning inom HPM-området med ett flertal parallella verksamheter vid universitet och militärakademier. Det mest kända institutet är troligen *Key Laboratory of Advanced High Power Microwave Technology* i Xi'an varifrån många av de kinesiska vetenskapliga publikationerna inom området kommer. Man har upprepat västerländsk forskning inom området och gått vidare med utveckling av nya avancerade koncept, till exempel kompakta supraledande magneter för att generera magnetfält till olika typer av elektronrörsbaserade strålkällor.

166 Raytheon to build defensive microwave antenna systems for U.S. military, https://raytheon.mediaroom.com/2023-12-19-RTXs-Raytheon-to-build-defensive-microwave-antenna-systems-for-U-S-military.

167 Killing drones with Thor's hammer: Air Force eyes counter-UAS 'Mjölnir' weapon, https://www.defensenews.com/air/2022/02/28/killing-drones-with-thors-hammer-air-force-eyes-counter-uas-mjolnir-weapon/.

Ryssland har länge varit framstående inom HPM-forskning rörande elektronrörsteknik. Det är dock osäkert om man har tillgång till den teknik som krävs för att utveckla nya transistorer för AESA-HPM.

I Tyskland har Diehl Defence sedan många år tillbaka sålt HPM-system framtagna för att stoppa bilar och båtar med utombordsmotor. Under den senaste femårsperioden har dessa vidareutvecklats för att bli mer effektiva mot små drönare.

Teledyne-e2v i Storbritannien som, i likhet med Diehl Defence, byggt HPM-vapen för att stoppa bilar och båtar utvecklade för några år sedan en version för att stoppa små drönare. *Defence Science and Technology Laboratory* (Dstl) i Storbritannien arbetar med integrationen av Teledyne-e2v-systemet.

CEA-Gramat i Frankrike har forskat kring HPM-strålkällor och HPM-system i många år och en del av tekniken som utvecklas förs över till industrin. Företaget ITOPP (Alcen) har tagit fram två olika prototyper på HPM-system, ett som bygger på traditionell rörteknik och ett som bygger på AESA-teknik. Thales, som har en lång tradition av att utveckla elektronrör för radar, medicinsk teknik och acceleratorer, håller också på att utveckla ett C-UAS-system baserat på HPM. Mycket lite är publicerat men systemet verkar gå under namnet E-TRAP.[168]

## Lästips

High Power Microwaves, 4th edition, DOI: 10.1201/9781003287704.

Del Monte, L.A., War at the Speed of Light: Directed-Energy Weapons and the Future of Twenty-First-Century Warfare, https://doi.org/10.2307/j.ctv1f70m1m.

168 E-TRAP, l'arme à micro-ondes de Thales pour lutter contre les essaims de drones, https://www.youtube.com/watch?v=5RMh9vVMRs0.

# Laservapen

*Matts Björck och Lars Sjökvist*

## Inledande beskrivning

Laservapen som koncept har existerat i stort sett sedan den första lasern demonstrerades 1960 och under lång tid var forskningen inom området synonym med stora tekniskt komplicerade gaslasrar. De senaste två decennierna har diodpumpade fastatillståndslasrar, speciellt fiberlasrar, utvecklats till ett lovande alternativ. Mycket av den grundläggande tekniken utvecklades av tillverkningsindustrin för applikationer som svetsning och skärning. Dessa tekniska framsteg har sedan anpassats till de militära behoven avseende t.ex. god strålkvalitet och höga medeleffekter. I dagsläget har utvecklingen kommit relativt långt. Flera länder har utvecklat demonstratorer och vissa mindre system är förbandssatta.

Till skillnad från traditionella kinetiska vapen sker verkan med laservapen genom att en del av laserljuset absorberas av målet vilket orsakar en lokal uppvärmning. När målet upphettas kan material förlora sin bärighet och bränsle och/eller sprängämnen antändas. Även elektronik och styrenheter kan slås ut av de höga temperaturerna. På grund av verkansprincipen tar själva förloppet tid, några sekunder. Eftersom det är lätt att ändra effekten från en laser kan även graderad verkan uppnås, dvs. effekten kan ställas in på nivåer där vapnet istället för att ha förstörande verkan mot strukturer bländar eller förstör sensorer.

Den främsta fördelen med ett laservapen är att det endast kräver elektrisk ström och därför kan bekämpa många mål så länge det finns tillräckligt med energi tillgängligt. Även snabbheten i vapnet, där verkan efter mållåsning kan ske med ljusets hastighet, samt dess precision, brukar framföras som fördelar. Nackdelar är ett väderberoende som påverkar effektiviteten och att fri sikt från vapnet till målet krävs. Baserat på dessa egenskaper ses laservapen idag främst som ett defensivt vapen i form av närskyddsluftvärn för att skydda mot UAV:er, granater, robotar och raketer.

Utvecklingen av mindre laservapen, under 10 kW (kilowatt) medeleffekt, har fått mycket uppmärksamhet under de senaste åren då dessa förutses kunna vara ett effektivt motmedel mot små UAV:er. Större laservapen (upp mot 100 kW) kan verka mot inkommande artillerield, raketer och robotar. För laservapen som även kan skydda mot t.ex. kryssningsrobotar brukar det nämnas att flera hundra kW krävs.

## Trender och exempel

Med högre lasereffekt kan hårdare mål bekämpas. Tabell 3 visar vilka effektnivåer som behövs för olika måltyper. Här börjar tabellen med laservapen runt 10 kW som främst är effektiva mot mjukare mål som UAV:er. I det segmentet finns idag

flera exempel på demonstratorer och kommersiella system, bland annat *Compact Laser Weapon System* (CLWS) från Boeing som visas i figur 9, HELMA-P (2 kW) från CILAS samt *LiteBeam* (7,5 kW) från Rafael. Dessa system kan integreras på mindre fordon.

**Tabell 3** Exempel på olika effektnivåer hos laservapen och möjlig användning mot olika typer av mål. Tabellen är översatt från O'Rourke's rapport till den amerikanska kongressen. Notera att vissa mål går att bekämpa på närmare håll vid lägre effekter än vad tabellen anger.

| **Laservapens effekt och möjliga typer av mål som kan bekämpas** | | | | |
|---|---|---|---|---|
| ~ 10 kW | Tiotals kW | ~100 kW | 100+ kW | ~1 MW |
| UAV:er | | | | |
| | Raketer, granater, robotar | | | |
| | | | Flygplan | |
| | | Sjömålsrobotar, Kryssningsrobotar subsoniska | | Supersoniska samt ballistiska robotar |

**Källa:** Ronald O'Rourke, Navy Shipboard Lasers for Surface, Air, and Missile Defense: Background and Issues for Congress, CRS Report R41526 (2015).

Större system på 10-tals kW kan bekämpa hårdare mål som större UAV:er på längre avstånd samt RAM-hot (*Rockets, Artillery and Mortars*). Dessa system kräver mer utrymme och kan inhysas på större fordon. Som ett exempel har ett 50 kW laservapen installerats på ett Strykerfordon[169], se figur 9. Ännu större system upp mot 100 kW har en storlek som närmar sig en container och kan därmed endast installeras på större plattformar som exempelvis lastbilar. Den här klassen av laservapen är också intressant för fartyg eftersom dessa kan ha tillgång till mer elektrisk effekt och utrymme jämfört med markfordon. Det mest kända exemplet i 100 kW-klassen är Rafaels demonstrator *Iron Beam*.[170] *Iron Beam* har enligt uppgift skjutit ner robotar på ett avstånd av 7 km.[171]

Vid strax över 100 kW går också gränsen för vad som i dagsläget har visats med modern teknologi och redovisats i öppna litteraturkällor. Under 2024 presenterades att Lockheed Martin, General Atomics och Raytheon med olika tekniker uppnått lasereffekter på 300 kW[172] men inga uppgifter om demonstratorer som använder dessa lasrar har uppvisats. Lasrar i megawattklassen har inte byggts med fastatillståndslasrar. Tidigare laservapenprojekt som *Airborne Laser* (ABL) hade kemiska lasrar i megawattklassen, som dock var både tekniskt och logistiskt väldigt komplexa och dyra. Detta ledde också till att de avvecklades till förmån för mer lovande lösningar baserade på fastatillståndslasrar.

169 https://www.army.mil/article/249239/army_advances_first_laser_weapon_through_combat_shoot_off.

170 https://www.rafael.co.il/system/iron-beam/.

171 https://worldisraelnews.com/israels-iron-beam-a-new-era-in-defense-technology/.

172 T. Karr, The new laser weapons, Physics Today 77 (1), 32–38 (2024).


**Figur 9** Överst, Boeings system CLWS (5 kW) monterat på en Polaris jeep (foto: FOI). Nederst, US Army 50 kW prototyp integrerat på ett Stryker fordon (Källa: US Army Jim Kendall).

Det finns även diskussioner om att installera laservapen ombord på flygplan. Detta medför stora utmaningar eftersom tillgänglig plats och energi på t.ex. stridsflyg eller helikoptrar är starkt begränsad. Det israeliska företaget Elbit har demonstrerat ett laservapensystem monterat i ett flygplan av Cessnatyp och skjutit ner drönare.[173]

Sammantaget är laservapenområdet under stark utveckling där flera företag har demonstrerat vapen med effekter över 100 kW, vilket gör vapnen effektiva även mot hårdare mål såsom robotar på avstånd som närmar sig 10 km. Det betyder i sin tur att nyckelteknologierna (laser, strålformning/adaptiv optik, målföljning) finns tillgängliga och möjliga att sätta samman till ett system. Det bör dock tilläggas att varje delsystem uppskattas ligga i den tekniska framkanten för vad som är möjligt att realisera med dagens teknik, vilket gör att prototypsystem är relativt kostsamma att utveckla.[174] Dock är kostnaden per skott låg eftersom endast elektrisk energi behövs för att driva systemen. En utmaning i framtiden är troligtvis att sänka kostnaden och att anpassa teknologin ytterligare för taktiska tillämpningar och miljön på slagfältet.

Eftersom det redan i dag finns förbandssatta system med lägre lasereffekter kommer troligtvis dessa spridas till andra länder under de kommande 5–10 åren och sannolikt bli operativa. En naturlig utveckling är att först använda systemen som basskydd vid militära flygplatser och andra fasta installationer där det finns gott om plats och god tillgång till elektricitet. Därefter kommer system som kan placeras på fartyg samt markfordon att implementeras. System i storleksklassen ett par 10-tals kW kan antas förekomma på markfordon och upp till 100 kW eller högre på fartyg beroende på plattformsstorlek.

På längre sikt (10–25 år) kommer tekniken att utvecklas och storleken minska, vilket möjliggör att system med högre effekter kan placeras på mobila plattformar. Eftersom källor med medeleffekten 300 kW har visats är det rimligt att anta att system med 300 kW eller högre effekter finns tillgängliga för armén och marinen inom den här tidsperioden. Under tidsperioden kan även system för egenskydd av flygande plattformar dyka upp. Optimering av systemen avseende vikt, effektförbrukning och volym är avgörande för denna tillämpning.

Om laservapen börjar användas i en signifikant volym på slagfältet kommer också målen att anpassas med skydd mot laserverkan. Eftersom dagens mål inte är anpassade överhuvudtaget kommer det bli en duellsituation mellan skydd och verkan där gammal, ej anpassad, materiels användbarhet kan minska kraftigt. Det betyder också att effekten på laservapnen måste ökas för att förbli effektiva. Exempel på möjliga anpassningar är mer värmebeständiga material, högreflektiva ytor samt användning

173 https://www.timesofisrael.com/defense-ministry-shoots-down-drone-with-plane-mounted-laser-in-latest-test/.

174 Ronald O'Rourke, Navy Shipboard Lasers for Surface, Air, and Missile Defense: Background and Issues for Congress, CRS Report R44175 (2024).

av material/ytor som offras genom förångning och därmed tar upp energi alternativt skapar skyddande plasma eller gasplym framför målet.

## Särskilda delområden

En kritisk teknologi för laservapen är själva laserkällan. Den dominerande teknologin är diodpumpade fastatillståndslasrar. En framgångsfaktor för att utveckla kompakta och effektiva laserkällor är själva pumpdioderna. De är halvledarlasrar som kombineras till moduler på flera hundra watt och används sedan för att mata laserförstärkaren. För att bygga dessa lasrar krävs tillgång till halvledarfabriker. Viss tillverkning av halvledarlasrar återfinns i Europa men i begränsad omfattning jämfört med till exempel Kina. Den dominerande tekniken för diodpumpade fastatillståndslasrar är fiberteknik, dvs. fiberlasrar. De är dopade optiska fibrer som pumpas med ljuset från pumpdioderna. En utmaning är att optimera fiberlasrarna med avseende på hög verkningsgrad, generering av hög effekt och bra strålkvalitet. I industriella fiberlasrar offras vanligtvis strålkvaliteten för att nå högre effekter vilket inte kan tillämpas i militära lasrar då laserstrålen måste hållas samman över långa avstånd.

Eftersom varje fiberlaser, i dagsläget, kan ha några kW uteffekt behöver flera förstärkare kombineras för att nå relevanta lasereffekter för en vapentillämning. Det betyder att strålkombinering är ytterligare en nyckelteknologi. Här är två metoder relevanta, spektral och koherent strålkombinering. Spektral strålkombinering nyttjar dispersiva element (gitter). Varje laser stäms av till att ha en unik våglängd. Dessa lasrar fås sedan att överlappa på de dispersiva elementen med en korrekt vinkel så att de olika strålarna kombineras till en gemensam stråle (jämför med ett prisma där ljuset färdas baklänges). I den här tekniken är gittren centrala eftersom de måste klara höga effekttätheter utan att skadas eller orsaka försämrad strålkvalitet. Koherent strålkombinering, å andra sidan, använder en laserkälla med lägre effekt som delas upp och där varje del förstärks för sig. Dessa förstärkta delstrålar kombineras sedan vid utgångsaperturen eller på målet med hjälp av fasmodulatorer (dvs. vågfronten hos ljuset anpassas). Här ligger en utmaning i själva kontrollsystemet för att hålla delstrålarnas fas låsta till varandra.

För att skapa verkan måste träffpunkten på målet hållas stabil. Noggrannheten för den följning som krävs är i storleksordningen några centimeter på kilometeravstånd. Det ställer höga krav på målföljningssystemet, både avseende hårdvara och signalbehandlingsalgoritmer. Dessutom orsakar atmosfären distorsioner av laserstrålen, vilka försvårar målföljning och ökar strålfläckens storlek. Distorsionerna kan i ett första steg kompenseras med fininriktning av den optiska strålgången, så kallad *tip/tilt*-kompensering. Vid längre avstånd än några kilometer och högre effekter än några 10-tals kW behöver även fasen på vågfronten justeras med adaptiv optik. Detta kan åstadkommas med deformerbara speglar eller genom koherent strålkombinering där delstrålarna låses direkt på målet istället för vid utgångsaperturen.

Även skyddsåtgärder för egna vapen och plattformar är teknologier kopplade till laservapen. Dessa är kritiska för att möta det hot som laservapen kommer att utgöra i framtiden och inkluderar både materialforskning och aktiva motmedel.

## Samverkande och förutsättande teknikområden

Laservapen drivs av elektrisk energi och därför är energiförsörjning en viktig förutsättning för implementeringen av laservapen. Det har påverkan både på uthålligheten (antal bekämpningar) och den totala effekten som kan implementeras på olika plattformar. Möjliga tekniker för energiförsörjning inkluderar batterier och superkondensatorer.

Den elektriska verkningsgraden hos en fiberlaser är oftast 30–40% vilket innebär att det utvecklas relativt mycket värme som måste kylas bort. Värmeavgivningen från vapnet är dock liten i jämförelse med t.ex. en motor på en stridsvagn. Eftersom utrymmet på de flesta plattformar är begränsat är optimering av kylsystemets vikt, volym och effektivitet viktig.

Själva laservapnet behöver visas in mot målet och är tänkt att ingå i en bekämpningskedja. Därmed krävs teknik för målupptäckt som kan ske aktivt med radar eller passivt med spanande IR-sensorer. För att vara effektivt måste även laservapnet vara integrerat i ett ledningssystem som kan skicka målkoordinater till laservapnet samt prioritera i vilken ordning multipla mål ska bekämpas.

## Påverkan på militär förmåga

Fram till 2050 bedöms laservapen främst användas som ett luftvärn med kort- och medellång räckvidd. Det kommer även användas mot mindre mål som små båtar, minor och känsliga infrastrukturer. Därmed kommer laservapen främst att påverka förmågorna bekämpning och skydd.

Laservapen har en mycket kort reaktionstid tills verkan startar. Antalet bekämpningar (”skott”) är avhängigt energitillgången och kan därför vara mycket större än för kinetiska vapen. Detta gör att ett laservapen kan bidra till ett uthålligt skydd mot svärmar av UAV:er. Dock påverkas effektiviteten av väderförhållanden och laservapen bör därmed ses som ett komplement och inte som en ersättning till konventionellt luftvärn. Dess främsta egenskap är att med en låg kostnad per bekämpning öka uthålligheten hos luftvärnet.

Effekten hos ett laservapen kan varieras vilket betyder att graderad verkan kan uppnås, dvs. mindre effekt kan användas mot mjukare mål för att åstadkomma skada hos vitala komponenter hos ett hot. Kombinerat med den höga precisionen kan kritiska komponenter eller infrastruktur slås ut eller forceras ljudlöst vilket kan ge taktiska fördelar. Exempel inkluderar här antenner, kraftledningar, kameror, taggtråd eller stängsel.

Små laservapensystem implementeras redan i dagsläget på mindre mobila mark- eller luftplattformar. För dessa plattformar kommer vikt, volym och effekttillgång vara begränsande faktorer. Detta gör att dessa laservapen främst kan fungera som egenskydd för mindre enheter/trupper med en räckvidd på någon eller några kilometer för skydd mot UAV:er men även till viss del mot mindre raketer och robotar samt artillerield.

De kraftfullaste laservapnen kommer troligtvis att skydda större plattformar och installationer som fartyg och baser. Med sin höga lasereffekt kommer vapnen kunna ge skydd mot inkommande raketer, robotar, granater och UAV:er. Viss bekämpningsförmåga kommer även att finnas mot mindre och delvis oskyddade plattformar som helikoptrar och mindre flygplan.

## Aktörer

De senaste decennierna har teknikutvecklingen inom laservapenområdet dominerats av USA även om de flesta större militärnationer har sina egna program. Den amerikanska flottan, US Navy, var tidigt ute med att integrera demonstratorer på fartyg.[175] År 2014 installerades *Laser Weapon System* (LaWS) med effekt på cirka 30kW ombord på fartyget USS Ponce. Denna utveckling har fortsatt och den senaste laservapendemonstratorn är tänkt att nyttja 150 kW effekt. US Navy har även utvecklat bländlasern ODIN (*Optical Dazzling Interdictor Navy*) mot sensorer, vilken har börjat installeras på fartyg. ODIN är tänkt att uppgraderas med en modul som möjliggör förmåga till bekämpning.

Även US Army utvecklar laservapen. Under 2023 presenterades ett laservapensystem på ett Strykerfordon som är tänkt som skydd för egen trupp. Detta har levererats i flera exemplar till förband för att utvärderas.[176] Amerikanska tillverkare som Boeing[177] och Blue Halo[178] presenterar mindre laservapen (under 10 kW) som produkter på sina hemsidor.

Israel, genom tillverkaren Rafael, har också presenterat olika laservapensystem från små system som *Lite Beam* upp till *Iron Beam*, med en effekt på 100 kW, och som är tänkt, som namnet antyder, att ingå i *IronDome*-systemet.

I Europa utvecklar flera länder laservapen. Tyskland har, genom tillverkarna MBDA och Rheinmetall, tagit fram en 30 kW demonstrator för flottan som monterats

175 Ronald O'Rourke, Navy Shipboard Lasers for Surface, Air, and Missile Defense: Background and Issues for Congress, CRS Report R44175 (2024).

176 https://breakingdefense.com/2024/03/exclusive-strykers-with-50-kilowatt-lasers-in-centcom-for-experiment-army-no-2-says/.

177 https://www.boeing.com/defense/missile-defense/directed-energy.

178 https://bluehalo.com/c-uas-autonomous-systems/c-uas-directed-energy/#locust.

på fartyget Sachsen och provats under ett år i Östersjön.[179] I Frankrike har Cilas utvecklat HELMA-P, vilken var en del av skyddet av OS i Paris under 2024.[180] Storbritannien utförde, i början av 2024, de första demonstrationerna med nedskjutning av UAV:er med ett laservapen utvecklat av Qinetiq och MBDA.[181]

Även andra större militärnationer studerar laservapen. Australien har två företag (EOS[182] och AIM Defence[183]) som utvecklar laservapen och som demonstrerat sina system. Även Kina har visat upp laservapen på flera mässor. Ryssland har förbandssatt ett laservapen, Presevet, vid de strategiska robotstridskrafterna. Detta är dock troligtvis inriktat mot att blända eller förstöra sensorer på satelliter.[184] Rykten har även florerat om ett laservapensystem kallat Zadira.[185] Ukraina utvecklar också laservapen.[186,187]

Sammanfattningsvis så studerar och utvecklar de flesta större militärmakter laservapensystem. USA framstår som klart ledande i utvecklingen med prototyper framtagna för både mark- och sjöarenan. Även Israel är långt framme med flera demonstratorer med hög effekt. I Europa visar Storbritannien, Tyskland och Frankrike upp demonstratorer för bekämpning av UAV:er. *European Defence Fund* (EDF) har haft två utlysningar som syftar till att utveckla europeiska laservapen och de nyckelteknologier som krävs för dessa. Europeiskt samarbete inom laservapenområdet sker också via EDA (*European Defence Agency*). Även Sydkorea, Australien och Kina har visat upp laservapensystem. Kina bedöms ha både kompetens och teknisk förmåga tillgängliga för att ta fram laservapensystem.

Det kan förväntas att majoriteten av dessa länder i någon form kommer att börja använda laservapensystem innan 2050.

179 https://www.mbda-systems.com/press-releases/bundeswehr-successfully-concludes-laser-weapon-trials-at-sea/.

180 https://www.cilas.com/news/3-more-helma-p-french-armed-forces.

181 https://www.defenseadvancement.com/news/laser-directed-energy-weapon-system-achieves-uk-first/.

182 https://eos-aus.com/.

183 https://www.aimdefence.com/.

184 https://www.thespacereview.com/article/3967/1.

185 https://www.bbc.com/news/world-europe-61508922.

186 https://thedefensepost.com/2025/04/15/ukraine-unveils-laser-weapon/.

187 https://mezha.media/en/oboronka/ukrajinska-lazerna-zbroya-proti-fpv-droniv-rozrobnik-rozkriv-detali-303850/.

## Lästips

O´ Rourke, Ronald. Navy shipboard lasers: background and issues for congress, DTIC, AD1218019, (2023).

Perram, G, Cusumano, S., Hengehold, R., Fiorino S., An Introduction to Laser Weapon Systems, DEPS, Albuquerque, (2009).

Venugopal, V., Zapping enemy targets: Viable laser weapons remain critical to military strategy, Photonics Focus, SPIE, 01 March, (2024).

Karr, T., Trebes, J, The New Laser Weapons, Physics Today, Jan. 01 (2024) DOI: 10.1063/PT.3.5380.

Steinvall, O. The potential role of lasers in combating UAVs, part 1: detection, tracking, and recognition of UAVs, Proc. SPIE, vol. 11866, (2021).

Steinvall, O. The potential role of laser in combating UAVs: part 2; laser as a countermeasure and weapon Proc. SPIE, vol. 11867, (2021).

Björck, M. et al., A laser weapon demonstration to counter small UAS: lessons learned, Proc SPIE, vol 13675, (2025).

# Del 3 – Förmågeområden

## Inledning

*Göran Kindvall, Anna Lindberg och Cecilia During*

Del 2 fokuserade på teknikområden som i många fall är möjliggörande för mer förmågeinriktade områden som plattformar, rymd, cyber, ledning med flera.

Den möjliga utvecklingen av de senare mot 2050 presenteras här i Del 3. Vi tar avstamp i system och förmåga för domänerna mark, sjö, luft, rymd och cyber, bland annat genom att beskriva den möjliga utveckling vi kan se avseende plattformar och förmåga inom dessa. I alla fysiska domäner diskuteras de bemannade plattformarnas framtid och vilken roll obemannade, eller autonoma, plattformar kan få i framtiden, enskilt eller i nära samverkan med bemannade plattformar eller mänskliga operatörer.

Inom Natos forskningsorganisation (*Science and Technology Organization*, STO) genomfördes våren 2023 en aktivitet där de traditionella plattformssystemens framtida roll diskuterades.[188] Resultatet blev att de har en roll, men att deras användning kan begränsas av nya hot.

Natos utveckling av ett koncept för mutidomänoperationer (*Multi Domain Operations*, MDO) innebär en planering för att konflikter sker i flera (eller alla) domäner samtidigt. I konceptet ingår även synkronisering med andra, även civila, aktörer. Detta diskuteras mer i samband med syntesen i Del 4.

Vissa ser också den mänskliga hjärnan som en sjätte domän. Vi går inte så långt här, men vi inkluderar kapitel om både soldatsystem och mänsklig förstärkning.

Strukturen för kapitlen i denna del är:

- Inledande beskrivning
- Trender och exempel
- Särskilda delområden
- Samverkande och förutsättande förmågor och tekniker
- Påverkan på militär förmåga
- Aktörer
- Lästips.

188 Ovegård, E., Kindvall, G. och Mårtensson, T., Reserapport SAS-174 Research Specialists' Meeting "Are the Major Weapon Platforms Obsolete?, FOI Memo 8218, 2023-06-27.

# Plattformar i markdomänen

*Johannes Andersen*

## Inledande beskrivning

I detta kapitel behandlas främst de markplattformar som återfinns i de mekaniserade brigaderna och i stridsgruppen samt i mindre utsträckning den motoriserade brigaden. Särskilt fokus blir på de stridsvagnar, pansarbandvagnar, bandvagnar, pansarterrängbilar och drönare som används i markstriden.

Striden i markdomänen förändras konstant, men ibland – ofta i samband med en konflikt – förändras den så pass snabbt med nya medel och nya motmedel att det blir svårt att bedöma hur en mogen framtida taktik med en avvägd blandning av nya och mer traditionella förmågor kommer att gestalta sig. Det pågående kriget i Ukraina, som naturligtvis på olika sätt präglas av de stridande parternas olika förutsättningar att föra detta krig, visar att metoderna, organisationen och materielen kontinuerligt och snabbt förändras. Det befintliga kombineras med nytt i en kamp där förutsättningarna för manöverkrigföring förändrats i grunden. De nya förmågorna som kommer att vara en nödvändighet för att möta hotbilden kan inte ses som tillägg till befintlig materiel och taktik, utan måste integreras från början. Organisationen behöver byggas utifrån ett taktiskt koncept som utgår från dessa förmågor snarare än att förmågorna anpassas, och i viss mån begränsas, utifrån befintlig organisation och taktik. Detta innebär exempelvis att nuvarande organisation kommer att stöpas om, där vissa markplattformar lyfts ut för att bereda plats för det som behöver tillkomma. Adaptiv förmåga inom organisation och metod, och framförallt en kultur som premierar detta, kommer att ha mycket stor påverkan på den operativa effekten.

De senaste årens krig i Ukraina och Mellanöstern indikerar att den västerländska förhoppningen om korta intensiva krig som slutar med att motståndaren erkänner sig besegrad inte stämmer överens med Rysslands och Irans syn på krigföring. Istället för att acceptera nederlag ändrade Ryssland strategi från ett manöverkrigstänkande till utnötningskrig. Kvantitet har kommit att dominera framför kvalitet på allt från strategisk till stridsteknisk nivå.

Förband som verkar på marken nyttjar olika markplattformar som skiljer sig signifikant från varandra och som är anpassade för att lösa olika uppgifter. Det finns plattformar som stammar från civil användning så som skotrar, drönare, motorcyklar och lastbilar, men det finns även de som är speciellt framtagna för militär användning så som terrängbilar, splitterskyddade bandvagnar, patrullrobotar och stridsvagnar. Utvecklingen och kravställningen skiljer sig åt beroende på om utvecklingen drivs av militära eller civila behov. Hur dessa kommer utvecklas i framtiden kommer att påverkas av en mängd olika faktorer.

När ett fordon designas eller utformas är det en komplex avvägning att balansera uppgift/roll, vikt och ekonomi. Generellt finns en trend att framförallt stridsfordon har fått fler och fler komplexa tekniska system för att öka deras förmåga att lösa sina stridsuppgifter. Detta har lett till både ökad vikt och dyrare system som följd, och det är en viktig fråga för alla länders försvar att balansera kostnaderna för systemen mot de förhöjda förmågorna som kan uppnås med olika system. Exempelvis har kostnaden för en pansarbandvagn, justerat för KPI, ökat med mellan 500-1000 gånger från 60-talet till idag.

Ofta är det inte brist på tekniska lösningar, utan snarare bedömningen av vilka lösningar som ger störst operativ effekt i förhållande till kostnaderna, som utgör den största utmaningen.

### Det glesa och transparenta slagfältet

Manöverkrigföring och sensortäckning är samverkande men även motpoler när det gäller försvarsförmåga. Traditionell manöverkrigföring kommer att anpassas till det glesa och transparenta slagfältet och funktioner hos markplattformarna och förmågor hos markförbanden kommer att genomgå motsvarande förändring. Även om särskilda åtgärder från endera parten tillfälligtvis kan förvirra, vilseleda eller direkt störa motpartens lägesbild så kommer det behöva finnas grundläggande förmågor hos markplattformarna som kommer att dimensioneras med utgångspunkt från att motståndaren har en mycket god sensortäckning av slagfältet. Möjligheten att verka på djupet med hjälp av mindre flygande system med verkansdelar gör att den traditionella uppdelningen av slagfältet i REAR-CLOSE-DEEP[189] i vissa avseenden behöver nyanseras när man ur ett verkans- och skyddsperspektiv måste se hela djupet som CLOSE. Direktbekämpning med patrullrobotar sker redan idag på mer än 50 km djup, med längre porté än konventionellt eldrörsartilleri.

I vissa operationsområden ska få förband verka i stora områden och kommer av den anledningen att sprida ut sig, vilket också innebär att markplattformarna utgör mer svårupptäckta och svårbekämpade mål. Att vara utspridd begränsar dock möjligheterna till kraftsamling med lokal överlägsenhet och riskerar att sänka tempot. Utspridda markplattformar leder till utmaningar för funktionsförband som ska stödja manöverförbanden, till exempel fältarbeten, logistik och sjukvård. Om brigaden ska strida på det glesa slagfältet behöver denna typ av funktioner integreras på ett annat sätt än idag. Markplattformar kommer i större utsträckning än idag att behöva kunna medge att besättningen befinner sig längre tider i fordonet, och olika aspekter av komfort och självförsörjning kommer att få större betydelse.

189 REAR, CLOSE och DEEP är begrepp enligt Natostandarden ALLIED JOINT DOCTRINE FOR LAND OPERATIONS som beskriver stridens djup och hur striden förs i förhållande till fienden. REAR handlar i stor utsträckning om förutsättningsskapande, CLOSE är den direkta striden och DEEP är strid mot fiendeförband eller resurser som inte är i direkt strid.

I andra områden finns större kvantiteter av förband och plattformar inom mindre geografiska områden och närmare en motståndares territorium. Förbanden och materielen inom markdomänen måste utformas för flera typer av miljöer, uppgifter och insatser.

## Trender och exempel

Det finns grundläggande skillnader mellan hur olika arméer bedriver sin strid och fordonen har designats efter dessa behov. Sverige sticker ut med en ovanligt hög grad av mekanisering, det vill säga enheter försedda med skyddade och ofta terränggående fordon, för våra soldater. Kvalificerade fordon som Stridsfordon 90 används för att förflytta hela grupper och där striden förs av- eller uppsuttet med stöd från vagnen. Det är tänkbart att med växande numerär och en väsentligt högre kostnad per fordon så kan denna typ av kvalificerade vagnar, som i många fall är utrustade för att ha goda duellvärden med sina motsvarigheter på motståndarsidan, i större utsträckning behöva kompletteras med enklare fordon där den direkta duellen är underordnad möjligheterna att verka indirekt. Det som berättigar stridsfordonen en roll i framtidens strid är deras förmåga till genombrott och kraftsamling samt förmågan att över tiden behärska terräng/områden under längre tid, i ”alla” väder och under ”alla” siktförhållanden. Om man kan förutse en längre lågintensiv konflikt finns det bättre och mer kostnadseffektiva lösningar än stridsfordon. Stridsfordonens förmågor inklusive deras psykologiska effekt kan dock inte ersättas helt av relativt billiga drönare och/eller patrullrobotsystem. Detta förändras inte av att drönare existerar, men det kräver anpassning av stridsfordonens förmågor inklusive skydd mot nya hot där bl.a. drönare kommer att vara närvarande. Komplexa system kräver dessutom längre utbildningstid vilket blir utmanande med en värnpliktsarmé. Utformningen av fordonen är därför avhängigt vilken typ av förband som Sverige skall ha samt var och hur vi vill strida med dem.

### Pansarbandvagnar, pansarterrängbilar och stridsvagnar

Modern teknik ger stridsfordonen nya möjligheter med bättre stödsystem där exempelvis maskininlärning stöttar med automatisk måligenkänning, hybriddrift ger reducerad signatur och minskad logistik, bättre ballistiska skyddsmaterial och aktiva skyddssystem ger ett bättre skydd, förbättrad skyddsförmåga nås genom adaptivt kamouflage, och så vidare. Olika typer av modularitet kommer att bidra till flexibilitet och framtidssäkring, men kan också leda till oönskade kompromisser.

Det finns ett antal befintliga och kommande fordonskoncept där framförallt skyddet har utvecklats, exempelvis genom att för stridsvagnar ha besättningen i chassit. Varnar- och Motverkanssystem, VMS[190], kommer att fortsätta utvecklas för att

190 Den engelska akronymen är APS, Active Protection System.

innefatta skydd mot drönarattacker så som patrullrobotar men även integreras i stödsystem för att bidra till besättningens lägesbild.

Kvalificerade och dedikerade fordonsburna motmedelssystem för drönare kommer att behöva framrycka i takt med manövern, och de kommer ha en mix av störning, kinetisk bekämpning och bekämpning med mikrovågsvapen[191] eller laser. Även om utvecklingen av drönare kommer att konvergera mot specifika plattformar för att lösa specifika uppgifter kommer både drönarnas numerär och möjligheterna att med låg utvecklingskostnad och på kort tid utveckla dessa plattformar leda till att den krigsekonomiska asymmetrin motiverar en flexibel och adaptiv motmedelsförmåga.

En effekt av närvaron av luftburna sensorer är att rörelse markant ökar risken för upptäckt och att rörlighet i sig inte längre ger lika stort bidrag till skydd mot långräckviddig bekämpning som tidigare på grund av styrda långräckviddiga precisionsvapen som exempelvis patrullrobotar. För en manöver på det transparenta slagfältet är det därför av central betydelse för förbandet att, vid förflyttningar eller framryckningar, röra sig med hög hastighet. Framtidens markplattformar kommer av den anledningen att behöva en högre rörlighet och en högre robusthet i termer av framkomlighet. Av samma anledning kommer markfordonen att ha behov av signaturanpassning eller -minimering.

För att maximera effekten av ett i förhållande till motståndaren begränsat antal markplattformar kommer förmåga till samverkan, med stöd av automation, mellan markplattformar att spela en viktig roll. Ett populärt exempel är förmågan till bekämpning enligt *best sensor any shooter* som potentiellt är en del av denna samverkan men viktigare är informationsöverlägsenhet och förmågan att sortera och tillse att relevant och koncis information når de som behöver den. Resultatet är en förkortad OODA[192]-loop, men samverkan i denna betydelse kräver också teknik med hög kapacitet för att kunna skicka och ta emot information, vilket innebär betydande risker och svagheter. En framtida markplattform måste vara utrustad med robusta kommunikationslösningar som medger utbyte i hög informationstakt och med låg risk för störning och hackning. Motståndarens förmåga att påverka vår lägesbild för att vinna taktiska fördelar kommer fortsatt att vara stark.

Inom verkanssystem går kalibrarna för huvudbeväpning generellt upp, med 130 eller 140 mm kanon för stridsvagn där automatladdare är nödvändig. För pansarbandvagnar kommer huvudbeväpningen fortsatt behöva kunna vinna duellsituationer mot motsvarande fiendeplattform, men en verkanspalett med pansarvärnsrobotar, patrullrobotar och FPV-drönare[193] kommer att utgöra ett mycket mer betydelsefullt komplement till huvudbeväpningen. Beroende på uppgiften behöver inte nöd-

191 Med mikrovågsvapen avses HPM, High Power Microwave.

192 OODA, Observe, Orient, Decide and Act, är en modell som syftar till att förekomma sin motståndare i beslutsprocesser, att själv ha möjligheter att kunna agera medan ens motståndare bara hinner reagera.

193 FPV står för First Person View och associeras normalt sett till de mindre kvadkoptrar som styrs av piloter till skillnad från patrullrobotar som har högre nivå av automation i styrningen.

vändigtvis dessa system vara monterade på plattformen och ett exempel på detta är patrullrobotar som kan tillhandahållas, det vill säga föras fram och avfyras, från bakre förband men slutfasstyras av de främre förbanden.

### Logistikfordon

De två främsta utmaningarna inom logistik är energi- och drivmedelsförsörjning samt skydd mot bekämpning av mindre flygande plattformar. Omställningen till alternativa energikällor och framdrivningssystem kommer att i hög utsträckning ha ett beroende till den civila omställningen till icke-fossila energibärare och det kommer inte att vara möjligt för militära förband att ha helt unika energilösningar. De flesta alternativ till de fossila drivmedel som används idag som energibärare till markplattformarna har lägre energidensitet. Detta innebär att utöver andra egenskaper som alternativa energikällor kan ha så riskerar det logistiska fotavtrycket att öka. Framtida energisystemslösningar kommer åtminstone inte initialt erbjuda samma uthållighet för förbanden och försvåra förrådsställning, men ger beroende på energibärare andra fördelar kopplat till signatur, framkomlighet och möjligheter att driva elektromagnetiska vapen.

Samtliga logistikfordon kommer att behöva eget skydd mot mindre flygande plattformar. På det glesa slagfältet kommer möjligheten för fienden att helt kringgå främre förband, där kvalificerad motmedelsförmåga kommer att finnas, i kombination med utmaningar kopplade till att ha skydd över ytan, göra att logistikfordon kommer att behöva egna plattformsskydd.

### Flygande system

Mindre flygande plattformar med och utan verkansdelar har funnits en lång tid, men det är först på de senaste 10 till 15 åren som den företrädelsevis civila utvecklingen av så kallade drönare gjort att tillgängligheten och användningen ökat på ett sådant sätt att markstridens karaktär förändrats. Spaningsfunktionen hos de mindre flygande plattformarna medger en uppdaterad lägesbild och i takt med att motmedel kommer att störa denna förmåga kommer systemen i större utsträckning bli fler, autonoma och samverkande så att de alla bidrar till en sammansatt, eller fusionerad, lägesbild. Systemen kommer primärt med automation sammanställa operatörers behov av aktuell lägesbild, och den pilotstyrda och i någon mening specifika spaningsförmågan kommer att vara sekundär.

Flygande plattformar som verkanssystem kommer att utgöras av tre olika typer av system som löser olika militära problem. Det kommer att finnas kvalificerade system för strategisk bekämpning bortom befintligt bortre område för de mekaniserade förbanden, det kommer att finnas system som löser förbekämpning och kompletterar pansarstriden som är fordonsburna men som i stora delar är likt användningen av pansarvärnsrobotar och det kommer finnas soldatburna system med kort räckvidd som löser uppgifter jämförbara med det hos pansarskott eller handgranater.

Sannolikt kommer mindre obemannade flygande plattformar vara ett kostnads-, logistik- och volymmässigt intressantare alternativ för att lösa uppgifter som annars löses av attackhelikoptrar.

## Samverkande och förutsättande förmågor och tekniker

Autonoma markplattformar i en militär kontext avser oftast fordon som kan lösa fler och mer komplexa uppgifter än vad som omfattas av begreppet i civila sammanhang där exempelvis begrepp som förarlösa fordon förekommer. Ibland beskrivs och samlas de olika automatiska funktionerna under det samlade begreppet uppdragsautonomi, där autonomi i termer av att kunna framföra fordonet i terräng, att kunna klassificera och identifiera olika objekt eller liknande automatiska funktioner tillsammans med en överordnad uppgift ger en nivå av automation så att plattformarna kan tilldelas uppdrag.

Det finns flera användningsområden för autonoma plattformar som kan vara förhållandevis enkla i sin karaktär, som olika typer av logistiktillämpningar, men även mer komplexa uppgifter där exempelvis automatisk bekämpning av mål kan ingå, och där det finns juridiska frågor att hantera kopplat till systemets handlingsregler.

Användning av obemannade markplattformar för att stödja den mekaniserade striden kommer att öka i takt med att systemens robusthet och fältmässighet ökar. I takt med att de automatiska funktionerna i obemannade markplattformar utvecklas kommer de teleopererade[194] inslagen att minska, till nivån att sidoordnade plattformar kan tilldelas uppgifter, och i viss mån uppdrag, för att tillsammans med bemannade plattformar föra striden, det vill säga koncept enligt *Loyal Wingman*. Logistik kommer att lösas till del av autonoma system.

Även inom bemannade plattformar kommer olika automatiska funktioner, eller autonomi, utgöra stöd för besättningen och möjliggöra för dem att gå från roller som förare, skytt eller laddare till systemoperatörer. Markplattformar kommer att ha stöd för taktisk och stridsteknisk planering där exempelvis framkomlighet, energiförbrukning, skyl och egna siktlinjer beaktas. Utmaningen att fortsatt ha en värnpliktsarmé trots en tydligt ökad komplexitet i systemen kan också kompenseras med stödsystem.

Beslutsstödsystem kommer att minska den kognitiva belastningen hos besättningen, där den främsta funktionen kommer att vara att välja, eller filtrera, ut den information som är mest relevant för mottagaren givet den stora mängd underrättelser som är resultatet av den mycket stora mängden sensorer på slagfältet. Beslutsstöd i meningen att ge rekommendationer kommer åtminstone inledningsvis att vara underordnat informationshanteringen. Andra typer av stöd, så som

194 Med teleopererad avses styrning på distans, av en operatör.

delvis självkörande fordon, automatisk målsökning och liknande kommer också att avlasta besättningen hos markplattformarna.

## Lästips

Jack Watling: The Arms of the Future: Technology and Close Combat in the 21st Century, Bloomsbury Publishing plc, 2023.

Dr Jim Greer at the Maneuver Warfare Symposium, https://www.youtube.com/watch?v=bS-YSz9LkjA&t=50s.

Andreas Hörnedal: Rare Birds. A Look at the Low-density Battlefield and Armed Drones, FOI-R--5573--SE.

Robert Dalsjö: Det glesa slagfältet och försvaret av Sverige, 3/2019 av KKrVA Handlingar och Tidskrift.

Alexander Samimi Johansson et al: Uppdragsautonomi, FOI Memo 8862.

Jouni Rantakokko et al: Tekniköversikt autonoma och obemannade system - Del 2: Markstriden, FOI-R--4901--SE.

Maris-Tech Ltd: Military vehicles trends and technologies, https://www.maris-tech.com/blog/military-vehicles-forecast-trends-and-technologies/.

# Plattformar i sjödomänen

*Linus Fast och Ron Lennartsson*

## Inledande beskrivning

I detta kapitel behandlas sjöplattformar, dvs. bemannade och obemannade undervattens- och ytplattformar. På ytsidan innefattar detta ytstridsfartyg, plattformar för sjöminröjning och sjörörlig logistik samt i ökande grad obemannade plattformar. I undervattensdomänen innefattar detta ubåtar och i ökande omfattning obemannade plattformar kompletterade med fasta och utläggbara sensorsystem. De obemannade plattformarna kan verka under ytan, på ytan eller i luft.

Generellt sett är traditionella bemannade sjöplattformar mycket investeringstunga avseende såväl anskaffning, tekniskt vidmakthållande som bemanning över tid. Vanligen är livscykeln väldigt lång. Detta gör sammantaget att många länder har hamnat eller riskerar att hamna i ett otillfredsställande läge av kombinerad fåtalighetsproblematik och gradvis markant föråldring och förslitning av materielen.

De utdragna omsättningstakterna påverkar möjligheter och förutsättningar till att införa nya önskade systemförmågor negativt även om erforderliga nya teknologier och systemlösningar är kända och tillgängliga. Delsystem kan dock uppgraderas flera gånger under en plattforms livstid i syfte att dels vidmakthålla befintlig förmåga, dels tillföra ny förmåga.

Sjöplattformarna 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 de militära uppgifterna sjöövervakning, sjöfartsskydd, kustförsvarsoperationer samt andra typer av sjöoperationer som syftar till att skapa kontroll över sjöterritorium, alternativt att bestrida motståndares förmåga att etablera dito.

Marina plattformar utvecklas ofta utifrån ett operativt behov. De designas och konstrueras med utgångspunkt i vilka uppgifter de avses lösa och vilka förmågebehov som därmed behöver omsättas i en teknisk konkretisering. Därtill kan design och konstruktion behöva ta höjd för påverkansfaktorer som beror på i vilken typ av operationsmiljö plattformarna primärt avses användas. Exempelvis ställer Östersjöns unika förutsättningar särskilda krav för optimerad systemeffekt i samband med utveckling och anskaffning av kvalificerade marina plattformar för den svenska marinens behov.

Operationsmiljörelaterade påverkansfaktorer kan vara av olika natur. I fallet med Östersjön finns en direkt påverkan avseende geologiska och oceanografiska förhållanden med grunda och skiktade vatten som påverkar manövrerbarhet, signaturer och spaningsförmåga. Utöver detta finns påverkansfaktorer som kommer sig av att

operationsmiljön har sin början redan i anslutning till svenska marina basområden (inget eller inga behov av transit till operationsområdet) samt att (åtminstone ytgående) marina plattformar hela tiden kan exponeras för mark- och luftburna hot.

Risken för upptäckt kommer förmodligen att öka markant, även för relativt signaturanpassade plattformar. Tiden mellan upptäckt och beslut om insats bedöms också bli kortare. Denna förbättrade lägesbild gäller i alla delar av sjödomänen men i olika utsträckning. Lägesbilden kommer bli relativt sett bättre på ytan eller i luften jämfört med lägesbilden i undervattensmiljöer, där sensorräckvidderna även fortsatt kommer vara begränsade. Detta innebär att det asymmetriska värdet av att kunna operera med undervattenssystem bedöms öka.

För närvarande pågår en rad aktiviteter för att modernisera den svenska marinen, t.ex. uppgraderingar av korvetter och ubåtar samt anskaffning av ubåtar och nya ytstridsfartyg. Därtill sker en transformering av amfibieförmågan, syftande till att amfibiesystemet ska bli mer sjörörligt och att det ska kunna verka mot sjömål på väsentligt större avstånd än vad den egna sensorförmågan på enskild skjutande båt medger. Vidare pågår förberedande studier inför anskaffning av nästa ubåtsgeneration. Ett flertal länder i närområdet har på liknande sätt pågående omsättningsprogram.

Med anledning av senare års kraftigt försämrade säkerhetspolitiska utveckling bedöms det sannolikt att numerären av kvalificerade sjöplattformar kommer att utökas under kommande decennium. Produktion av kvalificerade plattformar tar dock tid, både på grund av materielens komplexa natur och att de industriella resurserna kraftigt har reducerats sedan slutet av det kalla kriget. Den bedömda tillväxten kommer därför att ta åtminstone något decennium. I sammanhanget kommer enskilda nationer att, som beställare av dessa plattformar, behöva göra vägval avseende traditionella systemlösningar baserade på beprövade teknologier och system för att riskminimera avseende leveranssäkerhet och ekonomi eller att exploatera nya teknologier och system, för olika former av förmågeutveckling inom sjöstriden.

Givet förväntad livslängd för dessa plattformar kommer de ovan nämnda vägvalen att ligga till grund för stommen av örlogstonnage som kommer finnas 2050. Det betyder att olika nationer, med sina olika plattformar, kommer ha olika möjligheter och förutsättningar att införa operativ nytta av tekniska framsteg till 2050.

Obemannade system är redan viktiga och kommer att spela en allt större roll i framtida marina operationer i perioden fram till och bortom 2050. I tidsperspektivet fram till 2050 ser vi främst att obemannade system kommer nyttjas i samverkan med bemannade plattformar, men successivt kommer obemannade system sannolikt kunna lösa allt fler och mer komplexa uppgifter självständigt.

I vilken takt och omfattning obemannade system kommer nyttjas beror till stor del på benägenheten att i relativ närtid ta tekniska och ekonomiska risker. Dessutom finns juridiska aspekter som behöver omhändertas för att möjliggöra införandet av

obemannade och autonoma system på bredare front. Med låg benägenhet till risktagning kan valet bli att omsätta en plattform med en ny liknande plattform; att vara evolutionär snarare än revolutionär. Detta kan skapa ett relativt underläge gentemot en kvalificerad motståndare som satsat på mer revolutionära system/plattformar.

Införandet av obemannade system behöver betraktas som både ett medel för egen förmågeutveckling och som ett hot, avseende motsvarande införande av obemannade system på motståndarsidan. I den ständigt pågående duellen mellan medel och motmedel kommer således behovet av att hantera stridsekonomiska aspekter att bli än mer central än vad den varit fram tills nu.

## Trender och exempel

### Ubåtsoperationer

Ubåtar kan nyttjas för en mängd uppgifter i hela konfliktskalan: spaning, underrättelseinhämtning, specialoperationer, undervattensarbete, minkrig, ubåtsjakt, sjömålsbekämpning och markmålsbekämpning. Den sista företagstypen innefattar kryssningsrobotar från konventionella ubåtar såväl som från atomubåtar (SSG/SSGN), samt ballistiska robotar från strategiska atomubåtar (SSBN).

Både nationellt och internationellt finns svårigheter (teknologiska, industriella, kompetensmässiga och finansiella) med att över tid vidmakthålla och utveckla ubåtsplattformar. Trots dessa svårigheter 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.

Förmåga till dolt uppträdande är en grundförutsättning för ett framgångsrikt genomförande av ubåtsoperationer. Konventionella ubåtar har idag 20 till 50 dygns operativ uthållighet, det vill säga 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). Baserat på utvecklingen av luftoberoende 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. Batteriutvecklingen bidrar också till ökad uthållighet, bly-syra-batterier kommer att ersättas med Li-jon. Li-jon och andra moderna batteritekniker kommer också väsentligen öka uthålligheten för ubåtar och obemannade undervattenssystem (UUV:er). På lite längre sikt kan metallförbränning tänkas ge möjlighet till ännu längre uthållighet och internationellt studeras och testas även lågeffektsreaktorer för ubåtar och stora UUV:er. I takt med att

ubåtens energisystem möjliggör längre tid i undervattensläge ställs hårdare krav på navigationssystem och livsuppehållande system såsom luftrening och syresättning.

Ubåtsutvecklingen förutsätter fortsatt förmåga till enskild strid men förmågan till strid med system i samverkan förutses få allt större betydelse i tiden fram till och bortom 2050. Detta innebär ett större fokus på nya sensorer, vapensystem och bredbandig informationsöverföring, såväl för den egna plattformen som för snabbt utläggbara system och UUV:er – i syfte att få en bättre systemeffekt i ubåtens eller angränsande operationsområden. Parallellt sker därför en utveckling av obemannade och autonoma system som komplement till ubåten i genomförandet av dess olika uppgifter.

Utvecklingen går mot system i samverkan där ubåten kan verka med långräckviddiga torpedsystem som avfyras och uppdateras med extern måldata som möjliggör vapeninsats mot mål långt bortom egen plattforms sensorräckvidd. Denna utveckling gör att ubåten i än större utsträckning kan bidra till tröskeleffekt samt att skapa osäkerhet för fienden i större geografiska områden. Vidare medför möjlighet till vapeninsats på större avstånd att ubåtens överlevnadsmöjligheter förbättras då skjutmomentet är ett signaturhöjande, om än transient, moment som riskerar röja ubåtens position. Detta ställer i sin tur krav på torpedens räckvidd och signatur tillsammans med andra fjärrstridsmedel som exempelvis beväpnade UUV:er och autonoma undervattensfarkoster (AUV:er) med stor räckvidd.

För att ubåten ska förbli oupptäckt även i undervattensläge sker kontinuerligt utveckling för att reducera ubåtars signaturer, i huvudsak akustiska, elektriska och magnetiska. Passiva röjningsavstånd för moderna konventionella ubåtar är i dag mycket korta. I grunda områden och förträngningar utgör dock fasta eller utläggbara sensorsystem och/eller mineringar alltjämt ett reellt hot. Vidare utrustas allt fler ubåtsjaktenheter med lågfrekvent aktiv sonar (ATAS) med i många fall relativt stora räckvidder. Det är därför av stor vikt att reducera den aktiva målekostyrkan för att reducera dessa systems detektionsavstånd, vilket gör användning och vidareutveckling av ekodämpande beläggningar viktig. Ett ökat hot från bi- och multistatiska aktiva sonarer understryker behovet av ekodämpade beläggningar.

I det fall ubåten upptäcks av fienden och därmed riskerar utsättas för ett fientligt torpedangrepp är det av stor vikt att kunna undkomma/möta detta hot. Även i detta skede är ubåtens låga signatur viktig. Vidare krävs förmåga att upptäcka och med fördel lokalisera de inkommande torpederna så tidigt som möjligt för att skapa möjlighet till motåtgärder. Tänkbara motåtgärder innefattar störning, vilseledning samt förstörande motmedel. Internationellt pågår för närvarande utveckling av Anti-Torped-Torped (ATT) system som ska skjutas mot den inkommande torpeden i syfte att förstöra den.

Införandet av obemannade undervattenssystem innebär att vi successivt i perioden fram till 2050 kommer behöva utveckla skydd mot en breddad hotbild som inkluderar beväpnade obemannade system som kan uppträda enskilt eller i grupp.

### Ytstrid – inkluderande eskort och luftförsvar

Under perioden sedan det kalla kriget tog slut har många länder – inte minst inom Europa – skalat ner numerär avseende kvalificerade ytstridsfartyg. Därtill har fokus snarare legat på vidmakthållande och viss anpassning av befintlig fartygmateriel, snarare än omsättning och nyanskaffning. Överlag föreligger därmed ett tidsintervall med ganska utbrett omsättningsbehov som kommer generera ryggraden av det fartygsbestånd som fortfarande kommer vara operativt fram till 2050. En del länder har beställt nya fartyg och andra länder står på tur, däribland Sverige.

Med idag rådande säkerhetspolitisk utveckling finns, utöver det direkta omsättningsbehovet av befintliga fartyg som faller för åldersstrecket, önskemål om såväl kvantitativ som kvalitativ förmågeutveckling – man vill ha fler fartyg och man vill därtill se en vidare marin förmågeutveckling baserad på enskilda tekniska system, exempelvis högeffektlasrar och andra tillämpningar med pulsad (el-)kraft, exempelvis HPM, som alternativ till kinetiska verkans- och skyddssystem, men även på högre systemnivåer genom förmåga att operera med system i samverkan. Det kan röra sig om samverkan mellan traditionella sjö- och luftplattformar, men även ett utökat införande av obemannade system i sjödomänen.[195]

Ett sätt att hantera de höga kostnader som är förknippade med investeringar i marin materiel, särskilt om både kvantitet och kvalitet ska beaktas, är att man diversifierar anskaffningarna – man använder enklare fartygssystem eller obemannade system för mindre kvalificerade, men nog så ansträngande, uppgifter som exempelvis sjöövervakning. Parallellt utvecklas mer kvalificerade fartygssystem för den direkt väpnade stridens behov.

Bakgrunden till denna trend ges på ett tydligt sätt i en artikel[196] om hur man inom Royal Navy (RN) försöker vidmakthålla operativa krav på antal fartygsplattformar genom att ersätta gamla system med en mix av dyra, kvalificerade, fartyg (Type

195 US Navy demands uncrewed warships delivered in 18 months, https://www.navylookout.com/us-navy-demands-uncrewed-warships-delivered-in-18-months/.

196 COMMENT: The Dilemma Behind The Navy's Type 26 And Type 31 Frigates, 2018-09-05, https://www.forces.net/stories/comment-dilemma-behind-navys-type-26-and-type-31-frigates.

26) och billigare, enklare, fartyg (Type 31) med lägre operativ förmåga.[197] Utifrån perspektiven hybridkrigföring och gråzonsaktiviteter kan man ytterligare behöva stärka numerären av fartyg för sjöövervakning och annan form av närvaro till sjöss över tid. I detta perspektiv ser lösningarna lite olika ut för olika nationer, beroende på hur den enskilda nationen har organiserat sitt sjöförsvar, med möjliga uppdelningar mellan en militär gren och en eventuell civil del (kustbevakning).

Med ”strid i samverkan” avses oftast förmåga till vapeninsats där skjutande plattform understöds med måldata från externa (främst eleverade/flygburna) sensorsystem. En sådan system-av-system-funktionalitet öppnar för det enskilda ytstridsfartyget att verka med långräckviddiga robotsystem på avstånd som vida överstiger fartygets egen sensorräckvidd. Därtill skapas viktiga förutsättningar till integrerat luftförsvar (IAMD) där egenskyddet hos enskilt fartyg kan ökas då luftvärnsrobotar kan skjutas mot inkommande hot som ännu ej befinner sig inom fartygets egen sensorräckvidd. Därtill bidrar en gemensam förmåga till att skapa och dela måldata mellan olika skjutande enheter, vilket innebär att den sammantagna förmågan till områdesluftförsvar blir märkbart högre än summan av de enskilda fartygens förmåga.

Den ovan beskrivna förmågan till system i samverkan finns operativt införd inom USN[198] och är under utveckling och/eller införande hos ett antal andra nationer.[199] Inom Europa bedrivs liknande utveckling, bland annat av Royal Navy[200], men även inom ramen för EU:s EDF-program,[201] varför denna typ av övergripande förmågeutveckling bedöms vara möjlig att operativt införa på bredden hitom 2050 även för andra, ”mindre”, sjönationer.

Förmågan till system i samverkan utgår från att ingående sensornoder företrädesvis opererar i aktiv sändande mod, men att skjutande enheter, vilka rimligen även

197 Se även:

Offshore Patrol Vessel Missions in Wartime, http://cimsec.org/opv-missions-wartime/8741.

‘Upgunned’ OPVs are still only constabulary vessels, https://www.defenceconnect.com.au/maritime-antisub/6208-even-upgunned-the-opvs-are-still-only-constabulary-vessel.

Universal appeal: OPVs and corvettes proliferate, https://www.naval-technology.com/features/universal-appeal-opvs-and-corvettes-proliferate/?cf-view.

Japan starts production of a new fleet of OPV, https://www.navalnews.com/naval-news/2025/04/japan-starts-production-of-a-new-fleet-of-opv/.

198 USN CEC- och NIFC-CA-koncept, se exempelvis https://secwww.jhuapl.edu/techdigest/Content/techdigest/pdf/V16-N04/16-04-APLteam.pdf och https://secwww.jhuapl.edu/techdigest/Content/techdigest/pdf/V23-N2-3/23-02-Grant.pdf.

199 Se exempelvis: https://militaryaerospace.com/computers/article/16714560/navy-beefingup-air-defense-capabilities-of-us-japan-and-south-korea-surface-warships, https://adbr.au/cec-engaged-ran-tests-cooperative-engagement-capability-on-new-hobart-class-ddgs/ och https://www.shepardmedia.com/news/digital-battlespace/us-and-canadian-navies-to gain-planar-array-antennas-for-cooperative-engagement-capability/.

200 https://www.navylookout.com/options-for-the-royal-navys-future-air-dominance-system-and-the-type-83-destroyer/.

201 Se exempelvis “Naval Collaborative Surveillance” (EDF WP 2022) och “Digital Ship and Naval Combat Cloud” (EDF WP 2025).

de utgör en sensornod, ska kunna operera passivt och genomföra vapeninsats på externa måldata. Detta gör sammantaget att de enskilda ytstridsfartygens behov av (och syfte med) signaturanpassning förändras. Behovet utgår dock inte.

Teknikutvecklingen gör att havsområden som inte täcks av egna och/eller fientliga sensorer i sjödomänen blir avsevärt mindre – särskilt för små och avgränsade hav som Östersjön. Risken för upptäckt kommer förmodligen att öka markant, även för relativt signaturanpassade plattformar. Tiden mellan upptäckt och beslut om insats bedöms också bli kortare. Till detta ska läggas den vapentekniska hotutvecklingen som medger allt högre hastigheter, längre skjutavstånd och eventuellt stöd med extern måldatahantering. Relationen mellan vapenhot och skyddsförmåga kan framöver komma att leda till att traditionella fartygsutformningar får olika operativ relevans avseende överlevnadsförmåga i olika insatsmiljöer med olika förutsättningar för påverkan från exempelvis markbaserade långräckviddiga system. Möjligen kan det därför behöva utvecklas olika konceptuella lösningar för hur nödvändiga förmågor ska realiseras för lösande av definierade uppgifter i varierande insatsmiljöer med associerade hot.

Avseende skyddsfunktionen ligger utmaningen i att åstadkomma en kostnadseffektiv och förmågemässig balans mellan smygteknik (signaturanpassning och taktiskt uppträdande), motmedelssystem som matchar målsökarutvecklingen samt utvecklade luftvärnssystem som kan verka i olika lager/räckvidder och riktningar. Hotutveckling kopplat till införande av hypersoniska sjömålsrobotar kommer att bli en stor utmaning att hantera. Därför är utbyggnaden av den marina luftförsvarsförmågan väsentlig för att bibehålla den marina handlingsfriheten.

### Ubåtsjakt

Ytstridsfartygen kommer även i framtiden bedriva ubåtsjakt tillsammans med helikoptrar och obemannade system (farkoster), med stöd av fasta och/eller utläggbara undervattenssensorsystem med associerade funktioner för undervattenskommunikation. Därtill föreligger ett behov av att utveckla snarlika (eller identiska) lösningar för att hantera hotet från obemannade undervattensfarkoster.

För svensk del finns särskilda behov av att utveckla en mer breddad ubåtsjaktförmåga med såväl bunden ubåtsjakt för skydd av strategiska sjötransporter som fri, obunden, ubåtsjakt på öppet hav för etablerande av sjökontroll inom ramen för Natooperationer.

Nya plattformsbundna lågfrekventa aktiva sonarsystem (ATAS) ger betydligt större upptäcktsavstånd mot ubåtar, även i hög spaningsfart, än tidigare aktiva sonarer. Genom införande av obemannade system, på och under ytan, som bär sensor- och/eller vapensystem, erhålls ett effektivare skydd genom att den sammantagna ubåtsjaktsfunktionen kan verka längre från skyddsobjekten vid bunden ubåtsjakt och därutöver kontrollera ett avsevärt större havsområde än med dagens system. Nyttjandet

av bi- och multistatisk sonarteknik och andra former av datafusion gör det svårare för ubåten att undkomma ubåtsjaktenheterna genom taktiskt uppträdande.

För skydd av farleder och andra skyddsvärda områden kan fasta undervattenssensorsystem ge tidig förvarning som medger upprättande av taktiska sökområden som kan avreglas eller förtätas ytterligare med utläggbara sensorsystem eller snabba ytgående obemannade farkoster med sensor- och vapensystem. Vissa grunda och svåravsökta områden inomskärs kan snabbt avspanas med luftburen lidar[202], vilket effektiviserar ubåtsjakten för enheter med aktiva spaningssonarer. Flygburen MAD[203] kan också bidra till ubåtsjaktförmåga, men har bäst potential i djupare havsområden där ingen eller åtminstone betydligt lägre påverkan från antropogena effekter och/eller störning från geomagnetiska anomalier i havsbotten föreligger. Nyttjande av MAD kan även tillämpas i kustnära/grunda vatten, men förutsätter då att geomagnetiska förhållanden i insatsområdet är kända, så att metoder för skillnadsdetektion kan användas.

Vid sidan av torpedinsats från fartyg, helikopter och obemannade plattformar kan raketburna undervattensstridsdelar, som kan avfyras från land eller fartyg, medge snabb vapeninsats mot undervattensfarkoster på invisning från förekommande sensorsystem inom insatsområdet.

### Sjöminkrig

Trenden inom området sjöminröjning är att traditionella minröjnings-/minjaktfartyg kompletteras, eller ersätts, med obemannade system fram till 2050.

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[204], är att man använder autonoma/semiautonoma självgående (ytgående och/eller undervattensfarkoster) system för detektion, klassificering och eventuellt även röjning av sjöminor. De mer futuristiska stegen är utveckling av kvalificerade system av system där obemannade/autonoma farkoster i realtid samverkar med varandra, utläggbara sensornoder samt traditionella minröjningsfartyg. En drivande förutsättning för detta är operativt införande av länkar och nätverk för undervattenskommunikation.

Ett väsentligt och effektgivande tekniksprång som kommer ha stor framtida påverkan är operativt införande av autodetektion och klassificering av minor och minliknande objekt på botten och nere i bottensediment med hjälp av autonoma system. CAD/CAC[205] är en förutsättning för sådan autonom förmåga och bedöms operativt realiseras i perioden fram till 2050.

202 Lidar: Ligth detection and ranging.

203 MAD: Magnetic Anomaly Detection.

204 Pågående materielanskaffning i Italien, Nederländerna, Frankrike och Belgien.

205 Computer Aided Detection/Computer Aided Classification.

Trots teknikutvecklingens möjligheter bedöms framtida sjöminröjning behöva kunna hanteras genom såväl minjakt som minsvepning.

När det gäller sjöminering kan konstateras att sjöminan, såväl utifrån ett historiskt som ett framtida perspektiv, utgör ett strategiskt vapensystem som i många delar även är tillgängligt för mindre sjönationer. Den psykologiska effekten av sjöminans (eventuella) förekomst inom större eller mindre havs-, kust- och skärgårdsområden gör att en avskräckande tröskeleffekt och avregling kan åstadkommas i grunda havsområden som lämpar sig för sjöminering. Hit räknas, i princip, hela det maritima svenska närområdet i form av Östersjön, Kattegatt, Skagerack och det vidare utloppet mot Nordsjön.

Sjömineringarna ställer en motståndare inför vägval som kan ha stor påverkan på operativa förlopp i stort, inte bara till sjöss, då motståndaren behöver avväga risker, tidsförluster och andra möjliga konsekvenser kopplade till alternativen att helt avstå sjöfart genom minerat område, röja/svepa minerat område eller att med hög risktagning segla igenom minerat område.

Minparken, sett ur ett globalt perspektiv, utgörs fortfarande – volymmässigt – av traditionella minor (förankrade kontaktminor samt förankrade eller bottenliggande avståndsverkande minor). Även äldre avståndsminor bedöms vara operativt relevanta fram till och bortom 2050 genom uppgradering av minsensorer och minalgoritmer. En av de största begränsningarna avseende sjöminering med dessa minsystem är tillgång till fartygstonnage (och skydd av dessa) som rent logistiskt kan lägga ut stora mängder minor.

Vid sidan av vidmakthållande och utveckling av traditionella sjöminor sker utveckling av rörliga sjöminor med kvalificerad sensorfunktionalitet, som med allt större räckvidder, mer eller mindre autonomt, kan transportera sig fram till ett långt framskjutet läge, varvid det operativa djupet, tekniskt sett, kan föras ända in i motståndarens utskeppningshamnar.

## Samverkande och förutsättande förmågor och tekniker

### Obemannade system i sjödomänen

Med obemannade system (autonoma eller ej) avses här huvudsakligen obemannade farkoster (undervattensfarkoster, ytgående farkoster och/eller flygande farkoster) som, enskilt eller som ingående i ett system-av-system, bär tekniska systemkomponenter, delsystem eller system som bidrar till realiserande av önskade förmågor.

Obemannade system har använts i flera decennier ombord på bemannade sjöplattformar. Det kanske tydligaste exemplet är fjärrmanövrerade undervattensfarkoster, bestyckade med kameror och mekaniska griparmar eller annan utrustning, som opereras genom bunden kabelförbindelse mellan farkosten och ett traditionellt

minjaktfartyg. Detta är ett exempel på ett enskilt obemannat system som utgör förmågehöjande *add on* till en traditionell plattformsorienterad systemdesign (fartygssystem).

För närvarande sker internationellt en kraftig utveckling av olika typer av obemannade system i form av fritt rörliga (utan kabelförbindelse) farkoster som främst bär nyttolaster i form av sensorer för detektion, lokalisering, följning, klassificering och identifiering av mål i luften, på ytan och under vattnet. Utveckling av dessa system bedrivs i ökande omfattning också i Sverige. Andra exempel på önskade tillämpningar är att använda obemannade system för miljökartering (inte minst bottenkartering), störning och vilseledning och som rörliga noder i kommunikationsnätverk. Redan idag finns exempel på obemannade system som är beväpnade. Utvecklingen av obemannade autonoma farkoster med verkansfunktion kan i västvärlden komma att begränsas eller försenas exempelvis med hänsyn till överväganden om deras legalitet och olika säkerhetsaspekter, inkluderande risk för felfunktion. En motståndare som inte tar lika stor hänsyn till sådana faktorer kan sannolikt utveckla förmåga inom detta område snabbare eller komma längre i utvecklingen.

De i sjödomänen förekommande obemannade systemen leds vanligen av en operatör som befinner sig ombord på en bemannad sjöplattform, vilken kan ha förmåga att leda ett flertal obemannade system av samma sort eller av olika typer. Dessa obemannade system utgör då, var för sig, förmågehöjande *add on* till olika funktioner i en traditionell plattformsorienterad systemdesign (fartygssystem). Vinsten är, utöver skydd av bemannad sjöplattform, betydande förmåga till ökad yttäckning långt bortom den bemannade sjöplattformen och dess ”funktionsporté” med sina egna, plattformsbundna tekniska system – sensorer, ledning och vapen för såväl luftförsvar, ytstrid som undervattensstrid. Redan idag kan obemannade system utgöra värdefulla, stödjande, komponenter i verkansfunktioner genom deras förmåga att generera och delge måldata till traditionella skjutande enheter. Dessa enheter får på detta sätt utökade möjligheter att nyttja den potential som finns inom långräckviddiga vapensystem, såsom mark- och sjömålsrobotar samt torpeder, men även för att få ut bättre effekt ur luftvärnssystem som till sjöss ofta blir begränsade av att fartygens egna, mastmonterade, sensorer begränsas av korta horisontavstånd.

Operativt införande av obemannade system har, genom teknisk integration mot bemannad plattform, en direkt påverkan på i princip samtliga grundläggande förmågor[206], varför dessa framöver kommer behöva sättas i en tydlig system-av-system-kontext på förbandsnivå eller högre, snarare än som idag kopplas till enskilda traditionella sjöplattformar.

Införandet av obemannade, och på sikt även autonoma, system kan ske i den takt önskade förmågekrav kan mötas med tekniska systemutformningar som är

206 TURVLUS: Tillgänglighet, Underrättelser, Rörelse, Verkan, Ledning, Uthållighet, Skydd.

ackrediterarbara mot gällande lagkrav, vilka över tid kan komma att justeras. Givet detta är det rimligt att vi under resan mot 2050 kommer att se en utveckling där, stegvist:

- Mängden av operativa obemannade *add-on*-system kraftigt ökar och att de nyttjas tillsammans med bemannade sjöplattformar.
- Autonoma, obemannade, farkoster helt själva (ensamma eller i grupp – möjligen som svärm) löser, från början enklare och sedermera allt mer komplexa, uppgifter som traditionellt har lösts med bemannade sjöplattformar.
- System-av-system-arkitekturen förändras så att tekniska systemkomponenter, delsystem eller system som bidrar till realiserande av önskade förmågor – mer eller mindre – avförs från bemannade sjöplattformar för att i stället bäras av ett system-av-system av samverkande obemannade system. Dessa har då tagit steget från att vara *add on* till att bli förmågebärande materielkomponenter. Bemannade sjöplattformar kan i denna kontext nyttjas som moderfartyg, inte minst för att säkerställa expeditionär förmåga i sjödomänen.

Framtiden kommer få utvisa om/när utvecklingen når så långt att förekomst av traditionella bemannade plattformar inte bara ifrågasätts utan även avförs till förmån för autonoma system.

### Energi

I resan fram mot 2050 finns det en helt avgörande utmaning som det idag inte finns en lösning på, och som föranleder en stor oro. Det är energiomställningen och därmed associerad utfasning av fossila drivmedel och bränslen. Till lands, särskilt avseende energiomställning inom civil transportsektor, avses omställningen i allt väsentligt baseras på elektrifiering av transportsystemen. Av flera skäl är det närmast omöjligt att idag se elektrifiering som annat än ett perifert bidrag till omställning av den civila sjöfarten. För militär sjöfart är förutsättningarna, om möjligt, än värre.

För ubåtar och undervattensfarkoster i övrigt finns visst ljus i form av bränsleceller, nya batterier och, på längre sikt, metallförbränning. För ytfartyg saknas idag (annat än möjligen reaktordrift) mogna och säkra alternativa koncept som möter idag vanligt förekommande krav på effektuttag under lång tid och elförsörjning av ombordvarande förbrukare (tekniska system).

## Aktörer

I princip alla betydande maritima nationer bedriver nationell FoU och har både varvs- och sjöfartsnäring samt sjöstridskrafter. Sammantaget utgör detta grunden i de internationella maritima strategierna och är även ett medel för att hantera internationell lagstiftning avseende sjöfart. Flera länder har dessutom fler än en FoU-organisation samt ett flertal branschorganisationer för utveckling.

USA, Storbritannien, Kina, Ryssland och Indien är de som främst driver utvecklingen inom det marina området. Operativt införande av framförallt amerikansk teknologi sker dock i bland annat Japan, Sydkorea, Kanada, Australien och Nya Zeeland.

Alla större västliga marina nationer bedriver forskning och utveckling av marina system och plattformar, exempelvis Frankrike, Tyskland och Holland. Därutöver sker verksamhet i Norge, Sverige, Danmark med flera nationer. Dessutom bedrivs utveckling allt mer inom ramen för internationell samverkan, exempelvis inom EU och Nato.

## Lästips

COMMENT: The Dilemma Behind The Navy's Type 26 And Type 31 Frigates, https://www.forces.net/stories/comment-dilemma-behind-navys-type-26-and-type-31-frigates.

Universal appeal: OPVs and corvettes proliferate, https://www.naval-technology.com/features/universal-appeal-opvs-and-corvettes-proliferate/?cf-view.

Royal Navy's future Large Uncrewed Surface Vessels and the datalink challenge, https://www.navylookout.com/royal-navys-future-large-uncrewed-surface-vessels-and-the-datalink-challenge/.

Grant, C.J., CEC: Sensor Netting with Integrated Fire Control, https://secwww.jhuapl.edu/techdigest/Content/techdigest/pdf/V23-N2-3/23-02-Grant.pdf.

Sutton, H.I., What The Ultimate Submarine Could Look Like In 20 Years, https://www.forbes.com/sites/hisutton/2020/08/14/what-the-ultimate-submarine-could-look-like-in-20-years/.

# Plattformar i luftdomänen

*Tomas Mårtensson*

## Inledande beskrivning

Paradigmen att luftherravälde är en helt central förmåga för framgång i kris och krig ligger fast. Men det finns idag en osäkerhet runt vilka förmågekomponenter (och balansen mellan dessa) som bäst möter framtidens utmaningar i luftdomänen.

Den effektivitet som luftvärn demonstrerat över bland annat Ukraina kombinerat med de förmågebidrag som operationaliseringen av enorma mängder obemannade flygsystem demonstrerat i olika tillämpningar är två faktorer som bidrar till denna osäkerhet.

Under 2020-talet sker nu ett tydligt skifte från att fokusera på luftoperativ verkan i miljöer med luftherravälde till att framgent äga förmågan att hantera motståndare som har högteknologiska system i stora volymer. Denna omsvängning kommer samtidigt som antalet bemannade stridsflygplan i Väst aldrig varit så lågt som nu.

Utvecklingen av koncept för obemannade flygfarkoster som ska samverka med bemannat stridsflyg drivs med högt tempo. Dessa adjunktsystem[207] (eng. *collaborative combat aircraft*, CCA) är under införande i USA.[208] Målsättningen är att dessa system kostnadseffektivt ska skapa luftoperativ förmåga i många taktiska situationer. De ska vara så billiga att de kan förloras i strid, uttrycket *affordable mass* används alltmer. Ett adjunktsystem måste dock kunna flyga så fort att det hänger med ett stridsflygplan under större delen av ett uppdrag, bära vapen- och sensorlast, ha någon form av signaturanpassning för att inte bli upptäckt och dessutom ha en mycket robust datalänk så att det faktiskt går att kontrollera systemet från ett bemannat flygplan. Många av dessa förmågor är kostnadsdrivande och det som USA kan anse vara billigt, kan för många andra länder vara en helt orimlig prisnivå. Det återstår också många utmaningar, både tekniska och legala, innan det går att se vilken potential dessa system faktiskt kan erbjuda.

USA har nu ca 25 års bred erfarenhet av att operera större fjärrstyrda flygsystem, främst från operationer i områden med luftherravälde. Ekonomiska aspekter kopplat till obemannade system är av mycket stort intresse inför framtida anskaffningar. För stora (och dyra) obemannade system har en del jämförande studier genomförts. Trots att obemannade system flyger betydligt längre pass, är billigare i inköp

207 Loyal wingman var det första samlingsbegreppet för denna typ av system och det används fortfarande. Remote Carrier (RC) och Autonomous Collaborative Platform (ACP) är andra vanliga ord för denna typ av system.

208 Införandet är under utprovning på Nellis AFB 53rd Wing (CCA Experimental Operations Unit). https://www.defensedaily.com/u-s-air-force-to-refine-cca-increment-2-concept-as-service-announces-buy-of-more-increment-1-aircraft/air-force/.

och har hög tillgänglighet så har de en kortare förväntad livslängd och havererar i större omfattning än bemannade system. Skillnaden i kostnad över systemets livscykel behöver därför inte vara så stor.[209]

För adjunktsystem behöver nya ekonomiska modeller förmodligen utvecklas för att kunna värdera ekonomiska relationer när förmågebidrag från bemannade respektive obemannade system ska balanseras. Nya snabba tillverkningsmetoder kan komma att sänka prisnivån för den typen av system signifikant.

Transformation mot alltmer obemannade luftplattformar har accelererats av pågående konflikter. Antalet obemannade militära flygsystem och användningen av främst små och medelstora system är idag på nivåer som ingen förutspådde för tio år sedan.[210]

Militärt delas flygområdet traditionellt in i stridsflyg, transportflyg och helikoptersystem. Det står klart att andelen bemannade flygsystem kommer fortsätta sjunka i relation till obemannade system i alla dessa kategorier.

Med få undantag kommer stridsflyguppgifter som mark- och sjömålsbekämpning, spaning och övervakning företrädesvis ske med obemannade system i perspektivet 2050.

## Trender och exempel

### Nya typer av plattformar

Vridbara framdrivningssystem är i sig inget nytt. Det har funnits operativt sedan länge på bemannade system, till exempel Harrier (jet) och med propellersystem (tilt-rotor) på Boeings Osprey. Stridsflygplanet F-35 finns i en vertikalstartande version. Förmågan till vertikal start och landning är givetvis operativt mycket attraktiv. För stora system är detta fortsatt en kostsam lösning som innehåller komplexa och tunga tekniska lösningar. Kompromisser måste göras vad gäller främst räckvidd (jet) jämfört med motsvarande traditionella system.

Vridbara rotorsystem växer starkt för mindre och medelstora obemannade system där tillverkarna försöker få bättre räckvidder och högre hastigheter jämfört med rena rotorsystem. Tillverkaren Bells koncept HSVTOL (*High Speed Vertical Take-Off and Landing*) är en vision för framtidens helikoptersystem. Rotorbladen används endast vid start och landning och hela framdrivningsinstallationen vrids sedan till horisontellt läge under flygning. Propellrarna fälls bakåt för lägre luftmotstånd

209 I en studie av US Congressional Budget Office har till exempel RQ-4 (Global Hawk) 17 % lägre livscykelkostnad än havsövervakningsflygplanet P-8 (ett derivat av Boeing 737), se US Congressional Budget Office. Usage Patterns and Costs of Unmanned Aerial Systems (2021) https://www.cbo.gov/ publication/57260.

210 Pådrivet av kriget mot IS, konflikterna i Nagorno-Karabach men särskilt Rysslands fullskaliga invasion av Ukraina.

och motorn övergår till att vara en jetmotor. Detta betyder att systemet flygs och kontrolleras som ett vanligt flygplan och därför kan flygas i hastigheter som dagens helikoptersystem inte klarar av.[211]

En jetdriven farkost för en person (*jet pack*) utvecklades redan på 1950-talet av Bell Aerosystems i USA. Systemet hade undermålig räckvidd och var mycket svårt att kontrollera. Programmet lades ner under 1960-talet.[212] Olika koncept har efter det prövats genom åren. Under 2000-talet har företag med hjälp av miniatyrisering av framdrivningssystem och bättre styr- och reglersystem utvecklat nya typer av personliga flygsystem som nu operationaliserats.[213] Systemen har fortfarande (mycket) begränsad räckvidd men används framgångsrikt av till exempel specialförband där förmågan att genomföra kortare flygturer i vissa moment ökar effektiviteten i verksamheten, till exempel vid bordning av fartyg eller förflyttning i oländig terräng.[214]

Mycket högt flygande plattformar med uppgifter för främst spaning har varit operativa sedan länge (till exempel de bemannade U2 och SR-71). Utvecklingen av fjärrstyrda obemannade flygsystem under 2000-talet har satt många typer av så kallade HALE- och MALE-system[215] i operativ drift. Global Hawk är det mest kända exemplet på ett HALE-system och kan operera på höjder upp mot 18000 meter, vilket är över all kommersiell flygtrafik. Uthålligheten är upp till ca 24 timmar för denna typ av HALE-system.

De nya typer av mycket högt flygande plattformar som nu studeras runt om i världen avses flyga ännu högre, på höjder mellan 20 och 40 km, och kunna vara uppe i veckor, månader eller år. Både plattformar som är lättare och tyngre än luft är i operativ drift om än i liten skala.[216] På engelska används ofta förkortningen HAPS som kan uttydas som *High Altitude Platform Systems*, ibland som *High Altitude Pseudo Satellites*.

De flesta systemen som utvecklas flyger mycket sakta och högt. Nya typer av framdrivning med stora inslag av eldrift (från solpaneler), batteri- och hybriddrift studeras. Farkosterna är känsliga för turbulens och kräver lugna väderförhållanden vid start och landning. Lastförmågan är också mycket begränsad.

Mycket av marknadsföringen runt dessa system lovar ”rymdförmåga” till betydligt lägre kostnad än traditionella rymdsystem. Givet den snabba utvecklingen som

211 https://www.bellflight.com/experience/innovation/hsvtol.

212 Flygtiden var ca 30 sekunder. Medialt fick systemet ett visst genomslag då det 1965 använde i James Bond-filmen ”Åskbollen” och när det 1984 var en del av invigningsceremonin vid OS i Los Angeles.

213 https://gravity.co/.

214 Royal Marines Jet Suit Boarding Exercise.

215 MALE och HALE, Medium (High) Altitude Long Endurance.

216 Se till exempel: https://aerostar.com/ för ballongsystem eller https://www.baesystems.com/en/article/phasa-35--completes-first-successful-stratospheric-flight för fixed wingsystem.

sker på rymdsidan med ökad kommersialisering och prispress är det idag svårt att bedöma framtiden i detta avseende.

### Stridsflygutvecklingen

År 2050 kommer det vara 62 år sedan JAS 39 genomförde sin första flygning, motsvarande siffra för F-22 är 53 år. Systemet F-35 som flygs av de flesta större länder i väst kommer att ha varit operativt i 34 år och har mest sannolikt uppgraderats några gånger fram till 2050.[217] Av de utvecklingsprojekt i väst som syftar till utveckling av nästa generation stridsflygsystem är USA:s *Next Generation Air Dominance* (NGAD) det som idag kommit längst där Boeing i mars 2025 tilldelats utvecklingen av NGAD. US Air Force beteckning kommer bli F-47 för systemet.

F-47 förväntas bidra till ett säkrat luftherravälde och har varit under utveckling sedan mitten på 2010-talet. Plattformar kopplade till programmet har flugit i flera år enligt Pentagon. Även om väldigt lite är känt om flygplanet har de flesta bedömare antagit att systemet kombinerar låg signatur och flygprestanda till en ny världsledande nivå, väl över F-22.[218] US Navy driver också ett sjätte generationens stridsflygprogram med beteckning F/A-XX.[219]

USA:s erfarenheter från utvecklingen (och kostnaderna) av det extremt smyganpassade bombflygsystemet B-21 kombinerat med de möjligheter som adjunktsystem erbjuder gjorde att USA under 2024 satte programmet NGAD på paus för vidare utredning. Osäkerheter fanns om NGAD, i sin ursprungliga design, kommer lösa förväntade militära problem på ett kostnadseffektivt sätt.[220] Orsaken är USA:s fokus på Kina som militär motståndare. Det driver delvis nya förmågebehov. Kombinationen av det geografiska avståndet till Kina från möjliga amerikanska baseringsplatser tillsammans med Kinas alltmer högkvalificerade system[221,222] i stora kvantiteter utgör viktiga ingredienser i det militära problemet US Air Force (USAF) har att hantera.

Med de räckviddskrav som kinaproblemet innebär för USA så krävs mycket bränsle i ett framtida stridsflygsystem. Med krav på låg signatur behöver bränslet bäras

217 F-35 blev operativt (IOC) 2016 i US Air Force.

218 https://www.af.mil/news/article-display/article/4131345/air-force-awards-contract-for-next-generation-air-dominance-ngad-platform-f-47/.

219 Vid skrivandet av denna text har ännu ingen industri tilldelats utvecklingen av F/A-XX.

220 Kongressens utredningstjänst (Congressional Research Service) beskriver i en rapport hur det ekonomiska handlingsutrymmet i Flygvapnet också pressas av utvecklingen av B-21, F-35 och en nödvändig omsättning av interkontinentala ballistiska missiler (Från Minuteman III till LGM-35 Sentinel). https://s3.documentcloud.org/documents/25499020/if12805-1.pdf.

221 https://www.twz.com/air/yes-china-just-flew-another-tailless-next-generation-stealth-combat-aircraft.

222 I konflikten mellan Pakistan och Indien har kinesiska stridsflygplanet J-10 i början av maj 2025 enligt uppgifter från USA skjutit ner två moderna Indiska (fransktillverkade) Rafale. https://www.reuters.com/world/pakistans-chinese-made-jet-brought-down-two-indian-fighter-aircraft-us-officials-2025-05-08/.

internt, vilket betyder att plattformen blir väldigt stor. En väl etablerad metod för att öka räckvidden in i ett stridsområde är lufttankning. De flesta lufttankningsflygplanen är idag derivat av civila passagerarflygplan och saknar helt smygförmåga. De förväntas operera i områden där minst lokalt luftherravälde är etablerat. USAF har därför initierat studier om möjlig utveckling av smyganpassade lufttankningsflygplan, *Next Generation Air refueling System* (NGAS), för att skapa bättre räckvidder utan att bli upptäckt.[223]

Inom stridsflygområdet är utvecklingen av mindre obemannade system under stark tillväxt. Dessa adjunktsystem är på papperet ett attraktivt system för att hantera den förväntat stora mängden av kinesiska system. USAF har 2024 öppnat sin första flottilj som rutinmässigt ska operera adjunktsystem och de första CCA-plattformarna har fått flygvapenbeteckningar.[224] Kinaproblemet innehåller också ett större behov av att minska riskerna för bekämpning genom att kunna basera utspritt, något som CCA-plattformar skulle kunna bidra med. Vid kungörandet av att Boeing tilldelas utvecklingen av NGAD trycks det särskilt på att det är en familj med system som ska utvecklas, som tillsammans erbjuder ny överlägsen luftoperativ förmåga.

Att F-47-systemet har ca 15 års operativ tjänst 2050 förefaller inte osannolikt. Något av de pågående europeiska programmen bör också ha ett system i operativ drift vid denna tidpunkt. Användningen av adjunktsystem kommer att ha fört oss närmare ett svar på frågan om i vilka typer av uppdrag de erbjuder ett reellt förmågebidrag.

Hur snabbt de två europeiska stridsflygprogrammen SCAF[225] och GCAP[226] kommer utvecklas är osäkert. Givet omvärldsläget är det rimligt att anta att finansiering är säkrad i Europa för program som siktar på nästa generations stridsflyg. Båda programmen står i närtid inför viktiga beslut om anskaffning. Stora långsiktiga ekonomiska åtaganden med politisk enighet mellan parterna i respektive konsortium kommer krävas. Det återstår att se om båda programmen går vidare, och med vilket tempo och teknisk ambitionsnivå.

Ett svenskt beslut om försörjningslösning för stridsflyg kommer före 2030. Om det beslutas om en nationell nyutveckling återstår alltså att se. Om det blir så är

223 US Navy har redan gått denna väg och håller på att operationalisera ett hangarfartygsbaserat obemannat system för lufttankning (Boeing MQ-25 Stingray).

224 De två första CCA-plattformarna benämns YFQ-42A (tillverkare: General Atomics) och YFQ-44A (tillverkare: Anduril). Prefixen ”Y” står för prototyp och tas bort vid införande, ”F” för fighter och ”Q” för obemannad. Detta är USA:s första system där ett fightersystem kombineras med beteckningen för obemannat. https://www.af.mil/News/Article-Display/Article/4092641/air-force-designates-two-mission-design-series-for-collaborative-combat-aircraft/.

225 SCAF är en fransk akronym för Système de combat aérien du futur. SCAF är ett internationellt program för att utveckla ett sjätte generationens stridsflygplan inom ramen för ett större systemkoncept. Under ledning av Frankrike genomförs programmet av Frankrike, Tyskland och Spanien. De större industriella aktörerna är Dassault Aviation, Airbus and Indra Sistemas.

226 Global Combat Air Programme (GCAP) är ett trilateralt program för utveckling av ett nytt stridsflygplan under ledning av Storbritannien där Italien och Japan deltar. De större industriella aktörerna är BAE Systems, Leonardo och Mitsubishi.

det mest sannolikt under 2040-talet ett sådant system operationaliseras. Den samlade grundkompetensen inom stridsflygförmågan i Europa är god, frågan är dock hur rationellt det är att driva två (kanske tre) parallella stridsflygprogram i Europa.

Signaturanpassning bedöms fortfarande vara viktigt, även om utvecklingen av sensorer för upptäckt av flygsystem blir allt bättre. Mindre (fysiskt) signaturanpassade flygsystem bedöms ändå förbli mycket svåra att upptäcka eller innebära mycket korta förvarnings- och reaktionstider för den som vill bekämpa denna typ av system.

### Transportflyg och helikoptersystem

Flera militära transport- och lufttankningsflygplan är derivat av civila produkter och följer därför i stort sett civil utveckling. Det finns också renodlade militära transportflygplan. De har möjlighet till start och landning på korta och ej hårdgjorda rullbanor. Det senaste tillskottet på den marknaden är Airbus A400M (2009), i övrigt uppdateras övriga äldre system i denna kategori med nya motorer och ny avionik, till exempel C-130 och C-17. En intressant utveckling för lufttankning är obemannade lufttankningsflygplan, som Boeings MQ-25 Stingray, som flög 2019 och planeras bli operativ från hangarfartyg i US Navy under 2020-talet. Plattformen antas också kunna utföra vissa spanings- och kommunikationsuppgifter. Systemet kommer att öka flexibiliteten och förmågan hos både F-35 och framtida obemannade eller bemannade system som kommer operera från hangarfartyg.

Många större operativa helikoptersystem är i sin grundkonstruktion från 1960-talet, till exempel Black Hawk, Apache, Chinook och Mi-8. Det finns ett stort behov av att omsätta dessa. Det finns flera större program som tittar på framtidens helikoptersystem (*future vertical lift).* Främst handlar det om att öka räckvidd, hastighet och lastförmåga jämfört med dagens helikoptersystem.[227] En av de tydligare utvecklingslinjerna för att nå detta mål är olika typer av tilt-rotorsystem som beskrivits under stycket om nya typer av plattformar.

## Särskilda delområden

Ökad automation för både bemannade och obemannade flygsystem är det område som de flesta parter avsätter mest resurser till. Förhoppningarna om att adjunktsystem ska kunna ge ett reellt förmågebidrag är starkt kopplade till att kontrollen över farkosterna sker genom avancerad automation som medger en människa-maskin-interaktion där den kognitiva belastningen för piloten inte ska öka jämfört med dagens bemannade system. Idag styr en pilot, som till exempel ansvarar för en fyrgrupp stridsflygplan sina underställda via tal och med kommandon via datalänk,

227 Dalenbring, M., Edefur, H., Fallqvist, B., Hall, J-O., Tysell. T. (2023) En översikt av globala trender mot framtida helikoptersystemförmåga ur ett utvecklingsperspektiv - Redovisning av en plattformsteknisk exempelanalys av ett generiskt helikoptersystem, FOI-R-5370--SE.

ett arbete som i en stridssituation är mycket krävande. Begreppet *teaming* används ofta som begrepp för denna typ av forsknings- och utvecklingsarbete som syftar till ett effektivt samarbete mellan människa och maskin.

Avgörande för användningen av adjunktsystem är hur samband (länkar), automation, teaming och insatsregler kan kombineras. Användningen av större obemannade system i konflikterna under 2000-talets inledning har oftast skett i områden med eget luftherravälde. Där har det funnits ett mycket säkert samband mellan farkost och pilot då data- och styrlänkar gått via satellit. Förhållandevis komplexa insatsregler med mycket detaljer och avgränsningar i tid och rum för uppdragen har gått att hantera. Frånsett plattform- och viss sensorstyrning har graden av automation varit låg. Mycket långa uppdragstider har varit ett annat kännetecken (6-30 h).

Adjunktsystem för stridsflyg i en miljö där användaren inte har luftherravälde ställer andra och nya krav. Mindre system kommer sannolikt inte ha plats för antenner för rymdkommunikation utan får istället förlita sig på någon form av störtålig riktad kommunikation. Tidstempot kommer vara högre då uppdragstiden förväntas bli kortare med en eller ett fåtal timmar för ett uppdrag. Kortare eller längre avbrott i kommunikation är sannolika. För att kunna hantera komplexa insatsregler och kontrollera och styra flera adjunktsystem från ett bemannat stridsflygplan i denna typ av miljö måste tekniken automatiseras till en högre nivå.

Ovanstående resonemang belyser främst hur förmågan ska realiseras tekniskt. Det finns dock ett stort behov av att värdera adjunktsystem i många andra perspektiv för att få en balanserad bild av de samlade kostnaderna för förmågan. Den militära beskrivningen av förmågor i termer av DOTMLPFI är en bra utgångspunkt för en sådan analys.[228] Nedan listas några exempel på frågeställningar som behöver belysas inför ett införande av adjunktsystem:

- Vilka behov av ny infrastruktur uppstår vid ett införande av adjunktsystem för till exempel lagring, transport och underhåll?
- Vilka nya personalkategorier kommer med ett införande av adjunktsystem?
- Hur ska start- och landningsplats väljas i relation till de bemannade systemen och tänkt insatsområde?
- Hur ser logistik- och underhållskedjor ut för respektive adjunktsystem?
- Hur ska systemen effektivt kunna prepareras, uppdragsplaneras och ges startorder?
- Hur ska flygsäkerhetsaspekter hanteras organisatoriskt?
- Hur ska träning av piloter, tekniker och operatörer av adjunktsystem ske?

228 DOTMLPFI är en indelning av påverkansområden för en verksamhet - Doctrine; Organisation; Training; Materiel; Leadership; Personnel; Facilities; and Interoperability.

- Hur ska samverkan mellan flera bemannade system och adjunktsystem tränas?
- Hur (om) ska integration med civilt luftrum hanteras för adjunktsystem?
- Vilka standarder måste adjunktsystem vara kompatibla med?

Design och tillverkning av flygsystem är ett område som kommer utvecklas starkt i perioden fram till 2050. Traditionella flygtekniska discipliner som aerodynamik, flygmekanik och flygsignaturer utgör fortsatt grunden för att ha förmågan att värdera, designa och utveckla koncept för flygsystem i traditionella och nya tillämpningar. AI-metoder tar en allt större plats även inom dessa traditionella områden. Metoder utvecklas för att avsevärt snabba upp designloopar, minska behovet av experimentella data och för att kunna inkludera fler parametrar när faktorer ska avvägas mot varandra vid design av flygfarkoster (till exempel kostnader och hållbarhet). Behovet av digitala tvillingar kommer öka för att kunna tillgodogöra sig AI-utvecklingen på området. Nya och mindre företag kan i framtiderna få det lättare att ta sig in på marknaden för militära flygsystem. Företaget Anduril som levererar ett av adjunktsystemen som USA nu håller på att införa (YFQ-44A) är ett sådant exempel.

Utvecklingen av materialteknik och nya tillverkningsmetoder är också områden som fortsätter att utvecklas starkt. Nya material kombinerat med 3D-tillverkning kan ge helt nya möjligheter till att enkelt tillverka strukturer med låg signatur eller att ge materialet i sig en funktion, till exempel som antenn eller sensor.

Om det blir kostnadseffektivt att tillverka adjunktsystem i stora volymer så kommer nya forskningsfrågor att behöva besvaras. I fred kanske ett fåtal plattformar finns som det övas på. Vid konflikt eller krig snabbtillverkas nya system efter behov. Vilka krav ställer det på lagerhållning (komponenter och maskiner) och var ska tillverkningsplatserna finnas sett ur ett militärt perspektiv? Hur affärsmodellen ser ut för en sådan lösning är också en fråga som behöver analyseras.

Träning och utbildning av piloter och operatörer av militära flygsystem kommer förändras för att möta den tekniska utvecklingen. Ett träningskoncept som integrerar verkliga flygplan, bemannade simulatorer och artificiella agenter kallas LVC; *Live, Virtual* och *Constructive*.

Inslaget av LVC kommer öka då det möjliggör mer krigslik träning där fler piloter kan öva i ett och samma scenario med fler entiteter (obemannade och bemannade). Samtidigt har LVC ekonomiska fördelar där distribuerad träning och datorgenererade mål och agenter inte kräver fysiska motsvarigheter. Utöver detta så har LVC fördelar då endast en begränsad del av scenariot kan observeras i verkligheten (i luften) och en motståndare därför har svårare att spionera och förstå tänkt taktiskt uppträdande.

## Påverkan på militär förmåga

### Militära tillämpningar

Flyg- och rymdsystem har sedan de infördes varit överlägsna i att skapa en bra lägesbild över ett geografiskt område. I en konflikt med en högteknologisk motståndare är vikten av att kunna upprätthålla förmågan till kontinuerlig luftbevakning, spaning och stridsledning helt central för militärt beslutsfattande där planering och genomförande av alla typer av luftoperationer sker.

På samma sätt som markstriden i kriget mellan Ukraina och Ryssland i stort sett blivit transparent och direktsänds i en mosaik från olika typer av drönare (på båda sidor) så kan samma utveckling komma att ske i luftdomänen över större områden. Idag levereras denna lägesbild för tidig förvarning och stridsledning till stor del av stora och komplexa flygande (bemannade) plattformar. Dessa har alltid varit högprioriterade mål och viljan till risktagning har varit låg med dessa system.[229] Deras förmågebidrag är också starkt beroende av sensorernas räckvidd och de kan därför inte operera för långt bort från ett intresseområde om de ska kunna leverera användbar information. Effektivare luftvärn och telekrigssystem kommer göra det svårare för dessa system att bidra till lägesbilden.

Mindre och fler obemannade luftplattformar som bidrar till lägesbilden i ett intresseområde kombinerat med rymdbaserade sensorer kommer utgöra byggstenar (för de resursstarka länderna) när de bygger framtidens förmåga att behålla informationsöverläge relativt sin motståndare.

Med få undantag kommer stridsflyguppgifter som mark- och sjömålsbekämpning, spaning och övervakning företrädesvis ske med obemannade system i perspektivet 2050.

Traditionella flygsystem har sedan länge använts inom land- och sjödomänen, historiskt främst för spaning och vissa typer av vapeninsatser. Vad som utgör ett flygsystem ur ett legalt perspektiv är ofta väl definierat men tekniskt är olika typer av patrullrobotar, drönare och alltmer avancerade markmålsmissiler också flygsystem. Med en sådan bred definition är användningen av obemannade flygsystem för mark- och sjötillämpningar kanske det område där utvecklingen kommer att bli som störst sett fram till 2050.

229 AEW&C – Airborne early warning and control. Exempel på system är svenska Global Eye, E-3 Sentry (USA, UK och Frankrike) och ryska A-50.

## Begränsande faktorer

*Militära och civila regler*

Frågor om hur ansvar och roller för adjunktsystem ska hanteras saknar idag svar, både sett till den militära ledningsstrukturen och ur ett flygsäkerhetsperspektiv, men det eftersträvas att så långt som möjligt nyttja beprövad metodik för företagsplanering. Inslagen av automation innebär även att folkrättsliga principer behöver beaktas, som till exempel kravet på mänsklig inblandning i beslutsfattande. FN:s panel *Convention on Certain Conventional Weapons* (CCW) har arbetat med frågan om autonoma vapensystem i många år. En grupp med experter från olika länder har getts uppdraget att under 2025 formulera ett ramverk med principer i frågan. Dessa ska inte skilja på vilken domän systemen verkar i.[230]

Civilt arbetar ICAO[231] med ett regelverk som har målsättningen att fjärrkontrollerade och bemannade system ska uppträda blandat och på lika villkor. Detta arbete har nu bedrivits under ca 15 år och det utvecklas efterhand regler och riktlinjer för hur nationer ska införa fjärrkontrollerade flygsystem i olika perspektiv.[232]

En viktig fråga för att detta ska bli verklighet är att fjärrstyrda system på ett säkert sätt klarar att upptäcka och undvika andra föremål i luften. Mycket forsknings- och utvecklingsarbete har lagts ner på detta område under 2000-talet. Då piloten styr från marken kommer det ställas särskilda krav på länkarna som används avseende data och cyberintrång. Den svåraste frågan att lösa är hur plattformsfel vid länkbortfall ska hanteras. Nödchecklistor, procedurer och metoder måste automatiseras till en sådan grad att flygsäkerheten kan bevisas vara på minst samma nivå som för bemannade system.

Det ska noteras att regelutvecklingen ovan hittills helt riktar in sig på antagandet om en pilot – en plattform. Själva flygningen (spakandet) är i stort sett helt automatiserad för fjärrstyrda system, något som också gäller för stora delar av dagens bemannande trafikflygplan. Den stora begränsande faktorn är fortfarande att flygning utom synhåll normalt inte medges för kommersiella aktörer. För myndighetsutövning (till exempel polis, kustbevakning och räddningstjänst) görs i många länder undantag vid behov.

Det finns också drivkrafter för att tillåta att en operatör kan hantera flera farkoster eller att systemet helt automatiseras (algoritmen flyger). Här återfinns många av

230 Ett utkast av ramverket (november 2024) återfinns på https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2024)/Revised_rolling_text_as_of_8_November_2024_final.pdf.

231 International Civil Aviation Organization.

232 En överskådlig sammanfattning AV ICAO:s arbete inom området finns i denna presentation: https://www.icao.int/APAC/Meetings/2024%20UASRPAS%20Webinar2/ICAO%20APAC_2nd%20Webinar%20UAS_RPAS_2024_Leonardo%20Haberfeld-1.pdf#search=Search%2E%2E%2ERPAS.

de initiativ som handlar om transport av varor och människor på korta distanser, ofta med drönare som drivs av el. Mycket forskning och olika försök har genomförts under 2010-talet och framåt.

Det är först under senare år som nu också ICAO på allvar tar sig an frågan och startar arbetsgrupper inom *Advanced Air Mobility* (AAM). Att USA:s luftfartsmyndighet[233] 2023 definierade *powered-lift-aircraft* som en ny kategori av luftfarkoster är också ett tecken på att det finns stort tryck i frågan.[234]

Regelutvecklingen bestämmer i praktiken vad som blir möjligt för alla aktörer (privata som statliga) som utvecklar produkter och tjänster för denna marknad. Beroende på hur regelverken kommer att se ut, kommer framtiden utvisa vilka av alla dagens initiativ som kan skapa bärande affärsmodeller för sin verksamhet. Persontransport (*taxi-on-demand*) i städer med obemannade vertikalstartande system, paketleveranser (gods och mat) på korta avstånd, medicintransport eller ambulanstransporter på längre avstånd är exempel på verksamheter många investerar i idag.

## Lästips

Leftwich, J.A., DeBlois, B., Ortetsky, D.T. (2022). Supporting Combat Power Projection Away from Fixed Infrastructure. RAND https://www.rand.org/pubs/research_reports/RRA596-1.html.

The Department of the Air Force In 2050; Report to Congressional Committees https://www.govexec.com/media/general/2025/1/department_of_the_air_force_2050.pdf.

Col Mark A. Gunzinger, USAF (Ret.) with Maj Gen Lawrence A. Stutzriem, USAF (Ret.) and Bill Sweetman. The Need for Collaborative Combat Aircraft for Disruptive Air Warfare. The Mitchell Institute for Aerospace Studies Air & Space Forces Association Arlington, VA February 2024, The-Need-For-CCAs-for-Disruptive-Air-Warfare-FULL-FINAL.pdf.

by Lt Col Jesse Breau, USAFKeeley Erhardt, MIT and Maj Joshua Reddis, USAF Collaborative Combat Aircraft Need Data to Train for Combat No. 52 April 2023 The Mitchell Forum, MI_Forum_52-CCA-Need-Data-to-Train-for-Combat-FINAL.pdf.

233 FAA – Federal Aviation Authority.

234 Det är FAA:s första nya kategori för luftfarkoster sedan helikoptern infördes för 80 år sedan. https://aerospaceglobalnews.com/news/faa-reveals-first-new-civil-aircraft-category-since-1940s/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Can%20Boeing%20recover%20from%20%246%20billion%20loss%20and%20continued%20strike%3F&utm_campaign=AGN%20SNAPSHOT%2024%2F10%2F2024 (Besökt 2025-03-17) På svenska är ”vertikalstartande flygsystem” kanske den bästa översättningen. Flygsystem som kan starta och landa vertikalt men inte är ett helikoptersystem. Militärt är stridsflygplanet Harrier och F-35C exempel på denna typ av system.

Five Imperatives for Developing Collaborative Combat Aircraft for Teaming Operations, Heather R. Penney, The Mitchell Institute for Aerospace Studies Air & Space Forces Association Arlington, VA October 2022, Five-Imperatives-for-Developing-Collaborative-Combat-Aircraft-FINAL.pdf.

Musco Eklund, A. (2020). Meaningful Human Control of Autonomous Weapon Systems – Definitions and key Elements in the Light of International Humanitarian Law and International Human Rights Law, FOI-R--4928--SE.

Stensrud, R., Mikkelsen, B. & Valaker, S. (2024). Exploring human-autonomy teaming methods in challenging environments: the case of fighter pilots and loyal wingmen. Human-Intelligent Systems Integration, https://doi.org/10.1007/s42454-024-00050-y.

Dalenbring, M., Edefur, H., Fallqvist, B., Hall, J-O., Tysell. T. (2023) En översikt av globala trender mot framtida helikopter-systemförmåga ur ett utvecklingsperspektiv - Redovisning av en plattformsteknisk exempelanalys av ett generiskt helikoptersystem, FOI-R--5370--SE.

# Rymd

*Jonatan Westman och Linn Claesson*

## Inledande beskrivning

Rymden utgör redan idag en aktiv arena i krig, konflikt och kris. Allt fler länder hanterar rymden som en operativ domän jämte mark-, sjö-, luft- och cyberdomänen. Detta möjliggör att egna militära förmågor kan förstärkas med hjälp av rymdbaserade funktioner. Genom att dessutom anpassa sina militära strukturer och doktriner har flera länder skapat bättre förutsättningar för att kunna bedriva militära operationer mot, genom och i rymden. Vissa länder har även etablerat renodlade rymdstyrkor och/eller rymdkommandon.

Rymden utgör en så kallad global allmänning (*global common*), det vill säga att ingen kan äga områden i rymden. Det finns inte heller några tydliga gränser i rymden på det sätt som de finns i de traditionella domänerna mark, sjö och luft. Rymden är därför tillgänglig för alla stater, och såväl civila som militära aktörer. Andra länders civila och militära satelliter rör sig därmed fritt i bana runt jorden och passerar över Sverige otaliga gånger per dag.

Satelliter är komplexa tekniska system som kan nyttjas som sensorbärare, kommunikationsnoder och/eller som vapenbärare. Satelliter kan verka enskilt, i formation med flera andra satelliter och/eller integrerat med system i andra domäner.

Utvecklingen av rymddomänens militära dimension avspeglas även här hemma i Sverige. År 2020 pekade Försvarsmakten ut rymden som en av de fem domäner som tillsammans utgör den fysiska miljön enligt Försvarsmaktens doktrin för gemensamma operationer, och 2021 lades det övergripande ansvaret för aktiviteter i rymddomänen hos flygvapenchefen samtidigt som en rymdavdelning bildades på flygstaben. År 2023 fick Sverige sin första försvars- och säkerhetsstrategi för rymden, i vilken fyra pelare betonades: handlingsfrihet i rymden, en svensk rymdförmågeportfölj, aktiva internationella partnerskap samt en sammanhållen och kunskapsbaserad rymdpolitik.

## Trender och exempel

### Rymden som del i framtida konflikter

Den ökande militära användningen av rymden, det tilltagande beroendet av rymden i samhället i stort, tillsammans med den rymdkapprustning som nu sker, gör det högst sannolikt att rymddomänen dras in i framtida konflikter. Detta gäller oavsett om en konflikt startar i rymden och sedan eskalerar på marken eller tvärtom. Vid en asymmetrisk konflikt mellan en stor och en mindre rymdaktör kan det vara

attraktivt för den mindre aktören att slå mot rymdinfrastrukturen för störst effekt på motståndarens förmåga i de andra domänerna. Sårbarheten och de täta banden till andra operationsdomäner gör att rymddomänen ses som en egen krigsarena där både offensiva och defensiva förmågor behövs och numera utvecklas. Det pågår utbildning, träning och planering för krigföring i rymden som en del av traditionell krigföring. Motåtgärder för att hantera attacker mot rymdsystem utvecklas, både som rent tekniska motmedel och i form av redundans och resiliens på plattformsnivå och på system-av-systemnivå.

Traditionellt har vapenutvecklingen främst setts handla om krigföring mark-mot-rymd och rymd-mot-rymd. Vapen tilltänkta för rymd-mot-mark har setts som för kostsamma, men utveckling som medför ännu lägre kostnad per uppskjutet kilo kan göra att kalkylerna kring denna typ av vapen kan behöva omvärderas redan omkring 2035. Mark-mot-mark räknas inte som rymdkrigföring men det är viktigt att komma ihåg att krigföring riktad mot marksegment eller användarsegment kan leda till stora konsekvenser för rymdstödd militär förmåga.

### Avskräckning i rymden

Som en konsekvens av den tilltagande militära betydelsen har flera länder utvecklat avskräckningsstrategier för rymddomänen. Avskräckning i rymden kan ha en förnekande eller en bestraffande karaktär. Vid förnekande avskräckning är målet att göra angrepp mot rymdsystem mindre attraktivt genom att kunna behålla förmågan som systemet ger, även efter ett eventuellt angrepp. Detta kan uppnås genom att till exempel göra satelliterna mer motståndskraftiga mot angrepp eller att ha förmågan till snabb uppskjutning för att ersätta förlorade eller skadade satelliter. Vid bestraffande rymdavskräckning hotas potentiella angripare med vedergällning, antingen i rymddomänen mot sina egna satelliter, eller i andra domäner.

Gemensamt för avskräckningsstrategier är behovet av god och kontinuerligt uppdaterad rymdlägesbild. Detta möjliggör att i god tid kunna upptäcka risker och hot i rymddomänen för att antingen utföra undanmanövrer, peka ut aggressiva aktörer eller för att identifiera mål om avskräckningen misslyckas. Denna förmåga är kritisk för att upprätthålla effektiv och trovärdig avskräckning i rymddomänen.[235]

### Kommersiella rymdaktörer ökar i militär betydelse

Kommersiella rymdaktörer utgör idag en kraftfull förmågeförstärkare för försvarsmakter världen över. Innovationstakten inom den kommersiella rymdsektorn överstiger den statliga och militära på många områden, och de kommersiella rymdtjänsterna är nu på flera håll kapabla till att konkurrera med, eller överstiga, den förmåga som statliga och militära motsvarigheter erbjuder.

235 FOI, Omvärldsanalys Rymd 2023, 2023.

Där det en gång i tiden endast var rymdstormakterna som hade tillgång till högupplösta satellitbilder går dessa idag att köpa på öppna marknaden från ett stort antal kommersiella leverantörer. Utvecklingen inom både mindre och större bärraketer drivs nu framåt främst av kommersiella krafter. Stora konstellationer av satelliter erbjuder nya typer av tjänster som kan användas både civilt och militärt.

När stater förlitar sig på kommersiella rymdsystem riskerar de också mista den egna rådigheten kring hur och när systemet används. Utöver detta råder än så länge osäkerhet och otydlighet kring hur militära hot mot kommersiella rymdsystem ska hanteras.

Delar av de kommersiella initiativen utvecklas mer i detalj i avsnittet om särskilda delområden och förmågor nedan.

### Rymden som kritisk civil infrastruktur

Även om det militära beroendet av rymddomänen ökar, så går det inte att bortse från den civila sidans beroende – inte minst ur ett totalförsvarsperspektiv. Dagens system för satellitnavigation (GPS, Galileo, Beidou, GLONASS) har visat sig ha en tydlig svaghet i det att de svaga signalerna från satelliterna i medelhöga jordbanor (typiskt kring 20 000 km) är relativt lätta att störa ut nere på jordytan. Eftersom dessa signaler används för positionering, navigering och tidsangivelse (PNT) inom många samhällsviktiga funktioner är detta en sårbarhet som allt fler aktörer ser behöver adresseras. En tanke är att nyttja de kommande megakonstellationerna för att tillhandahålla en alternativ eller kompletterande PNT-förmåga. Den största mängden av dessa satelliter kommer ligga i låga jordbanor (typiskt kring 300-1 000 km), och nyttolaster på någon eller några av dessa konstellationer skulle därför kunna bidra till mer robust PNT-förmåga. Då det inte bara handlar om att producera nyttolasterna och rymdsätta satelliterna utan även om att implementera ändringar i användarsegmentets mottagare kanske detta inte hinner ske fullt ut till 2035, men utgör en reell möjlighet mot 2050.

På telekomsidan börjar allt fler aktörer titta på satellitburen 5G- och 6G-kommunikation. Det råder inga tvivel om att satellitkommunikation kommer att integreras i 5G och kommande generationer, däremot finns fortfarande olika uppfattningar om i vilken omfattning. Skulle direktuppkoppling mot satelliter bli en integrerad del i framtida infrastruktur för mobilnät introducerar detta nya beroenden och sårbarheter – samtidigt som vissa gamla beroenden och sårbarheter minskas eller helt byggs bort.

## Särskilda delområden

### Bärraketer

Pådrivet av stora tekniksprång inom teknik för bärraketer (exempelvis nya motorer och återanvändbara raketsteg) har kostnaden för att sända upp satelliter i rymden minskat kraftigt. Dessa sänkta kostnader har lett till att nya satellittjänster blivit enklare att räkna hem ekonomiskt, och tillströmningen av nya kunder för uppsändning av satelliter har i sin tur ökat omsättningen av bärraketer. Detta har gjort att det inte längre krävs samma långa framförhållning kring planering av uppsändning, vilket i sin tur möjliggör en rörelse mot så kallad responsiv uppsändningsförmåga, det vill säga att med kort varsel sända upp satelliter för att driftsätta en ny förmåga vid behov eller ersätta utslagna satelliter. Mot 2035 kommer ytterligare steg ha tagits mot såväl lägre kostnader som ännu större raketer. Det kommer därmed gå att rymdsätta större objekt och högre massa, vilket kan användas till att rymdsätta ännu större mängder satelliter per bärraket, men också möjliggöra helt nya koncept för satelliter och rymdstationer. Även mänskliga färder till månen, och senare möjligen även Mars, förväntas ske med dessa större raketer.

### Megakonstellationer

Genom att ha en stor konstellation av hundratals eller tusentals samverkande satelliter – populärt kallat megakonstellation – ges möjlighet till helt nya typer av tjänster. I nutid har satellitkommunikationskonstellationen Starlink orsakat svallvågor, och det långt innan den kommit upp i de 13 000 satelliter som den slutligen tänkts utgöras av. Som en effekt av detta planeras ett stort antal nya konstellationer på tusentals satelliter. Bakom detta står både kommersiella aktörer, drivna av den framgång som Starlink har haft, och statsaktörer, som sett vilken nytta Starlink kan bidra med militärt och säkerhetspolitiskt. Mot 2035 kommer ett antal av alla dessa konstellationer börja vara färdigbyggda, med stora civila och militära konsekvenser.

Länkar för optisk kommunikation mellan satelliter används i viss mån redan idag, och genom nyttjande av sådana kan en konstellation utgöra ett så kallat mesh-nätverk där data kan skickas mellan alla satelliter. Utöver de kommunikationstekniska fördelarna ger en sådan förmåga också en robusthet för hela systemet, då konstellationen kan länka ner data via flera olika markstationer.

Utöver satellitkommunikation kan megakonstellationer även användas för jordobservation och satellitnavigation. Fram tills nyligen kunde jordobservationssatellittjänster erbjuda en återbesökstid i storleksordningen dagar, vilket nu i vissa fall sjunkit till timmar. Mot 2035 kommer detta ha sjunkit ytterligare, och mot 2050 kan den så kallade GEOINT-singulariteten ha uppnåtts, det vill säga att varje punkt på jordytan kan observeras när som helst.

Tankar finns också på att använda dedikerade nyttolaster på en megakonstellations satelliter för att bygga upp en ny typ av satellitnavigationssystem, se avsnittet Rymden som kritisk infrastruktur ovan.

Den enorma mängden av satelliter i låga jordbanor innebär också en påverkan på jordens atmosfär. När den tekniska livslängden är slut återinträder dessa satelliter i atmosfären och brinner upp på hög höjd, där de resulterande förbränningsresterna blir kvar under lång tid och kan påverka både klimatet och atmosfären i sig. Det har redan skett en femfaldig ökning av antalet återinträdande satelliter 2020-2024, och om tillväxten i antal satelliter fortsätter som den gjort hittills så kommer ökningen i återinträdande rymdskrot bara tillta. Konsekvenserna av detta har ganska nyligen börjat beforskas och är inte fullt ut kända, men skulle i extremfall kunna leda till att satelliter måste utformas på nya sätt eller att tillåtna utsläpp på annat sätt begränsas.

### Rymdlägesbild

Att upprätthålla en militär rymdlägesbild innebär att ha en lägesbild av rymddomänen som kan användas som beslutsstöd vid egen planering samt vid bedömning av andra aktörers förmåga. I praktiken innebär det att med olika typer av sensorer (radar, optiska, laser, etc.) mäta in objekt i bana runt jorden samt att övervaka rymdvädret som påverkar rymdmiljön och därmed satelliternas banor. Inmätningar kan göras med sensorer placerade på både mark- och rymdbaserade plattformar.

Inom rymdlägesbild sker nu parallella paradigmskiften, rörande mängden objekt som behöver mätas in och vem som upprätthåller rymdlägesbilden. Som en konsekvens av tidigare beskriven utveckling inom bärraketer och megakonstellationer ökar antalet aktiva rymdobjekt som ska spåras, samtidigt som mängden rymdskrot som ska spåras också ökar. Sammantaget gör denna ökade trängsel i rymden (i relativa termer) att kraven ökar på mängden inmätningar, och på precisionen i inmätningarna. Traditionellt har rymdlägesbild upprätthållits av statliga aktörer men nu finns ett flertal kommersiella aktörer som erbjuder diverse rymdlägesbildtjänster, så som tillgång till sensorer för egen inmätning, försäljning av data, samt färdiga produkter med analyserade data. Trenden med kommersiella leverantörer av rymdlägesbild bedöms fortsätta mot 2050.

En utveckling som syns tydligt är förmågan att kunna hantera datafusion från olika typer av sensorer och andra informationskällor vilket i sin tur kommer leda till mer noggranna underlag om händelser i omloppsbanor runt jorden. Arbete med att förlänga rymdlägesbilden mot månen och Mars har redan börjat i och med att USA och Kina planerar att sända människor dit (till månen före 2030 och till Mars tidigt 2030-tal), och denna utökning av volymen som behöver mätas in utgör ännu en framtida utmaning.

### Rymdförnekande förmågor

Att förneka en aktör obehindrad tillgång till dennes rymdsystem kan ske på flera olika sätt: kinetiska vapen i form av ballistiska robotar eller manövrerande satelliter, mikrovågsvapen, cyberattacker, laserbländning och telekrigföring för att nämna några. Dessa attacker varierar både i sin grad av reversibilitet och förnekbarhet, samt i vilken utsträckning de bidrar till bildandet av rymdskrot. Även om förmåga till dessa typer av attacker generellt inte är något som det talas vitt och brett om så bedöms de flesta stora rymdmakter idag ha rymdförnekande förmågor i varierande grad. Det kan också vara ett attraktivt sätt för aktörer, som antingen är mindre eller har ett mindre beroende av rymddomänen, att asymmetriskt hota eller påverka större eller mer kvalificerade aktörer, som kan förmodas ha ett större beroende av sina rymdsystem. Då flera av dessa förmågor kan tros ha en förmånlig kostnads- och nyttoanalys lär utvecklingen av förmågorna fortsätta under tidsperioden. Som en konsekvens av rymddomänens allmänna utveckling kommer systemen troligen bli kraftigare och kunna verka mot större antal satelliter, och som en konsekvens av de relativt låga kostnaderna kommer förmågan sannolikt spridas till ett större antal aktörer. Hittills har det inte nåtts några internationella överenskommelser som reglerar normer och accepterat beteende i rymddomänen, vilket gör att utvecklingen på området sker i ett vakuum. Huruvida dylika överenskommelser kan nås kommer därför vara en av de viktigaste vägvisarna för utvecklingen inom tidsperioden.

## Samverkande och förutsättande förmågor och tekniker

Det finns många kopplingar mellan rymdområdet och andra teknikområden. En förutsättning för att bedriva rymdverksamhet, eller för att använda rymdtjänster, är ett mark- och användarsegment. Det behövs ett marksegment för drift av satelliterna, för att kontrollera dem och ta emot information om satellitens hälsa. Det är även via marksegmentet man tar ner data från satelliterna. Marksegmentet är typiskt en eller flera fasta anläggningar, och geografisk utspridning mellan dessa anläggningar är generellt önskvärt. Användarsegmentet är ett samlingsbegrepp för den utrustning som nyttjas av användare, exempelvis GPS-mottagare eller kommunikationsutrustning.

Både cyber- och informationsdomänen är i hög grad integrerade med rymddomänen. Det innebär att cyberhot i hög grad kan påverka både rymdinfrastrukturen och dess mark-/användarsegment. Rymdinfrastruktur, inte minst genom de stora konstellationer som både finns och är planerade, ger möjlighet till snabb och global informationsspridning.

I området mellan eller i överlappet mellan traditionellt luftrum och rymden finns förutsättningar för så kallade höghöjdsplattformar (HAPS, *High Altitude Platform Systems*) eller pseudosatelliter. Det handlar om obemannade system som är soldrivna och rör sig på höjder mellan satelliter och flyg. Till skillnad mot satelliter i

låga jordbanor kan de kontinuerligt verka över ett visst område och stanna på den höjden i veckor eller månader. De kan utgöra en plattform för både spaning, PNT-tjänster och kommunikation.

## Påverkan på militär förmåga

Det militära nyttjandet av rymden utvecklas för närvarande i raketfart, både hos rymdstormakterna och hos mindre aktörer, och det finns ingen anledning att tro att den utvecklingen skulle avstanna under tidsperioden. Det finns ett flertal faktorer som driver på utvecklingen, bland annat den snabba teknikutvecklingen som sker inom såväl satelliter som bärraketer, den stora tillväxten i antal satelliter och ett mer utbrett användande av kommersiella tjänster för militära ändamål. Sammantaget sker en djupare militär integrering av rymdbaserade förmågor, inte minst inom ramen för multidomänoperationer, och detta större beroende av rymdresurser inom samtliga övriga operationsdomäner gör i sin tur att försvarsåtgärder kring dessa resurser behöver beaktas. Försvarsåtgärder kan utgöras av tekniska lösningar för att med både passiva och aktiva medel bemöta hot, men också genom rymdanpassade avskräckningsstrategier. Utvecklingen inom båda dessa spår är fortfarande i sin linda och kommer sannolikt fram till 2050 präglas av en betydande utveckling genom nya medel och motmedel.

Flera nya kommersiella aktörer inom spaning och övervakning från rymden har hittills satsat på små satelliter men i stora konstellationer, vilket har möjliggjort en högre återbesöksfrekvens än traditionella tjänster som har färre och större satelliter, samtidigt som fler satelliter också har givit konstellationerna mer redundans och resiliens då enstaka utslagna satelliter inte längre nödvändigtvis ger en märkbar nedgång i förmåga. Mot 2035 har sannolikt en rörelse skett mot att även dessa nya konstellationer övergår till något större satelliter, för att kunna erbjuda både hög återbesöksfrekvens och högre bildkvalitet. Inom satellitkommunikation kommer teknikutvecklingen på både satellit- och mottagarsidan medföra allt kompaktare kommunikationsradioenheter, vilket gör att satellitkommunikation nyttjas alltmer ända ner på taktisk eller stridsteknisk nivå.

Försvarsmakten har under lång tid nyttjat olika rymdtjänster via olika typer av partnerskap och samarbeten. Till år 2035 planeras Försvarsmakten ha ett antal egna satelliter i drift, vilket kommer medföra att Sverige har viss egen rådighet inom ett antal rymdbaserade militära förmågor. Inom samma tidsram planeras därutöver Sverige ha förmåga att sända upp satelliter från rymdbasen Esrange, vilket kan ge såväl Sverige som internationella partners tillgång till responsiv uppsändningsförmåga.

## Aktörer

Det är stormakter som leder utvecklingen av rymdteknik och de som har den bredaste förmågan inom rymddomänen är USA, Kina och Ryssland där stort fokus finns på militärt nyttjande av rymden. USA menar att Kina, nu och framgent, är det dimensionerande hotet för militär rymdverksamhet, och det kan antas att detsamma gäller åt andra hållet. Kinas tillväxt inom militära rymdsystem har varit omfattade, inte minst inom militära spaningssatelliter där Kina tidvis haft en högre numerär än USA. Rysslands förmågor är fortfarande omfattande, men landet står inför ett antal strukturella utmaningar för att bibehålla sin status som rymdstormakt i ett längre tidsperspektiv. Flera andra länder gör omfattande strategiska satsningar på både kommersiell och statlig rymdverksamhet, men ligger i dagsläget så pass långt efter ledartrion att det är svårt att se att den föreliggande ordningen skulle förändras nämnvärt till 2035, möjligtvis att externa faktorer skulle kunna omkullkasta ordningen mot 2050.

I dagsläget bedriver aktörer i närmare 90 stater rymdverksamhet men att bedöma huruvida den utvecklingen av rymdteknik som sker är civil eller militär är vanskligt eftersom rymden är föremål för dubbla användningsområden, och även om nyttjandet av rymdsystem skiljer sig mellan militära och civila användare är tekniken i grunden ofta densamma. Antalet militära satelliter i omloppsbana ökar oavsett, och idag har omkring 30 stater aktiva militära satelliter i omloppsbana. För 15 år sedan var det 15 stater som hade detta. Även strategier, doktriner och andra policys som reglerar säkerhet, försvar och krigsföring i rymden tas fram av fler stater, nyligen bland annat Sverige genom den första svenska försvars- och säkerhetsstrategin för rymden. Inom tidsperioden kommer det snarare vara regel än undantag för alla nationer som bedriver någon rymdverksamhet att ha en doktrin för krig och konflikt i rymden. EU har antagit en strategi för försvar och säkerhet i rymden[236] och kommer sannolikt inom tidsperioden bygga upp egna satellitsystem specifikt för försvars- och säkerhetsändamål.

Den kommersiella sektorn bidrar redan idag till den snabba teknikutvecklingen för rymdteknik och -tjänster. De kommersiella aktörerna opererar idag majoriteten av de aktiva satelliterna i rymden och bland dessa äger det amerikanska företaget SpaceX cirka 60% genom sin megakonstellation för satellitinternet, Starlink. SpaceX utvecklar även satelliter för försvar och säkerhet, kallade Starshield, där det amerikanska försvarsdepartementet är en kund. Att kommersiella aktörer utvecklar produkter och tjänster för försvar och säkerhet i rymden förväntas fortsätta inom flera delområden, så som spaning och övervakning från rymden, rymdlägesbild samt satellitkommunikation, under tidsperioden mot 2050. Kinesiska kommersiella aktörers inflytande förväntas också öka inom tidsperioden, speciellt om det flertal megakonstellationer som utannonserats faktiskt realiseras.

236 European Union Space Strategy for Security and Defence (JOIN(2023) 9), Bryssel, 2023.

Uppskjutning har tidigare varit en aktivitet förbehållen statliga aktörer med stora bärraketsprogram, men det redan initierade skiftet mot kommersiella aktörer som dominerar kommer under tidsperioden att skifta mot att ännu fler kommersiella aktörer kommer kunna förse länder med uppskjutningsförmåga. Detta gäller både uppskjutningsplatser och bärraketer. SpaceX är förutom att vara satellittillverkare och operatör även en aktör inom uppskjutningssektorn med flera återbrukbara raketer. I dagsläget genomförs tester med SpaceX nästkommande raket (Starship), även den återbrukbar, som förväntas revolutionera uppskjutningsmöjligheterna genom att göra det möjligt att sända upp mycket större volymer i rymden. Aktörer i Kina arbetar också med nya tekniker för uppskjutning. Huruvida dessa kinesiska aktörer anses tillhöra privat eller offentlig sektor är svårt att uttala sig om. Utvecklingen av mindre bärraketer och etableringen av fler uppskjutningsplatser, om än i kommersiell regi, möjliggör att följande stater har egen rådighet för tillträde till rymden inom tidsperioden: Australien, Brasilien, Kanada, Norge, Singapore, Spanien, Storbritannien, Sverige, Turkiet och Tyskland.

## Lästips

J. Westman (red.) m.fl., (2023). Omvärldsanalys rymd 2023, FOI, Stockholm. FOI-R--5516--SE.

A. Wårlind (red.) m.fl., (2025). Kina i rymddomänen, FOI, Stockholm, FOI-R--5673--SE.

M. Karlsson m.fl., (2024). Svensk säkerhetspolitik och Försvarsmaktens operationsmiljö i rymddomänen 2050, FOI, Stockholm, FOI-R--5638--SE.

Rymdens roll i ett nytt säkerhetspolitiskt läge – Sveriges försvars- och säkerhetsstrategi för rymden, Regeringskansliet, Stockholm.

C. Swope m.fl., (2025). Space Threat Assessment 2025, Centre for Strategic & International Studies, Washington.

V. Samson (red.) m.fl., (2025). 2025 Global Counterspace Capabilities Report, Secure World Foundation, Washington.

P. Szymanski (red.) m.fl., (2023). Mastering Space War – The Advanced Strategies, Technologies, and Theories Needed for Victory, Nimble Books LLC, Michigan, ISBN: 9781934840122.

P. Magee m.fl., (2022). Space Domain Awareness, CEI Publications, Colorado Springs, ISBN: Paperback 978-1-7331679-2-5.

J. O'Connor (2024). A Short Introduction to Geospatial Intelligence, CRC Press, Oxon, ISBN: 9781032566948.D. L. Adamy (2021). EW 105 Space Electronic Warfare, Artech House, Massachusetts, ISBN: 978-1-63081-834-0.

# Cyberförsvar och cybersäkerhet

*Teodor Sommestad och Henrik Karlzén*

## Inledande beskrivning

Cyberdomänen byggs upp av de komplexa tekniker som tagits upp i de olika kapitlen om data, intelligenta system, informationssystem, informationsteknologi och ledningssystem. Därtill finns tydliga kopplingar till sådant som berörs i texterna om telekrigföring, kvantteknik samt mikroelektronik och halvledare. Förutsägelser om framtida konflikter eller operationer i cyberdomänen är därmed direkt beroende av prognoserna om teknikutveckling och användningen av informations- och kommunikationsteknologi (IKT). Exempelvis spelar det stor roll om militära ledningsplatser blir portabla, förlitar sig på digitala agenter och använder fjärrskrivbord eftersom detta påverkar vad som kan åstadkommas med offensiva cyberoperationer.

Cyberangrepp kan riktas mot både civila och militära mål och genomföras på många olika sätt. Nätfiske, mjukvarusårbarheter och leverantörsberoenden är vanliga metoder för att få tillgång till system. Skyddsåtgärder som begränsar användares behörigheter, håller mjukvara uppdaterad och upptäcker misstänkt trafik används för att försvåra sådana angrepp. Även om data rör sig snabbt i cyberrymden och angrepp kan ske hastigt, krävs ofta långvariga förberedelser för både offensiva och defensiva operationer. En offensiv förmåga kan till exempel innebära att bakdörrar underhålls i flera år för att säkerställa tillgång till system. En defensiv operation kan kräva noggrant arbete med kartläggning av normala dataflöden och omfattande övning.

Inom militär verksamhet är underrättelseinhämtning inom cyberdomänen sedan länge etablerat och välanvänt. Andra militära användningsområden för cyberoperationer är inte lika självklara eller etablerade. I Sverige har en doktrinansats[237] nyligen antagits som beskriver offensiva operationer, defensiva operationer och samverkan i gemensamma operationer. Det finns många likheter mellan denna doktrinansats och doktriner i andra länder, men också skillnader. Exempelvis anger USA explicit hur de avser att nyttja cyberoperationer på nivån under väpnad konflikt för att uppnå fördelaktiga förutsättningar.[238]

Smeets[239] har resonerat om fyra sätt för offensiva operationer att erbjuda strategiska fördelar. Den första fördelen är just att offensiva cyberoperationer uppfattas som att de ligger under nivån väpnad konflikt och erbjuder ett alternativ till exempelvis ekonomiska sanktioner. Övriga tre fördelar är att cyberoperationer kan samverka

237 Försvarsmakten, Doktrinansats Cyberförsvar, Försvarsmakten, FMLOG, 2024.

238 US Department of Defence, Cyber Strategy Summary of the Department of Defence 2023.

239 M. Smeets, "The Strategic Promise of Offensive Cyber Operations," Strategic Studies Quarterly, Fall, pp. 90–113, 2018.

med andra militära förmågor, utnyttjas för psykologisk dominans och nå effekt utan att riskera att spilla liv.

Handlingsutrymmet i cyberdomänen påverkas av vilka stater som har kontroll över IT-system och infrastruktur. Exempelvis finns inget behov av offensiva cyberoperationer från stat A mot system i stat B, ifall stat B använder IT-system som stat A har kontroll över. Alltså, om stat A redan har kontroll över och tillgång till data i relevanta system i stat B, föreligger inget behov av att göra intrång.

I takt med samhällets och försvarsmakters digitalisering och ökande nyttjande av sammankopplade IT-system, ökar cyberdomänens relevans.

## Trender och exempel

För 25 år sedan såg cyberdomänen annorlunda ut. I Sverige, som tidigt tog sig an internettekniken, hade ungefär varannan person tillgång till internet hemma och den mest sålda mobiltelefonen var Nokia 3310. Idag har så gott som alla svenskar höghastighetsuppkopplingar i sin mobiltelefon, med betydligt mer beräkningskraft än en kontorsdator hade för 25 år sedan. Trots denna snabba förändring är det svårt att peka på stora paradigmskiften eller tekniksprång inom cybersäkerhet. Tvärtom är cybersäkerhetsarbete ganska likt hur det var för 25 år sedan, även om det är fler som utför det och fler som jobbar heltid med det samtidigt som säkerhetsnivån överlag blivit bättre.

Nedan beskrivs fyra trender: ytterligare expansion av cyberdomänen, kombination av ärvda och nya tekniska sårbarheter, dold teknisk komplexitet i systemen och personalförsörjningsproblematik.

### Ytterligare expansion av cyberdomänen

En tydlig trend, utförligt beskriven i kapitlet om informationsteknologi och som kan väntas hålla i sig, är att samhällets beroende av cyberdomänen ökar på olika sätt. De senaste 25 åren har andelen människor som använder internet växt från cirka 5 % av jordens befolkning till cirka 70 % av jordens befolkning. Därtill har tiden en användare spenderar online ökat till mer än sex timmar per dag och mycket av kritisk infrastruktur är direkt eller indirekt beroende av cyberdomänen. Bland annat har en digitalisering nyligen skett av elkraftssektorn under paradigm som smarta elnät. Expansionen av cyberdomänen kommer med stor sannolikhet att fortsätta civilt. Allt annat lika innebär detta att värdet av cyberförsvar och cybersäkerhet kommer att öka.

Trots att internet ursprungligen var en militär teknologi har försvarsmakter under de senast decennierna varit sena med att tillämpa nya IT-lösningar och ovilliga att koppla ihop och upp system. Denna inställning har inte passat bra ihop med rådande marknadstrender, som i många delar handlat om att leverera systemlösningar som

tjänster via fjärruppkoppling snarare än produkter som kan installeras i avskilda miljöer. I takt med utvecklingen har kostnaden för att inte sammankoppla system och tillgängliggöra information blivit större och en trend nu är att ändå försöka använda den teknik marknaden erbjuder på olika sätt, trots de cybersäkerhetsrisker det kan innebära. Bland annat har begreppet *Internet of Military Things* myntats, vilket konceptuellt handlar om att ha tillgång till ett ekosystem med smart militär teknik som autonomt kan hantera och distribuera olika typer av sensorinformation.

De begränsade uppkopplingarna till och mellan militära system har begränsat potentialen för offensiva cyberoperationer. Begränsad användning av IT och uppkopplingar i militära plattformar har därmed fungerat som skydd mot offensiva cyberoperationer vilket får direkt effekt på slagfältet. I takt med ökande digitalisering inom det militära, samt genom att militära ledningssystem börjar sammankopplas i stor utsträckning, ökar cyberdomänens betydelse. Dels eftersom processer blir effektivare och nya möjligheter öppnar sig, dels då den potentiella effekten av offensiva operationer ökar.

### Ärvda sårbarheter består och nya uppkommer

För 25 år sedan såg cyberdomänen som sagt väldigt annorlunda ut. Lite kontraintuitivt är en erfarenhet från de senaste 25 åren också att många frågor kopplade till cyberförsvar och cybersäkerhet består eller förändras långsamt. Förhållandevis lite har exempelvis ändrats när det kommer till hur sårbarheter uppstår, vilka problem som finns i mjukvaror och hur angrepp går till. Exempelvis var angrepp på tjänster för nätverkskommunikation och behörighetshantering i operativsystemet Windows populära under tidigt 2000-tal[240], vilket de är ännu idag. Sårbarheterna i sig är också av liknande karaktär, även om de idag befinner sig bakom fler skydd och därför blir svårare att utnyttja. Kryptering av webbplatser med HTTPS har exempelvis blivit normen, delvis för att möta behovet av mer säkerhet när data och arbete blivit mer distribuerade geografiskt.

Den primära orsaken till den långsamma utvecklingen av cybersäkerhetsproblemens grundläggande karaktär är att dagens dator- och nätverksteknologier baseras på nästan samma plattformar som de som fanns på 1980-talet. Exempelvis var det då processorarkitekturen x86 slog igenom och programmeringsspråket C++ släpptes. Idag används fortfarande såväl x86 som C++ i många viktiga datorplattformar. I korthet innebär detta att samma typer av mjukvarusårbarheter (exempelvis buffertöverskridningsbrister i minneshanteringen) existerar än idag. Detta gäller särskilt inom försvarsmakter där omsättningstakten för IT-system är lägre än den är civilt. Under denna tid har det förvisso utvecklats en uppsjö av skydd för att begränsa effekten av dessa sårbarheter, men problemen har inte eliminerats helt ännu.

240 Se exempelvis Bruce Schneiers inlägg från 2005: https://www.schneier.com/blog/archives/2005/06/attack_trends_2.html.

Lite förenklat skulle en cybersäkerhetsexpert som gjorde en tidsresa från år 2000 till idag behöva sätta sig in i några nya varianter av de tekniker som personen redan kände till och lära sig några nya tricks för att ta sig runt nya skydd. Men väldigt lite av kunskapen personen tog med sig skulle vara obsolet. Troligtvis gäller detsamma för en cybersäkerhetsexpert som gör en tidsresa till 2050. De sårbarheter som behöver upptäckas för att skydda system eller beväpna cyberoperationer år 2050 kommer alltså förmodligen att vara snarlika dagens sårbarheter. Likt idag kommer säkerheten att hänga på vem som hittar mjukvarusårbarheterna först.

### Komplexitet och missförstånd bakom abstraktioner

Under 1980-talet var komplexiteten i många IT-system så låg att en programmerare ofta kunde ha insyn i allt ifrån kablage till användargränssnitt. Detta har med tiden förändrats och idag är det mesta av den IT som används så komplicerad att ingen enskild individ kan ha fullständig förståelse för hur allt hänger ihop. Gränserna för organisationers IT kan också vara luddiga, exempelvis för att mobila enheter används på olika fysiska platser och anställda sammanblandar privat IT med organisationens.

En starkt bidragande orsak till att mjukvara idag är mer avancerad och komplex är att det finns ypperliga möjligheter att abstrahera bort problem och återanvända kod. En utvecklare som skapar applikationer med ramverk eller bibliotek behöver inte förstå vad som händer under huven för att använda bibliotek eller interagera med tjänster. På liknande sätt kan användning av maskininlärning ses som ett sätt att abstrahera bort invecklade programmeringsuppgifter från mjukvaruutvecklare genom automatisk konstruktion av många if-satser baserat på övningsfall. Dessa förenklingar leder till ökad produktivitet och kan förbättra säkerheten genom att erbjuda standardlösningar för säkerhetsproblem som autentisering. Att utvecklaren inte alltid förstår koden som skapats kan samtidigt öka antalet säkerhetsproblem som orsakas av felaktiga antaganden. Att identifiera sådana tankevurpor kan visa sig svårare än att hitta klassiska programmeringsmisstag kopplade till minneshantering och liknande.

Abstrahering sker inte bara inom mjukvara utan även inom system-av-system och på datornätverksnivå. Molntjänster är ett sätt att slippa den komplexitet som en IT-avdelning traditionellt behöver hantera, exempelvis avseende kablage.

Det finns goda skäl att tro att antalet säkerhetsmisstag minskar med centralisering, standardisering och professionalisering. Samtidigt är det möjligt att de sårbarheter som finns kvar i systemen blir mer lika för fler organisationer eftersom allt fler använder samma underliggande plattformar, underleverantörer eller tjänster, och dessutom ofta utan att veta det själva. De senaste årens incidenter som involverar tjänsteleverantörer är exempel på detta. Olika sätt att kartlägga och dokumentera dessa beroenden kan komma att utvecklas – både för offensiva och defensiva operationer.

### Kompetensbrist och professionalisering

I takt med att cyberförsvar och cybersäkerhet blivit viktigare områden har det blivit påtagligt att det råder brist på personal inom dessa områden. Förutom ett generellt behov av personer för att fylla roller för sådant som cybersäkerhetsövervakning, vill man också rekrytera de skarpaste personerna till sin egen verksamhet. Många uppgifter inom cyberförsvar är nämligen av sådan karaktär att det kan skilja en faktor hundra mellan vad en topprekryt och en medelrekryt kan prestera. Att leta efter sårbarheter i mjukvara är ofta ett exempel på en sådan uppgift, där den som ska hitta sårbarheter behöver leta bättre än alla andra som försökt tidigare.

För att möta detta behov av personal och spetskompetens har myndigheter och näringsliv under de senaste decennierna bland annat utvecklat standardiserade kompetensbeskrivningar för roller i cyberdomänen[241], etablerat särskilda utbildningar inom cybersäkerhet på universitet och skapat ”hackerlandslag”. I Försvarsmakten har till och med särskilda personalkategorier införts. Denna professionalisering lär fortsätta under de kommande decennierna.

Parallellt med professionaliseringen sker en automatisering av uppgifter som tidigare gjordes manuellt. I första hand gäller detta rutinartade och enkla uppgifter. Under de senaste decennierna har det inneburit att uppgifter som att hantera säkerhetsuppdateringar och kontrollera installerade mjukvaror kan ske automatiskt. Utvecklingen idag går mot exempelvis stöd för att trimma in intrångsdetektionssystem och verktyg för att automatiskt isolera cybersäkerhetsincidenter. Detta lär fortsätta och eventuellt accelerera genom framstegen som görs inom maskininlärning.

## Särskilda delområden

Nedan belyses några allmänt erkända cybersäkerhetsproblem och vad som kan förväntas kopplat till dessa år 2050. Vissa ämnen av relevans tas upp i andra kapitel och läsaren hänvisas då dit. Det gäller särskilt hur kvantdatorer kan påverka cyberförsvar och cybersäkerhet samt kombinationen av cyberangrepp och telekrig (så kallad CEMA, *Cyber and Electro-Magnetic Activities*).

### Hitta sårbarheter i mjukvara

Stöd för att analysera mjukvara och system för att identifiera sårbarheter blir förmodligen ännu viktigare när IT-system bli mer komplexa och svårare för systemutvecklare att förstå.

För att identifiera sårbarheter i mjukvara används idag huvudsakligen två tekniker. Den ena tekniken använder fuzzers, som kör mjukvaror i en kontrollerad miljö och med indata som är ogiltig, oväntad eller slumpmässig. Målet är att identifiera vilka indata som gör att mjukvarorna kraschar eller uppvisar andra sårbarheter. Den andra

241 Se framförallt NIST:s ramverk National Initiative for Cybersecurity Education (NICE) från USA.

tekniken är statisk kodanalys, där källkod analyseras automatiskt för att identifiera användning av sådant som sårbara funktioner och kända programmeringsmisstag. Ingen av de nämnda teknikerna är för närvarande tillräcklig för att eliminera sårbarheter. En fuzzer är otillräcklig eftersom det finns många sätt att interagera med en mjukvara på, och att testfall på grund av tidsbegränsningar enbart kan skapas för en liten delmängd av alla dessa interaktioner. Statisk kodanalys är otillräcklig eftersom det inte är möjligt för ett kodanalysverktyg att effektivt spåra komplexa flöden i en applikation.

Mer omogna tekniker för att identifiera mjukvarusårbarheter inkluderar bland annat användning av symbolisk exekvering (en sorts emulering av koden) och stora språkmodeller för att förbättra sökandet, exempelvis genom att identifiera lämpliga indata till fuzzers. Tekniker för att hitta sårbarheter kommer sannolikt att utvecklas i sådana riktningar och leda till såväl enklare användning och bättre träffsäkerhet. Samtidigt är det osannolikt att alla sårbarheter försvinner. Likt idag kommer det förmodligen att vara viktigt om det är hotaktörer eller systemägare som är flitigast på att leta efter sårbarheter. Teknikutvecklingen påverkar alltså både offensiva och defensiva cyberoperationer.

### Analysera terrängen och beroenden

Terrängen inom cyberdomänen är, likt terrängen i andra domäner, av stor betydelse. Förståelse för den egna cyberterrängen är avgörande vid bedömning och hantering av cyberincidenter. Därtill är insikt i motståndarens terräng central vid planering och genomförande av offensiva cyberoperationer. Dessvärre är det svårt att förstå terrängen i cyberdomänen och göra meningsfulla kartor av den. I Försvarsmaktens doktrinansats[242] beskrivs exempelvis cyberdomänen i olika lager och det läggs vikt vid vem som har rådighet över olika delar.

För att skapa förståelse för cyberterrängen krävs meningsfulla modeller av denna, där modellerna passar de beslut som ska fattas. Det behövs alltså en god uppfattning om vilken information som krävs för att fatta beslut rörande säkerhet eller operationer. Idag saknas etablerade standarder för att beskriva cybermiljöer. Det finns standardiseringsförsök som *Security Content Automation Protocol* och informell praxis för att beskriva angrepp. Ett exempel är Mitre ATT&CK. Systemdokumentation och kartläggningar utformas på många olika sätt och ofta behövs även kunskap om exempelvis verksamhetsprocesser för att fatta kloka beslut. Det finns idag ingen bred enighet om hur meningsfulla modeller ska se ut.

Utöver en lösning på problemet med vad som utgör meningsfull information om terrängen behövs verktyg och tekniker för att samla in informationen. Verktyg som utför automatiska systemskanningar är sällan träffsäkra och särskilt inte om de används på system som kontrolleras av andra. Det kan behövas kompletterande

242 Försvarsmakten, Doktrinansats Cyberförsvar, Försvarsmakten, FMLOG, 2024.

tekniker och modeller för att göra kvalificerade gissningar när detaljer saknas, exempelvis för att kartläggningen görs av systemleverantörers eller antagonisters system.

Sannolikt kommer detta område att utvecklas under de kommande decennierna. Detta gäller bland annat eftersom terrängen i cyberdomänen förväntas bli mer komplex med större beroenden till tjänsteleverantörer och interna tjänster. Det går inte idag att ha full insyn i all komplexitet bakom en tjänst eller mjukvara som levereras av en extern part. Troligtvis blir möjligheten till insyn bättre under de kommande decennierna. MSB[243] har redan föreskrifter som säger att statliga myndigheter ska dokumentera ”hård- och mjukvara som används i varje enskilt informationssystem” (2 kap. 4§ MSBFS 2020:7). Lagstiftning som EU:s NIS2-direktiv innehåller steg i denna riktning genom bland annat krav på risk- och sårbarhetsbedömningar. Likaså är innehållsdeklarationer av typen programvaruförteckning och CE-märkning av mjukvaruprodukter något som tas upp i EU:s cyberresiliensförordning.

### Upptäcka angrepp och händelser

Att upptäcka pågående angrepp mot egna system och att undgå upptäckt vid angrepp mot andras system är båda av värde för cyberförsvar och cybersäkerhet. Det är också önskvärt att ha koll på angrepp mot andra och förmåga att spåra var angrepp kommer ifrån, exempelvis genom signalspaning. Forskning på dessa områden har sedan länge varit omfattande och innefattar sådant som optimal placering av sensorer och olika algoritmer som är tänkta att larma för angrepp.

Under de senaste decennierna har plattformarna för att samla in och bearbeta systemloggar och säkerhetsloggar utvecklats betydligt. Det är idag förhållandevis enkelt att sätta upp logginsamlingslösningar som samlar allehanda loggar i databaser, vilket underlättar bearbetning och sökning. De råa loggarna är i regel alltför många och detaljerade för mänsklig analys varför de kompletteras med system som skapar larm när sådant som tros vara riskabelt inträffar. Industripraxis är idag att generera larm när loggar motsvarar signaturer som stämmer med enkla angreppstekniker. Exempelvis larmas när en person anger fel lösenord flera gånger eller använder en mjukvara som ibland används för angrepp. Det finns många idéer om att använda automatiska analyser, baserade på komplicerade hotmodeller eller maskininlärning, för att minska mängden falsklarm som sådana signaturer leder till. Dessa idéer har dock inte omsatts i lösningar som används i stor skala. Det finns flera åsikter om varför det är så. En ofta citerad förklaring är att felklassificeringar ger alltför höga kostnader, att det saknas träningsdata, att analysresultat i form av anomalier är en alltför svag grund att agera på, att det finns alltför många varianter på loggar samt att det är oklart hur utvärderingar bör ske.[244]

243 Sedan första januari 2026 Myndigheten för civilt försvar.

244 Sommer, R., Paxson, V., 2010. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. Proceedings of the IEEE Symposium on Security and Privacy 305–316.

Logginsamlingssystem och säkerhetsövervakning är idag områden med stora system- och tjänsteleverantörer. Deras lösningar och tjänster kommer att förbättras oavsett om det sker stora tekniska språng inom logganalys eller detektion. Exempelvis sker detta kontinuerligt genom omsättning av hotunderrättelser till träffsäkrare signaturer för angrepp. Därtill finns det förbättrade analysmetoder som tycks vara mogna att implementeras ovanpå logginsamlingslösningar och användas idag, även om de ännu inte börjat användas på bred front. Till dessa nya analysmetoder hör modeller baserade på hotmodeller med flera angreppssteg i sekvens, stöd för intrimning av avvikelselarm, aggregering av loggar till händelser på en abstraktionsnivå som passar mänsklig analys samt språkmodeller som hjälper människor att söka i loggarna.

### Automation av uppgifter och roller

Det finns goda skäl att automatisera arbetsuppgifter inom cyberförsvar och cybersäkerhet. Dels finns ett underskott på kompetent personal, dels kan uppgifterna kräva att enorma mängder information analyseras samtidigt, dels kräver många uppgifter en reaktionshastighet som är svår för människor att tillhandahålla.

FOI gjorde för cirka fem år sedan en analys av vilka uppgifter som är enkla respektive svåra att automatisera inom cyberdomänen.[245] Resultatet av denna analys pekar på att det som är förhållandevis enkelt att automatisera är sådant som rör hantering av systemkonfigurationer, hantering av databaser och uppsättning av datornätverk. Något svårare är uppgifter som handlar om sådant som forensik, sårbarhetsanalys och incidenthantering. Svårast är uppgifter som kräver avancerade prediktioner och exempelvis handlar om planering av operationer eller hantering av hotunderrättelser. Hindren för ökad automation var i första hand brist på data för träning av statistiska modeller, i andra hand behov av att tänka kreativt och i tredje hand behov av att förstå social interaktion. Betydande framsteg på dessa områden kan alltså innebära att många roller helt eller delvis kan automatiseras. Som redan indikerats ovan finns det skäl att tro att verktygen för att upptäcka angrepp och händelser kan bli betydligt bättre ifall bra träningsdata blir tillgängliga eller om förutseende hotmodellering kan produceras.

Trots att det finns hinder för automation i många uppgifter inom cyberförsvar och cybersäkerhet bör betydande automatisering förväntas under de kommande decennierna. Bland annat kan de framsteg som redan gjorts inom språkbaserade maskininlärningsmodeller användas för att förenkla eller automatisera många deluppgifter inom cyberförsvar och cybersäkerhet. Så lär också ske redan under den kommande femårsperioden.

245 Teodor Sommestad, Joel Brynielsson, Stefan Varga, Möjligheter för automation av roller inom cybersäkerhetsområdet, FOI Memo 6737, https://foi.se/rest-api/report/FOI%20Memo%206737.

## Samverkande och förutsättande förmågor och tekniker

Flera teknologier påverkar hur cyberförsvar och cybersäkerhet kan eller bör bedrivas. Framsteg inom artificiell intelligens, såsom beskrivits under rubriken ”Automation av uppgifter och roller”, spelar en viktig roll. Det gör också utvecklingen av kvantdatorer, vilka kan få stor inverkan på området. Framtida telekrigföring kommer sannolikt också att dra nytta av tekniker som överlappar med cyberförsvar. Integration av telekrigsförmåga och cyberförsvarsförmåga kan då bli en självklarhet.

På en organisatorisk nivå finns det ett växande behov av samverkan mellan olika försvarsgrenar, andra försvarsmyndigheter och civila aktörer. Särskilt tydlig är kopplingen mellan underrättelseverksamhet och cyberförsvar, där informationsflöden och samordning blir avgörande faktorer.

Begränsningarna för att använda eller försvara sig mot cyberangrepp är inte alltid tekniska. Ibland utgör vissa etiska, juridiska och organisatoriska aspekter betydande hinder. Ansvarsfrågor mellan olika aktörer är ofta otydliga och kan försvåra både beslutsfattande och insatser. Svårigheten att bedöma effekter av cyberoperationer kan kräva svåra överväganden. Ett cyberangrepp mot ett kraftsystem som används militärt kan exempelvis ha potential att ge taktiska fördelar på slagfältet, men samtidigt orsaka allvarligt lidande för civilbefolkningen. Nyttjande av offensiv cyberförsvarsförmåga kan också innebära avvägningar mellan underrättelseinhämtning och effekt på slagfältet eftersom tekniska bakdörrar då avslöjas och därmed förloras som verktyg för framtida underrättelseinhämtning.

Varken i Sverige eller i andra länder är juridiken och ansvarsfrågorna kring cybersäkerhet helt tydliga eller brett förankrade. Internationellt bedöms cyberoperationer ofta befinna sig i ett konfliktläge mellan diplomatiska sanktioner och krig, men detta är ännu inte en etablerad norm. En bidragande orsak till denna praxis är sannolikt att få cyberoperationer med stor direkt påverkan på samhällen har genomförts, blivit allmänt kända och samtidigt otvetydigt kunnat kopplas till statsaktörer.

## Påverkan på militär förmåga

Det mesta av den teknik som används inom cyberförsvar och cybersäkerhet har både militära och civila tillämpningar. Viktiga händelser rörande cyberförsvar och cybersäkerhet sker dessutom ofta i en gråzon och kan genomföras både innan en konflikt och efter det att konflikten övergått i öppen militär konfrontation. Det är dessutom ofta otydligt om en statsaktör står bakom ett cyberangrepp eller inte, vilket försvårar gränsdragningen mellan militär förmåga, försvar och brottsbekämpning. Av dessa skäl är påverkan ofta svår att avgränsa och det finns betydande synergier att uppnå genom samarbete inom totalförsvaret. Detta gäller särskilt eftersom civil infrastruktur och tjänster är tänkbara måltavlor för den som vill försvaga en nations försvarsvilja och militära kapacitet. En god civil cybersäkerhet kan därför

ses som en del av militär förmåga. På liknande sätt kan stater som bara delvis byggt ut cyberdomänen klara sig med begränsad militär cyberförsvarsförmåga.

I den rent militära kontexten har cyberoperationer länge varit en central del av underrättelseinhämtningsarbetet. Cyberoperationer med tydlig effekt på slagfältet är mindre vanligt. Hur detta utvecklas framöver beror på hur snabbt cyberdomänen expanderar och i vilken utsträckning militära förmågor blir beroende av den. Beslut inom detta område påverkas också av internationella normer och praxis kring offensiva cyberoperationer. Om attacker mot kritisk infrastruktur blir ett återkommande inslag i framtida konflikter, eller om spektakulära cyberangrepp slår ut viktiga försvarssystem, kan det forma hur stater väljer att förhålla sig till cyberkrigföring. En möjlig framtid är att vapensystem och kommunikationsnätverk blir helt integrerade med civil digital infrastruktur. En annan möjlig utveckling är att sådana system blir, eller förblir, fristående och isolerade för att minimera cybersäkerhetsriskerna.

## Aktörer

Vad gäller defensiva förmågor har teknikutvecklingen den senaste 25-årsperioden varit nästan helt dominerad av civil utveckling och främst då inom näringslivet. Mycket av teknikutvecklingen sker inom de största IT-bolagen i deras egen utveckling eller genom deras förvärv av mindre bolag med framstående positioner inom cyberförsvar och cybersäkerhet. Samtliga dessa IT-jättar är USA-baserade. Troligtvis fortsätter detta gälla under den kommande 25-årsperioden. Dessa stora aktörer är även leverantörer till Försvarsmaktens digitala infrastruktur och vi bedömer att detta beroende kommer att kvarstå.

USA ligger långt framme även bland de många bolag som är specialiserade på cyberförsvar och cybersäkerhet. Det finns också EU-bolag från länder som exempelvis Finland, Spanien, Rumänien och Slovakien samt från övriga världen genom exempelvis Storbritannien, Japan, Israel och Ryssland. De olika ländernas bolag är samtidigt sammankopplade tekniskt, ekonomiskt och juridiskt.

Det finns många exempel på lagar som styr hur aktörer i cyberdomänen ska agera i frågor som rör cybersäkerhet, och dessa lagar är olika i EU, USA och Kina. Vilken geografisk tillhörighet ett IT-bolag har kan alltså spela stor roll för cybersäkerheten det kan erbjuda. Det finns också signaler om att USA alltmer kommer vilja gå sin egen väg. Om detta återspeglar verkligheten framöver kan det leda till att de amerikanska IT-bolagen satsar mindre på säkerhet ur EU:s perspektiv. Å andra sidan kommer säkerhetshoten troligen fortsätta att vara gemensamma för stora delar av IT-världen, där en och samma sårbarhet ofta finns både i egna system och i andras. En viktig faktor är också att en hel del av utvecklingen inom IT och cyberförsvar och cybersäkerhet har skett ideellt i informella samarbeten och med öppen källkod

som ledstjärna. Denna samhällsnyttiga verksamhet kommer förmodligen att fortsätta de närmaste 25 åren.

Marknaden för offensiv förmåga är mindre till storleken, betydligt mindre mogen och mer dunkel till sin natur. Det är svårt att se att en välfungerande marknad växer fram. Försäljning av underrättelser om sårbarheter och säkerhetsbrister lider av ett inneboende problem med transparens. En aktör som erbjuder en ny teknik för att ta över system kommer exempelvis ha svårt att belägga att deras teknik fungerar, särskilt inte utan att röja viktiga detaljer om tekniken. Det kan också vara svårt att sälja samma teknik flera gånger eller till flera kunder. Inom denna marknad finns en vag linje mellan verktyg för att testa IT-systemens säkerhet och vapen för illasinnade angrepp. Här är problematiken med *dual-use* stor, varför det finns olika rättsliga utmaningar med att exportera, sälja och använda verktygen. Vissa av bolagen är väletablerade inom mer öppen verksamhet kopplat till säkerhetstestning och kan därför vara mer öppna med sin verksamhet. Andra bolag bidrar mer till marknadens dunkel. I nyhetsmedier rapporteras det trots allt om relevanta bolag i framförallt USA, Storbritannien, Israel och Kina. Bolagens verksamhet är ofta relativt liten men kan också ha statsstöd. Troligtvis fortsätter denna ovanliga marknad vara omgärdad av mycket ovisshet.

## Lästips

Doktrinansats Cyberförsvar, Försvarsmakten, FMLOG, 2024.

T. Sommestad, J. Brynielsson, S. Varga, Möjligheter för automation av roller inom cybersäkerhetsområdet, FOI Memo 6737.

M. Smeets, The Strategic Promise of Offensive Cyber Operations, Strategic Studies Quarterly, Fall, pp. 90–113, 2018.

H. Karlzén, Cyberoperationers attribution, tillvägagångssätt och sofistikation, FOI-R--4834--SE, 2020.

H. Karlzén, D. Eidenskog, J. Falkcrona, C. Valassi. Varför har mjukvaror sårbarheter?, FOI-R--5550--SE.

P.-E. Nilsson, Unraveling the Myth of Cyberwar. Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War (2014–2023), FOI-R--5513--SE, 2023.

# Informationssystem

*Fredrik Söderström*

## Inledande beskrivning

### Informationssystem

Informationssystem utgör en sammanhängande helhet av teknik, information, människor och organisatoriska arbetssätt. De formar hur information skapas, bearbetas och används i verksamheten och är därmed centrala för militär ledning och samordnad verkan. Syftet med informationssystem är att stödja och utveckla organisationens arbetsprocesser och beslutsfattande genom samspelet mellan människor, teknik och struktur. De tekniska delarna, såsom nätverk, servrar, databaser, applikationer och molnbaserade tjänster, tillhandahåller lagring, bearbetning och distribution av data. Med stöd av algoritmer, AI och olika gränssnitt kan informationssystem generera beslutsunderlag och tjänster för både användare och andra system. Denna automatiserade funktionalitet bidrar till att omsätta data till information som kan användas för beslut och åtgärder. Detta kan även kopplas till andra begrepp som förekommer i denna antologi, som till exempel intelligenta agenter och digitala assistenter.

Eftersom informationssystem består av många tekniska komponenter som måste samverka över funktioner och nivåer, är gemensamma standarder, arkitekturprinciper och integrationslösningar avgörande för att systemen ska fungera effektivt och vara interoperabla. Informationssystem är dessutom dynamiska, eftersom syften, användningsbehov, organisatoriska förutsättningar och tekniska komponenter förändras över tid. En central del av informationssystemets funktion och utveckling är därför hur organisationen planerar, leder och förvaltar arbetet med systemutveckling, drift och kontinuerlig anpassning. Detta påverkar också direkt hur organisationen utformas och fungerar som en socioteknisk helhet. Informationssystem kan uppfattas som abstrakta eller reduceras till enbart tekniska lösningar. I praktiken är dock informationssystem högst konkreta, eftersom de utgör sociotekniska infrastrukturer där människor, teknik, organisation och arbetssätt samverkar för att skapa, bearbeta och använda information. I dessa system spelar mänskliga egenskaper och aspekter en central roll.[246]

De tekniska komponenterna lagrar, bearbetar och distribuerar både öppna och skyddsvärda data, medan de organisatoriska och mänskliga delarna avgör hur informationssystemet används, till exempel i ledning, samverkan eller samordnad verkan. Informationssystem utgör grunden för flöden av data, information och kunskap,

246 Peter Checkland and Sue Holwell, Information, Systems and Information Systems: Making Sense of the Field (John Wiley & Sons, Inc., 1998).

där systemets effektivitet och nytta i hög grad beror på hur väl systemet samspelar med verksamheten och processerna det ska stödja.[247] För att informationssystemet ska fungera krävs att den tekniska infrastrukturen, och den funktionalitet som systemet bygger på, finns på plats och är driftsäker. Utformningen av dessa infrastrukturer varierar beroende på tekniska, organisatoriska och säkerhetsmässiga krav.

Den tekniska utvecklingen har medfört att dagens informationssystem är tätt integrerade med till exempel materielsystem, plattformar och ledningsstrukturer, både inom och mellan förband, och därmed utgör en central del av militär verksamhet. Även om informationssystem ofta förknippas med digital teknik behöver de inte vara tekniska, utan kan även bygga på analoga metoder som karta, kompass, koordinater och ordonnanser. Beskrivningen i detta kapitel är övergripande och berör inte tekniska detaljer. De tekniska komponenterna som stödjer informationssystem behandlas mer utförligt i antologins kapitel om informations- och kommunikationsteknik i Del 2.

### Militära informationssystem

Militära informationssystem används för att säkerställa robusta och tillförlitliga informationsflöden, stödja beslutsprocesser samt möjliggöra samverkan och samordnad verkan över stridskrafts- och domängränser. I den alltmer digitaliserade militära verksamheten, är informationssystem centrala för flera funktioner. Bland annat utgör de en grundläggande del av materielsystemens funktionalitet och bidrar till att skapa lägesbilder och informationsöverlägen. Militära informationssystem är en förutsättning för en välfungerande ledningsförmåga eftersom de tillgodoser beslutsfattares och stabsmedlemmars informationsbehov.[248] En central utmaning är att utforma system som faktiskt levererar den funktionalitet som verksamheten behöver. Inhämtning, hantering, lagring och bearbetning av data har begränsat värde om inte informationssystemets avsedda användning och funktioner är tydligt definierade. Dessa förutsättningar förändras kontinuerligt i takt med utveckling av organisation, teknik och operationsmiljö.

Globala säkerhetsutmaningar och det föränderliga geopolitiska läget driver på utveckling av avancerade informationssystem inom militära organisationer.[249] Den tekniska utvecklingen skapar samtidigt nya möjligheter att tillgodose ett ökande informationsbehov inom militär verksamhet. Detta leder till allt mer omfattande och komplexa informationssystem. Detta ställer i sin tur krav på överblickbara och hanterbara informationsstrukturer. För att möta dessa krav behöver militära informationssystem utformas utifrån en arkitektur som möjliggör utveckling och

247 Paul Beynon-Davies, Business Information Systems, 2nd edn (Palgrave MacMillan, 2013).

248 JH Bryant and MA Todd, 'The Design and Implementation of Automated Military Information Systems', IEEE Transactions on Military Electronics 9, no. 2 (1965): 148–52.

249 Sorin Pînzariu and Ana-Maria Diaconu, 'Considerations Concerning the Necessity of Existence a Modern Military Information System in the Current Geopolitical and Geostrategic Context', Land Forces Academy Review 24, no. 4 (2019): 271–75.

anpassningar.[250] Dessutom skapas behov av ökad skalbarhet och flexibilitet, samt förbättrade möjligheter för förvaltning.[251] Detta kapitel behandlar militära organisationers behov av informationssystem, med särskilt fokus på hur dessa system stödjer ledningsfunktionen.

## Trender och exempel

### Samordnade system

Utvecklingen mot allt mer avancerade integrerade och samverkande system inom militär sektor beskrivs internationellt som samordnade system (eng. *unified systems*). Samordnade system definieras som en sammanhållen enhet av tekniska system, processer och personal som genom interoperabilitet, robusta informationsflöden och gemensamma rutiner för processer, möjliggör effektivt beslutsfattande, delad lägesbild och effektiv resursanvändning. Militära informationssystem utgör den centrala infrastrukturen i samordnade system och möjliggör den samordning och funktionalitet som dessa system kräver. Militära informationssystem gör det möjligt att integrera och samordna förmågor, vilket är avgörande för utvecklingen från isolerade insatser till en koordinerad och effektiv helhet. Den tekniska utvecklingen, med allt fler sensorer, tidskritiska informationsflöden och ökad korskoppling mellan förband, försvarsgrenar och domäner möjliggörs av informationssystem, men driver samtidigt på hur dessa system behöver utformas. Detta skapar ett växande behov av samordnade system som kan integrera funktioner och verkan över hela organisationen.

Samordnade system kopplas ofta ihop med förmågan att genomföra multidomänoperationer (MDO), vilkas syfte är att påverka motståndaren simultant i flera eller samtliga domäner.[252] För detta krävs sammankopplade, integrerade, övergripande och samverkande system som bygger på domänöverskridande informationsdelning, ledning och styrning. En modern militär informationsinfrastruktur är en viktig del av en nations försvar för att motverka och besvara samtida hot.[253] I en utblick mot 2050 bedöms samordnade system präglas av sömlös integrering över samtliga domäner, inklusive cyber och rymd, samt allt större integrering av användning av intelligenta och autonoma tekniker. Integreringen med allierade, internationella

250 Zhen Shu, Mengmeng Zhang, Honghui Chen, and Yu Jin, 'An Alignment Analysis of Military Information System Architecture Based on Portfolio Decision Approach', 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), IEEE, 2019, 428–33.

251 Fuxue Wang and Jie Zhang, 'Military Information System Based on Microservices Framework', 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC) 10 (2022): 943–50.

252 Ove Pappila, Vad Är Multi Domain Operations?, no. 1, Analys & Perspektiv (Kungliga Krigsvetenskapsakademien, 2024), 54–63.

253 Pînzariu and Diaconu, 'Considerations Concerning the Necessity of Existence a Modern Military Information System in the Current Geopolitical and Geostrategic Context'.

partners och aktörer inom totalförsvaret förväntas också öka, vilket ställer höga krav på interoperabilitet och gemensamma standarder.

### Ledning och organisation

Förstärkning av ledningsförmåga är en central drivkraft bakom trender och strategier för samordnade system. Allt mer avancerade och tidskritiska militära hot är en starkt bidragande faktor. Dessutom ställer hybrida hot nya krav på att agera över domäner och mellan aktörer. Det finns behov av informationssystem såväl inom militära funktioner, som mellan funktioner samt för informationsdelning med andra aktörer nationellt och internationellt. Nya intelligenta tekniker skapar nya möjligheter för inhämtning, bearbetning och analys av data för till exempel datadrivet beslutsstöd. Modern krigföring präglas av hög osäkerhet, decentralisering och snabba förändringar. Detta innebär att traditionella hierarkiska ledningsmodeller, som bygger på tydliga funktioner och linjära informationskedjor, kan få svårt att möta kraven i en dynamisk och snabbt skiftande operationsmiljö.

Integrering av system över organisatoriska gränser bygger på teknisk utveckling och skapar möjligheter för förbättrad effektivitet samt intern och extern koordinering, vilket stärker militär förmåga. Tanken bakom samordnade system kan spåras till tidigare initiativ där informations- och kommunikationsteknik (IKT), genom ökad integration och interoperabilitet, kan förbättra militär förmåga. Denna förbättring har bland annat berört områden som ledning, delad situationsförståelse, samarbete, samverkan och flexibilitet. Exempel på tidigare koncept är *Network-Centric Warfare* (NCW) och *NATO Network Enabled Capability* (NNEC). Drivande faktorer bakom dessa koncept är antaganden om att en robust nätverksbaserad förmåga och förbättrad informationsdelning bidrar till ökad kvalitet och effektivitet i samverkan samt förbättrad situationsförståelse.[254]

### Hantera komplexitet

Ökad samordning, samverkan och interoperabilitet leder även till ökad teknisk och organisatorisk komplexitet. Samordnade system bygger bland annat på en teknisk infrastruktur som sträcker sig över organisatoriska gränser, och sammankopplar olika delar av verksamheten på nya och ofta mer omfattande sätt. Även om utveckling av ny teknik är utmanande är det ofta ännu mer utmanande att utveckla nya militära doktriner, organisatoriska strukturer, processer, taktiker och procedurer som kan utnyttja tekniken.[255] Organisatorisk struktur påverkas också av nya tekniska möjligheter, till exempel genom förändrade ansvarsområden, roller, personella resurser och kompetenser. I Försvarsmaktens Riktlinjer och plan 2025 - 2035 beskrivs områden som bygger på ökad samordning, integrering och samverkan som prioriterade.[256]

254 Se t.ex. Holloman, ‘Complex Adaptive Systems Theory and Military Transformation’.

255 Holloman, ‘Complex Adaptive Systems Theory and Military Transformation’.

256 FM2024-21844:1, Riktlinjer Och Plan 2025–2035, nos FM2024-21844:1 (Högkvarteret, 2024).

Likt perspektivet på informationssystem, utgår samordnade system från ett holistiskt synsätt där människor, teknik och processer tillsammans bidrar till att skapa operativ förmåga. Nedan följer några exempel från tekniska grundläggande infrastruktursatsningar till förmågor som kräver väl fungerande informationssystem. Dessa kopplas tydligt till utvecklingen mot samordnade militära system.

### The Army Unified Network Plan

Den amerikanska arméns plan för ett enhetligt nätverk, *The Army Unified Network Plan* (AUNP), syftar till att synkronisera och modernisera arméns integrerade taktiska nätverk (ITN) och integrerade verksamhetsnätverk (IEN). Detta omvandlar nätverket från en tidigare osynlig tillgång till en kritisk resurs som utgör stöd för både vapensystem och genomförandet av MDO. Möjliggörandet av MDO-förmågan beskrivs även som en av de viktigaste drivkrafterna bakom planen. Syftet är också att stärka förmågan att möjliggöra effektivt beslutsfattande och förbättra den operativa förmågan, vilket förutsätter en motståndskraftig, säker och globalt tillgänglig nätverkskapacitet. Mot denna bakgrund anpassar planen flera komplexa insatser för att möjliggöra modernisering av nätverk och samordnade tillvägagångssätt som krävs för att stödja MDO.[257] AUNP syftar därmed till att integrera arméns taktiska nätverk och verksamhetsnätverk i syfte att bland annat möjliggöra datadrivet beslutsfattande inom ramen för MDO. Planen började implementeras 2021 och förväntas vara fullt operativ som MDO-kapabel styrka kring 2030.[258]

### Morpheus

Brittiska Morpheus beskrivs som ett försvarsprogram för att leverera nästa generations taktiska kommunikations- och informationssystem (*Tactical Communication and Information System*, TacCIS) för stridskrafter främst inom markdomänen, men även delar av sjö och luft. Initiativet genomförs i samverkan mellan funktioner som taktiska kommunikations- och informationssystem, arméns högkvarter, samt ledning för gemensamma styrkor. TacCIS ger en sammanhållen och fullt integrerad taktisk informations- och kommunikationsmiljö som förenklar användningen och gör det möjligt för förband att fokusera på uppdrag istället för systemen. Morpheus beskrivs som ett första exempel på *Defence-as-a-Platform* (DaaP) inom det taktiska området.[259]

Detta initiativ har dock haft tydliga utmaningar, och 2023 rapporterades att det brittiska Försvarsdepartementet ifrågasätts angående hur medel använts för programmet.

257 U.S. Army, The Army Unified Network Plan 2021 (2021), https://api.army.mil/e2/c/downloads/2021/10/07/d43180cc/army-unified-network-plan-2021.pdf.

258 U. S. Army, The Army Unified Network Plan 2.0 (2025), https://api.army.mil/e2/c/downloads/2025/03/04/0b7f95c5/army-unified-network-plan-2-0.pdf.

259 MOD, 'Morpheus Programme: Next Generation Tactical Communication Information Systems for Defence', GOV.UK, 2016, https://www.gov.uk/guidance/morpheus-project-next-generation-tactical-communication-information-systems-for-defence.

Programmets kostnad uppgick vid denna tid till cirka 3,2 miljarder GBP och riskerar därmed att påverka den brittiska arméns framtida digitaliseringsinitiativ. Utmaningarna relateras till leverantörers svårigheter att leverera tekniska lösningar, vilket också påverkar avveckling och utfasning av tidigare kommunikationssystem.[260] Morpheus finns fortfarande kvar som en del av *The Land Environment Tactical Communications and Information Systems* (LETacCIS), det större program som syftar till att leverera taktiska militära kommunikationssystem.[261] En oberoende projektgranskning avseende Morpheus för att klargöra framtid och hantering av utmaningar var planerad till tidigt 2025.[262] Programmet LETacCIS, som initierades 2013, ser dock ut att löpa enligt plan fram till 2035.[263]

### Joint All-Domain Command and Control

Det amerikanska Försvarsdepartementets strategi *Joint All-Domain Command and Control* (JADC2) lanserades 2019 för att möta behovet av att etablera en gemensam styrka över samtliga stridsdomäner samt inom hela det elektromagnetiska spektrumet i syfte att kunna möta motståndare oavsett tid och plats. Denna strategi är en vision som beskriver förbättrade gemensamma förmågor inom ledning och styrning genom att koppla samman sensorer med verkanssystem. JADC2 stödjer utveckling av lösningar som nyttjar avancerade och intelligenta tekniker i kombination med en vilja och inriktning att utveckla och modifiera befintliga organisatoriska strukturer och processer.[264] En genomförandeplan för JADC2 signerades 2022 och viss grundläggande funktionalitet var planerad till slutet av 2023 eller början av 2024.[265] Ett namnbyte till det utökade namnet CJADC2 (*Combined Joint All-Domain Command and Control*) genomfördes 2023 i syfte att betona behovet

260 Peter Felstead, ‘UK MoD Cancels Morpheus EvO Comms System Contract’, European, 2023, https://euro-sd.com/2023/12/major-news/35641/uk-mod-kills-morpheus-contract/.

261 MOD, ‘LETacCIS Programme’, GOV.UK, 2023, https://www.gov.uk/guidance/le-taccis-programme.

262 George Allison, ‘Defence Minister Confirms Delays to Morpheus Comms Project’, UK Defence Journal, 4 December 2024, https://ukdefencejournal.org.uk/defence-minister-confirms-delays-to-morpheus-comms-project.

263 MOD, ‘MOD Government Major Projects Portfolio Data March 2024’, Ministry of Defence, 2025, https://www.gov.uk/csv-preview/6787e4b2bca9366c9f56df7f/MOD_Government_Major_Projects_Portofolio_AR_Data_March_2024.csv.

264 DOD, Summary of the Joint All-Domain Command & Control (JADC2) Strategy (2022), https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf.

265 Jon Harper, ‘Pentagon Hopes to Ring in New Year with Minimum Viable Capability for JADC2’, Defensescoop, 15 December 2023, https://defensescoop.com/2023/12/15/dod-jadc2-minimum-viable-product-gide/.

av interoperabilitet tillsammans med internationella partners.[266,267] Den federala revisionsmyndigheten (*Government Accountability Office*, GAO) noterade emellertid 2025 flera tydliga utmaningar med CJADC2, bland annat en fragmenterad utveckling, avsaknad av övergripande organisatoriska ramverk, isolerade insatser, bristfälligt erfarenhetsutbyte samt alltför omfattande sekretess, vilket resulterar i begränsning av samverkan. GAO rekommenderade tydligare riktlinjer, förbättrad datadelning samt att hinder rörande interoperabilitet och policyer åtgärdas för att en potentiell tidsplan fram till 2030 skulle kunna hållas.[268]

### Integrated Air and Missile Defence

Natos integrerade luft- och missilförsvar (*Integrated Air and Missile Defence*, IAMD) är en del av Natos försvarsstrategi för att skydda alliansens territorium, civilbefolkning och styrkor mot olika typer av luft- och missilhot, inklusive ballistiska missiler, kryssningsmissiler och obemannade flygsystem. NATO IAMD integrerar sensorer, vapen och ledningssystem mellan medlemsnationer i syfte att säkerställa snabba och effektiva svar på luftburna angrepp. Syftet är att stärka Natos förmåga att hantera nuvarande och framtida utmaningar i en alltmer osäker omvärld.[269] Centrala principer omfattar bland annat ständig hotmedvetenhet, multidomänintegration, interoperabilitet, anpassad och flexibel respons, offensiva operationer och såväl kontinuerlig koordinering och anpassning som resiliens och överlevnadsförmåga.[270] Följande funktionsområden omfattas: luftövervakning, stridsledning, ledning, kommunikation och information, samt aktivt och passivt luft- och missilförsvar. En heltäckande lösning förutsätter effektiv samordning och integration av dessa funktionsområden.[271] En formaliserad målbild och fastställt slutdatum saknas, men initiativet kan sammankopplas med andra Natoinitiativ som *European Sky Shield Initiative* (ESSI).[272]

---

266 Jaspreet Gill, 'Return of CJADC2: DoD Officially Moves Ahead with "Combined" JADC2 in a Rebrand Focusing on Partners', Breaking Defense, 16 May 2023, https://breakingdefense.com/2023/05/return-of-cjadc2-dod-officially-moves-ahead-with-combined-jadc2-in-a-rebrand-focusing-on-partners/.

267 Joseph Clark, 'Hicks Announces Delivery of Initial CJADC2 Capability', U.S. Department of Defense, 21 February 2024, https://www.defense.gov/News/News-Stories/Article/Article/3683482/hicks-announces-delivery-of-initial-cjadc2-capability/.

268 GAO, 'Defense Command and Control: Further Progress Hinges on Establishing a Comprehensive Framework', U.S. Government Accountability Office, 8 April 2025, https://www.gao.gov/products/gao-25-106454.

269 NATO, 'NATO Integrated Air and Missile Defence', North Atlantic Treaty Organization, 2025, https://www.nato.int/cps/ua/natohq/topics_8206.htm.

270 NATO, 'NATO Integrated Air and Missile Defence Policy', North Atlantic Treaty Organization, 2025, https://www.nato.int/cps/ie/natohq/official_texts_233084.htm.

271 NATO, 'NATO Integrated Air and Missile Defence Policy',, North Atlantic Treaty Organization, 2025, https://www.nato.int/cps/ie/natohq/official_texts_233084.htm.

272 NATO, '14 NATO Allies and Finland Agree to Boost European Air Defence Capabilities', North Atlantic Treaty Organization, 13 October 2022, https://www.nato.int/cps/en/natohq/news_208103.htm.

## Särskilda delområden

Utveckling av förmågor inom samordnade militära system kräver en helhetssyn där centrala delområden identifieras, avgränsas och vidareutvecklas. Dessa delområden utgör grundläggande komponenter i ett sammanhängande informationssystem och omfattar organisatoriska, tekniska och operativa aspekter vilka tillsammans möjliggör samordnad verkan i enlighet med militär doktrin. Nedanstående delområden lyfts därför fram som särskilt viktiga för utvecklingen av samordnade militära system.

### Standarder och ramverk

Standarder och ramverk används för att säkerställa att system från olika funktioner, domäner och allierade parter kan samordnas och samverka. Militära ramverk omfattar både arkitektur- och säkerhetskrav, inklusive teknisk säkerhet och cybersäkerhet, i syfte att skydda konfidentialitet, tillgänglighet och integritet. Standarder för systemarkitektur stödjer utvecklingen av modulära och skalbara lösningar som kan anpassas till förändrade operativa behov med bibehållen säkerhet. Eftersom samordnade system förutsätter interoperabilitet, skapar detta ett behov av utveckling av gemensamma standarder. Den ökande användningen av avancerade tekniker såsom AI, molnbaserade lösningar och autonoma funktioner skapar ytterligare behov av nya standarder och ramverk. Samordnade system möjliggör även MDO, vilket påverkar doktrin och strategi och innebär att standarder och ramverk kontinuerligt måste utvecklas vidare för att möta framväxande strategiska, operativa och taktiska krav.

### Interoperabilitet och integration

Interoperabilitet och integration möjliggör datautbyte och koordinering mellan system och förband, vilket är avgörande för gemensamma operationer. Interoperabilitet innebär att militära system, utrustning och styrkor kan dela information, kommunicera och verka tillsammans. Samordnade system är både ett resultat av och en drivkraft bakom ökad interoperabilitet, vilket i sin tur ökar behovet av standardisering av arkitektur, protokoll och gränssnitt. En samordnad systemarkitektur främjar utvecklingen av modulära lösningar som kan integreras med både befintliga och nya system. Detta påverkar dessutom hur militära system kravställs gentemot leverantörer. Ökad interoperabilitet medför även nya risker och utmaningar, bland annat inom cyberdomänen men även organisatoriska utmaningar kopplade till finansiering, prioriteringar och tolkningar av uppdrag.

### Säker och robust kommunikation

Säker och robust kommunikation är grundläggande för samordnade militära system och möjliggör delning av data i realtid för inriktning och samordning av operationer. Integrering av autonoma system, förband och satelliter ökar den operativa potentialen men ställer samtidigt höga krav på motståndskraft mot cyberangrepp,

signalspaning och störningar. Samordnade system hanterar stora mängder känslig information, vilket kräver starka säkerhetslösningar såsom kryptering, säkra protokoll och härdad hårdvara. Den ökade integreringen över domäner gör infrastrukturen för kommunikation mer komplex och introducerar nya sårbarheter när varje delsystem kopplas in. Standardiserade kommunikationsprotokoll är nödvändiga för interoperabilitet, men kan också skapa gemensamma svagheter, öka angriparytan och göra trafikmönster alltmer förutsägbara.

### Logistik och försörjningskedjor

Dedikerade logistiksystem kan spåra resurser i realtid medan samordnade system gör det möjligt att integrera denna information med lednings-, underrättelse- och operationsdata. Detta skapar förutsättningar för en gemensam lägesbild och samordnad verkan, vilket stärker beslutsfattande och möjliggör proaktiv resursallokering. Standardiserade protokoll och utrustning underlättar dessutom resursdelning inom organisationen och med allierade parter. Prediktiv analys inom underhåll och försörjning är inte nytt, men AI och sakernas internet (eng. *Internet of Things*, IoT) gör det möjligt att automatisera och förfina denna förmåga genom realtidsdata och snabbare analys. Detta kan öka precisionen i planering och därmed stärka förbandens uthållighet. När logistikdata integreras i bredare dataflöden blir teknisk säkerhet och cybersäkerhet kritiska faktorer. Påverkan på dessa flöden kan få konsekvenser för hela försörjningskedjan eller dess delar.

### Cybersäkerhet

Ökad integration i samordnade system ställer höga krav på cybersäkerhet. Cybersäkerhet behövs för att skydda konfidentialitet, integritet och tillgänglighet i dataflöden samt för att motverka otillåten åtkomst. När fler funktioner, plattformar och sensorer kopplas samman ökar även systemens angreppsyta. Det innebär att en komprometterad komponent kan påverka stora delar av nätverket. Denna beroendestruktur gör robusta säkerhetsåtgärder avgörande. Cybersäkerhet omfattar både förebyggande skydd och övervakning liksom cyberförsvar för att upptäcka och hantera nya hot i realtid. I takt med att militära system blir mer beroende av leverantörer på den civila marknaden samt kommersiell teknik krävs att säkerheten säkerställs genom hela leveranskedjan.

### Träning och simulering

Träning och övning är centrala för att utveckla och vidmakthålla militär förmåga. De kan dessutom användas för att identifiera brister i interoperabilitet, testa system och stärka kravställningen vid utveckling av samordnade system. Genom realistiska simuleringar och gemensamma träningsmiljöer kan samarbete över domäner tränas. Därigenom identifieras behov av standardiserade processer och arbetssätt. Samordnade system gör det möjligt för olika domäner att träna tillsammans genom

realtidsdelning av data och gemensamma lägesbilder, vilket också möjliggör simulering av MDO där händelser i en domän påverkar andra domäner. Digitala tvillingar kan användas för att simulera framtida scenarier och utvecklingsförlopp. Detta stärker analysen av handlingsalternativ, anpassningsförmåga och beslutsfattande. Förmågan att dela tränings- och simuleringsdata mellan tjänster och allierade parter förstärks dessutom.

### Ledning

Samordnade system utformas med utgångspunkt i ledningsförmågans krav på kommunikation, koordinering och samordnad verkan över domäner och i samverkan med allierade. Detta förutsätter standarder för interoperabilitet som säkerställer att olika tjänster, system och aktörer kan kopplas samman på ett säkert och enhetligt sätt. Effektiv ledning har alltid byggt på snabb informationsdelning och god situationsförståelse. I dagens komplexa och snabbrörliga operationsmiljö är digitala och datadrivna beslutsstöd, inklusive viss automatisering, av växande betydelse. Samordnade system sammanställer information från flera funktioner och domäner till en gemensam lägesbild, vilket stärker helhetsförståelsen och underlättar koordinerat och delegerat beslutsfattande. I många situationer måste dessa system även hantera komplexitet över organisatoriska gränser, exempelvis när förband, funktioner eller totalförsvarsaktörer verkar tillsammans. Då krävs att systemen fungerar över olika organisatoriska gränser och domäner, även när doktriner, tekniska standarder eller beslutsprocesser skiljer sig åt.

## Samverkande och förutsättande förmågor och tekniker

Informationssystem kan utformas på olika sätt beroende på syfte, användningsområde och organisatoriska förutsättningar. Nedan beskrivs kortfattat följande tre centrala systemkategorier: integrerade system, samordnade system samt komplexa adaptiva system (CAS). Dessa kategorier är valda eftersom de representerar tre centrala sätt att strukturera informationssystem som direkt påverkar ledning, samverkan och samordnad verkan.

### Integrerade system

Integrerade system består av flera tekniska komponenter som sammanförs i ett gemensamt och vanligen centraliserat ramverk. Exempel är lösningar för kommunikation, vapensystem, sensorer och logistisk. Syftet är att skapa en enhetlig och tekniskt sammanhållen helhet som stödjer och möjliggör specifika militära förmågor. C4ISR[273]-system är ett typiskt exempel, där ledning, kommunikation, digitala system, underrättelser, övervakning och spaning integreras för att stärka beslutsfattande och koordinering av operationer. Integrerade system kan innehålla interope-

273 Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.

rabla delsystem men är i första hand konstruerade för att fungera som ett enhetligt system inom en organisation eller plattform, snarare än att binda samman system över domän- eller organisationsgränser. De utgör därmed en teknisk grund som stödjer flera militära funktioner och förmågor, inklusive sådana som är centrala för MDO. Medan informationssystem tillhandahåller infrastrukturen för hur data lagras, bearbetas, delas och används, implementerar integrerade system denna funktionalitet på en teknisk nivå genom att koppla samman de delsystem och komponenter som behövs för att stödja verksamheten.

### Samordnade system

Samordnade system är utformade för att fungera som en sammanhållen helhet och utformas vanligtvis från början för att stödja gemensam ledning och beslutsfattande. De bygger på standardiserade gränssnitt, gemensamma processer och hög interoperabilitet som ska möjliggöra samverkan mellan stridskrafter, funktioner och allierade parter. Till skillnad från integrerade system, som främst kopplar samman tekniska funktioner inom ett enskilt system, fokuserar samordnade system på att knyta samman flera system och verksamheter på ett enhetligt sätt i realtid. Samordnade system utvecklas i allt högre grad för att också stödja interoperabilitet mellan autonoma plattformar och sensorer. Dessa system utformas som hybrida lösningar där centraliserade informationsflöden, exempelvis för styrning och lägesbild, kombineras med decentraliserad flexibilitet vid genomförande. Målet är att uppnå både robusthet och hög anpassningsförmåga. Framtida utveckling pekar mot mer dynamiska och distribuerade system där AI-stöd och automatiserad analys integreras för att komplettera det mänskliga beslutsfattandet. Kärnan i samordnade system är att flera stridskrafter och funktioner kan förenas genom ett gemensamt informationslager som möjliggör samordnad verkan.

### Komplexa adaptiva system

Moderna militära organisationer ställs ofta inför komplexa utmaningar och problem som inte kan lösas med hjälp av traditionella metoder och angreppssätt.[274] Perspektivet på komplexa adaptiva system (eng. *Complex Adaptive Systems*, CAS) erbjuder ett sätt att förstå och hantera denna komplexitet genom att fokusera på interaktionerna mellan systemets delar istället för att studera delarna var för sig. I sådana system uppstår nya egenskaper och beteenden genom interaktionerna mellan systemets delar och de måste därmed studeras ur ett holistiskt perspektiv. Ett komplext system är ett system som består av många interagerande heterogena delar, där själva interaktionerna ses som viktiga, ibland till och med viktigare än

274 Holloman, 'Complex Adaptive Systems Theory and Military Transformation'.

enheterna själva.[275] CAS är därmed ett teoretiskt perspektiv för att studera hur ordning, mönster och struktur växer fram i komplexa sociotekniska system genom kontinuerlig återkoppling och anpassning. I militär kontext används perspektivet för att förstå och stödja MDO, där decentraliserade aktörer samverkar och skapar effekt över flera domäner.[276]

## Påverkan på militär förmåga

### Integrerade perspektiv för stärkt militär förmåga

Kombinationen av perspektiven informationssystem, samordnade system och komplexa adaptiva system (CAS) kan stärka militär förmåga genom bättre anpassning, samordning och beslutsstöd. Informationssystem utgör den grundläggande infrastrukturen för att samla in, bearbeta och dela information som stödjer ledning och möjliggör en gemensam förståelse. Samordnade system skapar en struktur för att knyta samman olika stridskrafter och funktioner, vilket i sin tur möjliggör bland annat gemensam lägesbild, koordination och samordnad verkan. CAS-perspektivet bidrar till en förståelse för hur militära organisationer kan agera effektivt i distribuerade och dynamiska miljöer genom återkoppling, framväxande mönster och delegerat beslutsfattande i linje med uppdragstaktik. Tillsammans kan dessa perspektiv öka motståndskraften, handlingsfriheten och förmågan att utnyttja framväxande mönster, exempelvis genom att identifiera och utnyttja motståndarens sårbarheter.

Samtidigt innebär utvecklingen mot samordnade system betydande utmaningar och kan leda till grundläggande förändringar i en militär organisation. Övergången från statiska och avgränsade IT-lösningar till modulära och interoperabla system som kan samverka över funktioner och nivåer påverkar både strukturen för lägesbild och formerna för beslutsfattande. Detta skapar förutsättningar för att uppgifter som tidigare hanterades genom centraliserade beslut istället kan hanteras med större inslag av uppdragstaktik och delegering, vilket därigenom ökar anpassningsförmåga, handlingsfrihet och tempo. Utvecklingen innebär också ett större behov av att balansera kontroll och autonomi, eftersom stark centralisering kan hämma flexibilitet medan för hög decentralisering kan leda till fragmentering. Organisationens struktur och arbetssätt påverkas därför i grunden. Dessutom behöver kulturella faktorer som berör ledning, ansvarstagande och användning av teknik beaktas. Detta medför också krav på att doktriner, utbildning och ledningsstrukturer utvecklas för att säkerställa att innovation, återkoppling och lärande får lika hög prioritet som

275 Matthew TK Koehler, Jose L Bricio-Neto, Ernest H Page, and Andreas Tolk, 'Applying Complex Adaptive Systems Research Results to Combat Simulations of the Generation-after-Next', The Journal of Defense Modeling and Simulation, SAGE Publications Sage UK: London, England, 2024, 15485129241233608.

276 Benjamin Selzer, 'Taking Cues From Complexity - How Complex Adaptive Systems Prepare for All-Domain Operations', Joint Force Quarterly 113, no. 2nd Quarter 2024 (2024): 4–13.

tydliga procedurer och kontroll. Sammantaget indikerar perspektiven en möjlig väg mot en mer resilient, adaptiv och effektiv militär förmåga.

### CAS och uppdragstaktik

I en alltmer oförutsägbar operationsmiljö ökar behovet av decentraliserat beslutsfattande på flera ledningsnivåer. Detta innebär att taktiska, operativa och strategiska aktörer snabbare kan anpassa sig till lokala förhållanden och förändrade förutsättningar, i linje med både principerna för uppdragstaktik och perspektivet på komplexa adaptiva system (CAS). CAS betonar att aktörer på olika nivåer behöver kunna fatta beslut utifrån lokal information särskilt när central kommunikation är begränsad eller när situationen förändras snabbt. Genom att betona lokalt beslutsfattande, återkoppling och kontinuerlig anpassning, förklarar CAS varför decentraliserad ledning stärker organisationens totala handlingsförmåga under osäkerhet. I detta ramverk görs även samordnade system ytterligare flexibla, eftersom de kan fortsätta fungera trots störningar i enskilda komponenter genom alternativa flöden, redundans och lokala beslut. Samordnade system kan därmed bli flexibla och självkorrigerande samtidigt som organisationen som helhet blir bättre på att lära och dela kunskap.[277]

I en tid av ökande maktkonkurrens försöker militära aktörer dessutom utnyttja komplexitet som strategisk fördel. Detta kan omfatta utveckling på flera nivåer, från strategi och operativ inriktning till taktik och stridsteknik, exempelvis inom hybridkrigföring, nätverk för desinformation samt MDO.[278] Samtidigt skapas möjligheter att identifiera och utnyttja svagheter och sårbarheter i motståndares CAS. Exempel på sådana är sårbarheter i informationsflöden, beslutsprocesser, organisatoriska gränssnitt samt anpassningsförmåga.[279]

CAS erbjuder en teoretisk grund för att stärka militärt organisatoriskt lärande genom att betona återkoppling och anpassning. Militära organisationer kan med stöd av CAS integrera dessa principer för att stärka sin förmåga att lära av misstag och dela kunskap över domängränser.[280] Perspektiv på komplexa system blir alltmer relevanta i takt med ett ökande behov av operationer som sträcker sig över samtliga stridskrafter och domäner. Det behövs därför perspektiv som betonar sammankopplingen av olika domäner och främjar utveckling av förståelse för hur handlingar i

277 Holloman, 'Complex Adaptive Systems Theory and Military Transformation'.

278 Sherrill Lee Lingel, Matthew Sargent, Timothy R Gulden, Tim McDonald, and Parousia Rockstroh, Leveraging Complexity in Great-Power Competition and Warfare - Volume I, An Initial Exploration of How Complex Adaptive Systems Thinking Can Frame Opportunities and Challenges (RAND Corporation, 2021).

279 Lingel et al., Leveraging Complexity in Great-Power Competition and Warfare - Volume I, An Initial Exploration of How Complex Adaptive Systems Thinking Can Frame Opportunities and Challenges.

280 Eric M Murphy, Complex Adaptive Systems and the Development of Force Structures for the United States Air Force, Air University Press, 2014.

en domän påverkar och påverkas av andra domäner.[281] Sammanfattningsvis bidrar CAS till att samordnade system kan utvecklas till att bli mer flexibla, anpassningsbara och resilienta genom att betona interaktioner, återkoppling och decentraliserat beslutsfattande.

## Aktörer

Nyckelaktörer i utvecklingen mot samordnade militära system omfattar militära organisationer, försvarsindustri, teknikföretag, statliga myndigheter samt internationella aktörer som Nato och EU. Militära organisationer är de primära slutanvändarna men också viktiga partners i utvecklingen. Försvarsindustrin ansvarar för design och implementering, medan civila teknikföretag får en allt större roll exempelvis genom teknik för molntjänster, AI och cybersäkerhet. Statliga myndigheter sätter ramar genom standarder, finansiering, regelverk och tillsyn, och internationella aktörer driver interoperabilitet och gemensamma arkitekturprinciper. I praktiken möter dock utvecklingen av komplexa systemlösningar, som samordnade system, betydande utmaningar genom hela livscykeln. Från behovsanalys och kravställning till leverans, drift och förvaltning. Det ökande beroendet av externa aktörer kan skapa sårbarheter, intressekonflikter och bristande kontroll över kritisk teknik. En särskild risk är att samordnade system behandlas som traditionella IT-system, trots att de måste vara dynamiska, modulära och anpassningsbara. Den största utmaningen ligger därför i att utveckla såväl organisatorisk som teknisk förmåga att hantera komplexitet över tid.

## Lästips

### Informationssystem och systemperspektiv

Checkland, P., & Holwell, S. (1998). Information, systems and information systems: Making sense of the field. Chichester, UK: John Wiley & Sons.

Hanseth, O., & Bygstad, B. (2012). ICT architecture and project risk in interorganizational settings. In Proceedings of the 20th European Conference on Information Systems (ECIS 2012) (Paper 130). Barcelona, Spain: Association for Information Systems.

Maier, M. W. (1998). Architecting principles for systems-of-systems. Systems Engineering: The Journal of the International Council on Systems Engineering, 1(4), 267–284.

281 Selzer, 'Taking Cues From Complexity - How Complex Adaptive Systems Prepare for All-Domain Operations'.

### Komplexa adaptiva system

Lingel, S. L., Sargent, M., Gulden, T. R., McDonald, T., & Rockstroh, P. (2021). Leveraging complexity in great-power competition and warfare—Volume I, An Initial Exploration of How Complex Adaptive Systems Thinking Can Frame Opportunities and Challenges. Santa Monica, CA: RAND Corporation.

Schilling, R. D., Beese, J., Haki, M. K., Aier, S., & Winter, R. (2017). Revisiting the Impact of Information Systems Architecture Complexity: A Complex Adaptive Systems Perspective. In Proceedings of the International Conference on Information Systems (ICIS 2017). Seoul, South Korea: Association for Information Systems.

Selzer, B. (2024). Taking Cues From Complexity—How Complex Adaptive Systems Prepare for All-Domain Operations. Joint Force Quarterly, 113(2), 4–13.

### Komplexa system och militär ledning

Berggren, P., Hörling, P., Mårtenson, C., Schubert, J., Suzic, R., & Svenson, P. (2007). Viktig informationsfusionsforskning i omvärlden 2006 (No. FOI-R--2252--SE). FOI – Totalförsvarets forskningsinstitut.

Frelin, J., & Norén, A. (2012). Recent Developments in Evaluation & Conflict Analysis: Tools for Understanding Complex Conflicts (No. FOI-R--3406--SE). FOI – Totalförsvarets forskningsinstitut.

Johansson, B. J. E., Berggren, P., & Trnka, J. (2015). Research on Agility and Agile Command and Control Organizations: A Review of Contemporary Literature (No. FOI-R--4068--SE). FOI – Totalförsvarets forskningsinstitut.

# Ledning

*Niklas Hallberg*

## Inledande beskrivning

Den framtida operationsmiljön kommer att präglas av komplexitet, osäkerhet och snabba förändringar. Detta ställer krav på militära organisationer att snabbt kunna anpassa sig och anamma ny teknik för att överträffa motståndare. Modern teknik har stor potential att göra människor och organisationer effektivare och mer precisa i att lösa sina uppgifter. Införandet av teknik bör dock inte ske i syfte att helt ersätta människor, exempelvis i beslutsfattande, utan ses som ett komplement som stärker förmågan. När det gäller ledning är teknikens roll en viktig aspekt att beakta, då frågor som moral, etik, kontroll och ansvar behöver hanteras.

Modern krigföring kommer att involvera flera stridskrafter i genomförandet av operationer, med verkan samordnat i flera domäner. Involverade stridskrafter kan utgöras av egna förband, men också av internationella partners och nationella aktörer inom Totalförsvaret. Genomförandet av samordnade operationer beskrivs i koncept såsom *Multi-Domain Operations* (MDO)[282], *Joint All Domain Operations*[283] och Gemensamma operationer[284].

Försvarsmaktens ledningsförmåga ska tillse att dessa stridskrafter kan genomföra operationer enskilt eller tillsammans i en eller flera av de fem domänerna mark, sjö, luft, cyber och rymd. Att leda i en försvarsmaktskontext handlar dock inte enbart om att leda militära operationer, utan även om att leda utveckling, skapande, vidmakthållande och avveckling av förmågor, förband och system. Detta kapitel begränsas dock till ledning av operationer, även om delar kan generaliseras till övrig ledning.

Förmågan att leda ska säkerställa att militära operationer genomförs med rätt insats, vid rätt tidpunkt och med rätt resurser. Försvarsmakten definierar ledning som att inrikta och samordna tilldelade resurser för att koncentrera verkan och nå uppsatta mål.[285] Inom Nato förordas att ledning måste innefatta förmågan att orkestrera (eng. *orchestrate*) egna resurser och synkronisera (eng. *synchronize*) med andra aktörer för att kunna hantera den komplexa framtida operationsmiljön i form av så kallade multidomänoperationer (MDO).

282 Abdelzaher, T., Taliaferro, A., Sullivan, P., & Russell, S. (2020, May). The multi-domain operations effect loop: from future concepts to research challenges. I Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications II (Vol. 11413, p. 1141304). SPIE.

283 Voltz, C., Reith, M., Long, D., & Dill, R. (2021, February). Improving joint all domain operations (JADO) education. In International Conference on Cyber Warfare and Security (pp. 401-408). Academic Conferences International Limited.

284 Försvarsmakten (2020). Doktrin för Gemensamma operationer (FM2018-18369:30). Försvarsmakten.

285 Försvarsmakten (2020). Doktrin för Gemensamma operationer (FM2018-18369:30). Försvarsmakten.

En framtida adekvat militär ledningsförmåga förutsätter ledningsplatser som kan ta emot och nyttja information från sensorer och andra källor, oavsett i vilken domän dessa befinner sig. Ledningsplatserna måste också ha förmåga att leda resurser och samverka med enheter oberoende av vilken stridskraft dessa tillhör. Detta ställer i sin tur krav på nyttjandet av avancerade tekniska stödsystem, flexibilitet, integration, interoperabilitet och säker informationshantering.

Då ledning är en kritisk förmåga för genomförandet av militära operationer utgör ledningsplatser högvärdiga mål för motståndare. För att undvika att slås ut måste ledningsplatser vara en kombination av skyddade, dolda, rörliga och spridda.

## Trender och exempel

Genomförandet av militära operationer kommer att kräva snabb respons och samordning mellan förband från olika försvarsgrenar och nationer. Även samverkan med civila aktörer kommer att vara viktigt. Detta ställer omfattande krav på en stärkt ledningsförmåga, som kan leda olika typer av förband och funktioner för insatser över domängränser, enskilt och tillsammans med allierade och civila aktörer. Att stärka ledningsförmåga förutsätter förmågan att kontinuerligt kunna anskaffa och tillgodogöra sig ny teknik som stöd för kommunikation, informationshantering och beslutsfattande. Vid införandet av ny teknik är det samtidigt viktigt att beakta de icke-tekniska egenskaperna såsom personalens kompetens, metod, organisation och regelverk, för att erhålla ett socioteknisk system i balans.

### Dynamisk ledning

Den traditionella militära ledningen bygger på en fast hierarkisk struktur och tydliga beslutsvägar. För att framgångsrikt kunna genomföra militära operationer i en osäker och föränderlig miljö krävs dock en ledning som flexibelt kan anpassas efter situationen. Särskilt då operationer kräver samordning av stridskrafter och civila aktörer, som kan agera snabbt och samordnat med hög precision i flera domäner samtidigt. Dynamisk ledning innebär att styrningsform, organisation och ledningsförmåga anpassas efter uppgiftens karaktär och rådande omständigheter.

I enlighet med uppdragstaktik eftersträvas att de som är nära situationen ska ges stor handlingsfrihet att avgöra hur de ska lösa tilldelade uppdrag. Men att det finns situationer som kräver begränsningar av denna handlingsfrihet, till exempel vid behov av hög grad av samordning och när beslut riskerar att få långtgående politiska och strategiska konsekvenser. I sådana fall behöver mer av direktstyrning tillämpas, med tydlig avgränsning av hur uppgifter ska lösas och vilka resurser som får nyttjas. Det är en betydande utmaning att avgöra vilken ledningsnivå som beslut ska fattas på. Men en dynamisk ledning innebär att kontinuerligt kunna anpassa grad av uppdragsstyrning utifrån situationen. Denna form av ledning förutsätter en

kultur baserad på tillit, ansvarstagande samt som uppmuntrar till initiativtagande och nyttjande av erfarenheter för kontinuerligt lärande och utveckling.

Ledningsorganisationer behöver vara skalbara utifrån den ledning som krävs för att lösa en aktuell uppgift. De behöver också kunna anta en lämplig form för genomförandet, såsom en funktions- eller lagstruktur. Det kommer att finnas behov av att snabbt kunna skapa tillfälligt sammansatta ledningsfunktioner för att lösa uppgifter och utnyttja uppkomna möjligheter, där situationen är avgörande för vem som bör leda respektive underställas. En möjlig dynamisk organisationsstruktur skulle kunna vara en funktionsindelad grundorganisation, som nyttjas för att kontinuerligt avknoppa ledningslag vilka ges stor handlingsfrihet att lösa specifika uppgifter och situationer. Ledningsförmågan hos dessa ledningslag måste kontinuerligt kunna justeras utifrån uppdragets krav, den aktuella situationen, förutsedd händelseutveckling och de resurser som ska ledas.

För att en dynamisk ledning ska fungera i praktiken ställs höga krav på tillförlitliga sambandssystem och anpassningsbara beslutsstöd, kompetens och beslutsförmåga, socioteknisk interoperabilitet samt en etablerad kultur avseende tillit och förtroende.

### Resilient ledningsstöd

Den framtida ledningsförmågan kommer att i stor utsträckning vara beroende av tekniska stödsystem. Därav kommer motståndare att göra sitt yttersta för att påverka och begränsa ledningsförmågan genom bland annat telekrigföring och cyberangrepp. Detta medför att tekniska stödsystem inte kan förutsättas fungera fullt ut och/eller att information inte är tillförlitlig. För att upprätthålla ledningsförmågan måste denna vara anpassningsbar i förhållande till de ledningsstödsystem som finns att tillgå. Ett stöd för att säkerställa motståndskraft hos ledningsförmågan är att tillämpa principerna för modellen PACE (*Primary, Alternate, Contingency* och *Emergency*) för att skapa motståndskraft vid bortfall av stödsystem. Detta kan ske genom att exempelvis anpassa arbetssättet, såsom att planera för flera nivåer av degradering så att verksamheten kan fortsätta även vid störningar i de ordinarie stödsystemen.

- *Primary* (sv. primärt) avser det föredragna och mest effektiva arbetssättet, vilket förutsätter att ordinarie stödsystem fungerar som avsett.
- *Alternate* (sv. alternativt) utgör ett alternativt arbetssätt som i möjligaste mån bibehåller effektiviteten men är oberoende av de tekniska stödsystem som nyttjas primärt.
- *Contingency* (sv. reservlösning) används när varken det primära eller det alternativa arbetssättet är genomförbart. Det ska fortfarande möjliggöra beslutsfattande och kommunikation, men med lägre tempo och större arbetsinsats.

- *Emergency* (sv. nödlösning) utgör den sista utvägen när samtliga andra stödsystem har fallit bort. Syftet är att bibehålla en grundläggande ledningsförmåga, även om den är starkt begränsad.

Genom att tillämpa PACE-principen vid utformningen av ledningssystem kan ledningsförmågan upprätthållas även under förhållanden med tekniska störningar och motståndares aktiva påverkan.

### Datadriven ledning

Data kommer att utgöra en central del i framtida krigföring och beslutsfattande. Genom att systematiskt samla in, bearbeta och analysera stora mängder data från sensorer och andra informationskällor skapas förbättrad situationsförståelse samt förutsättningar för att utveckla och vidmakthålla modeller för AI-baserade beslutsstöd. Detta möjliggör att bättre och snabbare beslut kan fattas även i en komplex och föränderlig operationsmiljö.

Datadriven ledning bygger på integrerade informations- och kommunikationssystem som möjliggör ett kontinuerligt och rikt dataflöde. Till detta krävs automatiserade analysverktyg som kan identifiera mönster samt förutsäga motståndarens agerande och optimera det egna agerandet. Utvecklingen av den datadrivna ledningsfunktionen ställer höga krav på tillgången till tillförlitliga data, resilient infrastruktur, avancerade beslutsstöd samt förmåga att skydda information och system mot cyberangrepp och telekrig.

För att den datadrivna ledningsfunktionen ska bli effektiv förutsätts även att tekniken harmoniseras med ledningssystemets övriga delar, såsom kompetenser, metodik, organisation och regelverk. Beslutsfattare måste kunna samverka med tekniska system och samtidigt kritiskt värdera och ifrågasätta de underlag som genereras. En väl utvecklad datadriven ledningsfunktion bidrar till ökad precision, tempo och situationsanpassning i militära operationer.

### Digitala assistenter

För att utnyttja den potential som den digitala tekniken erbjuder, kan gränssnittet till detta tekniska ledningsstöd utformas i form av digitala assistenter. Dessa assistenter är intelligenta agenter baserade på AI som kan besvara frågor och utföra uppgifter.[286] Digitala assistenter kan vara röst- eller textstyrda och finns i flera olika former – från virtuella assistenter i mobiltelefoner, datorer och högtalare, till holografiska[287] och *Augmented Reality* (AR, sv. förstärkt verklighet) lösningar samt

286 Maedche, A., Legner, C., Benlian, A., Berger, B., Gimpel, H., Hess, T., ... & Söllner, M. (2019). AI-based digital assistants: Opportunities, threats, and research perspectives. Business & Information Systems Engineering, 61, 535-544.

287 AlShaghroud, S., AlShuwaier, A., & AlRakaf, L. (2023, July). Artificially Intelligent and Interactive 3D Hologram. In International Conference on Human-Computer Interaction (pp. 367-373). Cham: Springer Nature Switzerland.

fysiska robotar.[288] De har förmåga till prediktiv såväl som emotionell interaktion. Prediktiv interaktion innebär att de kan tolka ofullständiga kommandon och förstå mänskliga aktörers intentioner. Emotionell interaktion innebär att de anpassar interaktionen till de mänskliga aktörernas känslomässiga reaktioner och tillstånd, t.ex. baserat på ansiktsuttryck, röst eller kroppsspråk.[289]

Digitala assistenter kan utvecklas för att stödja militärt stabsarbete genom att effektivisera informationshantering och beslutsfattande.[290,291] De fungerar som en del av ledningslaget och stärker de mänskliga stabsmedlemmarna i deras uppgifter. Digitala assistenter kan bidra till taktiserande genom att föreslå insatser som är spelteoretiskt optimala. De utgör en central komponent i gränssnittet mellan de mänskliga aktörerna och de tekniska stödsystemen. De kan stödja uppgifter som att:

- sammanställa och analysera information
- föra minnesanteckningar och passa radiokommunikation
- översätta information mellan olika språk
- omvandla information mellan text, ljud och bild
- upptäcka svaga signaler och anomalier i stora datamängder
- ta fram beslutsunderlag och förbereda rapporter till högre chef
- hantera sambandssystem och kommunikation
- tolka uppgifter, föreslå och värdera inriktningar och planer.

Digitala assistenters stöd kan ske i form av autonoma funktioner eller genom dialog med beslutsfattare och andra stabsmedlemmar. På en ledningsplats kan digitala assistenter antingen vara anpassade för specifika uppgifter eller ha mer generella roller. De kan därmed vara avpassade till att stödja en individ, ett arbetslag, eller en funktion. Digitala assistenter kan ge förbättrad interaktion för människor med tekniska beslutsstöd och information. Detta genom att ge chefer och stabspersonal ökade möjligheter att visualisera och interagera med komplexa datamängder för att jämföra olika handlingsalternativ och fatta mer informerade beslut.

---

288 Dalberg, E., During, C. Alenljung, Z., Wickenberg Bolin U., Hagström, M., Hallberg, N., Johansson, BJE., Kindvall, G. & Lindberg, A. (2023). Social robotik - en avskanning av forskningsfronten (FOI-R--5487--SE). Totalförsvarets forskningsinstitut.

289 Castellano, G., Kessous, L., & Caridakis, G. (2008). Emotion recognition through multiple modalities: face, body gesture, speech. Affect and Emotion in Human-Computer Interaction: From Theory to Applications, 92-103.

290 Schubert, J., Brynielsson, J., Nilsson, M., & Svenmarck, P. (2018, November). Artificial intelligence for decision support in command and control systems. In 23rd International Command and Control Research & Technology Symposium "Multi-Domain C2" (Vol. 2, pp. 18-33).

291 Kerbusch, P., Keijser, B., & Smit, S. (2018). Roles of AI and simulation for military decision making. In STO Meeting Proceedings MP-IST-160. NATO.

## Särskilda delområden

Det finns ett flertal modeller för att beskriva ledning, exempelvis indelat i förmågor. I detta avsnitt beskrivs en modell som strukturerar ledning i sex generiska ledningsförmågor och hur dessa stöds av de digitala assistenterna. De generiska ledningsförmågorna är: (1) inhämta data och information, (2) skapa lägesbild, (3) etablera situationsförståelse, (4) skapa inriktning och planer, (5) skapa och delge order samt (6) sammanställa och skicka rapporter.

### Inhämta data och information

Stora mängder data och information erhålls kontinuerligt från sensorer och andra informationskällor, exempelvis rapporter från underställda. Dessutom finns det en omfattande mängd information tillgänglig via internet. Stabilt samband och digital infrastruktur ger förutsättningar för att lokalisera källor för att inhämta data och information. För att stödja förmågan att inhämta data och information kan digitala assistenter nyttjas för att:

- identifiera källor med relevant data och information samt inhämta dessa
- ta emot inkomna data och information
- annotera, klassificera och kvalitetsbedöma data och information
- passa radion och dokumentera det som kommuniceras via den
- identifiera och larma om kritiska händelser som kräver omedelbar uppmärksamhet från ledningsplatsens medarbetare, exempelvis misstänkt fientlig aktivitet.

### Skapa lägesbild

En lägesbild är en teknisk representation av den faktiska situationen och en förutsättning för att kunna erhålla korrekt situationsförståelse. Förmågan att skapa en lägesbild innebär att omsätta insamlade data och information, vilka beskriver aktuell, historisk och prognostiserade situationer. För att stödja förmågan att skapa lägesbild kan digitala assistenter nyttjas för att:

- skapa relationer mellan data och information
- generera digitala lägesbilder baserat på erhållen information
- generera prognostiserade digitala lägesbilder om framtida situationer.

### Etablera situationsförståelse

För att chefer och medarbetare ska uppnå relevant situationsförståelse måste de ha tillgång till representativa och aktuella lägesbilder som kan betraktas med olika perspektiv, exempelvis avseende tid, rum, aktörer och sekvenser av händelser. För att underlätta interaktionen med en lägesbild kan denna omsättas till en digital

tvilling av operationsområdet. Möjliga handlingsalternativ kan prövas utifrån den digitala tvillingen för att skapa förståelse av potentiella utfall och konsekvenser av både egna och motståndarens ageranden. Detta möjliggör en djupare insikt i situationen och hur den kan förändras beroende på vidtagna åtgärder. AR-tekniker kan användas för att åskådliggöra lägesbilden, vilket ytterligare förbättrar förståelsen av den operativa situationen. För att stödja förmågan att etablera situationsförståelse kan digitala assistenter nyttjas för att:

- visualisera den digitala lägesbilden
- anpassa lägesbilden och interaktionen för specifika användare, uppdrag och aktuell situation
- dialogisera läget och möjliga handlingsalternativ
- stödja genomförandet av spel för att betrakta möjliga händelseutvecklingar.

### Skapa inriktning och planer

Utifrån det erhållna uppdraget och förståelsen för situationen skapas inriktningar för vad som ska uppnås samt planer för hur de efterfrågade effekterna ska uppnås. För att stödja förmågan att skapa inriktningar och planer kan digitala assistenter nyttjas för att:

- utveckla, värdera och föreslå inriktningar
- utveckla, värdera och föreslå planer
- påtala om beslutade insatser inte ligger inom ramen för uppdraget och insatsregler (eng. *rules of engagement*)
- stödja spelandet av beslutade planer i den digitala lägesbilden för att kvalitetssäkra och förankra genomförandet av insats
- stödja diskussioner om handlingsalternativ genom att identifiera och påtala möjligheter och risker.

### Skapa och delge order

En militär order styr hur operationer ska genomföras. Dessa är formellt formulerade för att säkerställa att involverade ska förstå vad som förväntas av dem. För förmåga att skapa och delge order kan digitala assistenter nyttjas för att:

- formulera ett utkast till order utifrån beslutad inriktning och plan
- kvalitetssäkra order utifrån beslutad inriktning och plan.

### Sammanställa och skicka rapporter

För att kunna dela information om genomfört uppdrag och hur en situation utvecklas skickas rapporter till högre chefer, partners och underställda. Att kunna sprida information om händelser och delge sin lägesbild är en viktig del i denna förmåga. Krigsdagböcker förs för att dokumentera händelser och aktiviteter vid militära operationer och krig. Dessa krävs bland annat för att i efterhand kunna analysera genomförda operationer, vilket bland annat ger möjlighet att lära av erfarenheter. Krigsdagböcker är också viktiga underlag för eventuella rättsliga tvister. För förmågan att skapa och skicka rapporter kan digitala assistenter nyttjas för att:

- sammanställa underlag av information som ska skickas
- kvalitetssäkra rapporter
- föra krigsdagbok.

## Samverkande och förutsättande förmågor och tekniker

Teknik för kommunikation och informationshantering utvecklas i snabb takt och skapar nya förutsättningar för en alltmer kompetent ledningsförmåga. Därmed blir förmågan att effektivt kunna tillgodogöra sig den tekniska utvecklingen en avgörande faktor för att stärka framtidens ledningsförmåga.

### Digitala informationssystem

Grunden för ledning är situationsförståelse och beslutsfattande. Därför är den digitala informationsteknikens utveckling av stor betydelse för ledningsområdet. Den tekniska utvecklingen drivs bland annat av att datorer kan göras mindre, med högre beräkningskapacitet samt att algoritmer och modeller som baseras på artificiell intelligens (AI) blir kraftfullare. Detta ökar möjligheterna att nyttiggöra den växande mängden data som produceras av sensorer, men som också finns tillgänglig via andra datakällor.

### Resilient digital infrastruktur

En förutsättning för att kunna nyttja modern digital teknik är tillgången till en resilient digital infrastruktur. Denna typ av infrastruktur är robust och självläkande.[292] Den behöver tillhandahålla digitala tjänster som stöd för militär ledning, såsom hög kapacitetsöverföring, videokommunikation, säker kommunikation och informationsdelning samt tillgång till datalager och beräkningskapacitet. Genom att data lagras och bearbetas på flera platser i nätverket, med stöd av teknologier såsom molnbaserade lösningar och *edge computing*, ökar både tillgänglighet och kapacitet. Denna infrastruktur måste tillåta att anslutna enheter som förlorar uppkopplingen

292 Al-Rubaye, S., Rodriguez, J., Al-Dulaimi, A., Mumtaz, S., & Rodrigues, J. J. (2019). Enabling digital grid for industrial revolution: self-healing cyber resilient platform. IEEE Network, 33(5), 219-225.

fungerar autonomt samt att de kan återanslutas sömlöst. För att vara robust måste infrastrukturen vara utformad för att motstå cyberattacker, telekrigföring, elektromagnetiska hot (EMP) och tekniska fel utan att förlora funktionalitet. Att infrastrukturen är självläkande innebär att den har förmågan att automatiskt identifiera och åtgärda problem, vilket ökar dess driftsäkerhet och tillgänglighet. Militär verksamhet är beroende av effektiv kommunikation och informationshantering – brister inom dessa områden begränsar förmågan till samordning och beslutsfattande. En resilient digital infrastruktur är även en förutsättning för att kunna vidmakthålla och kontinuerligt uppdatera AI-baserade system.

### Kommunikationssystem

Ett robust och säkert samband skapar förutsättningar för en digital infrastruktur, vilket är en nödvändighet för att kunna genomföra militära operationer. Kommunikation måste kunna ske inom ledningsplatser, med högre och underställda förband samt med sidoordnade ledningsplatser. För att säkerställa robusthet måste de kommunikationssystem som utgör grunden för samband baseras på flera olika tekniker, såsom fiber, radionät, mobilnät och laser. Se även kapitlet om kommunikationsteknik.

Radionät utgör idag grunden för militär kommunikation, särskilt i stridsområden och för enheter utan fast anslutning, såsom fartyg och flygplan. Samtidigt pågår initiativ för att öka möjligheten att använda civila mobillösningar för militär kommunikation, eftersom dessa system i allt högre grad uppfyller militära krav. Femte generationens mobilnät (5G) har egenskaper som gör det intressant för militära tillämpningar, särskilt med dess ökade kapacitet och resiliens jämfört med tidigare generationer.[293] Forskning pågår redan om nästa generations mobilnät, 6G, vilket ytterligare kan stärka den militära kommunikationsförmågan.[294]

För att undvika behovet av fiberdragning mellan noder inom ledningsplatser kan radiokommunikation med mycket höga frekvenser (runt 60 GHz) användas.[295] Detta möjliggör hög överföringshastighet över korta avstånd, där den begränsade räckvidden också minskar risken för upptäckt av en motståndare. Laserbaserad kommunikation kan användas vid fri sikt (eng. *line-of-sight*) och erbjuder mycket hög överföringskapacitet.[296] Dess fördelar inkluderar svårigheten att upptäcka och störa signalen. Dock har tekniken en begränsning i att den är väderberoende, nederbörd och dimma kan kraftigt försämra eller helt omöjliggöra dess användning.

293 Lee, M., Dimarogonas, J., Downing, B., Geist, E., Manuel, S., & Schwankhart, R. A. (2023). Opportunities and Risks of 5G Military Use in Europe. RAND Corporation.

294 Longhurst, K., & Wittenberg, V. (2024). 6G waves magazine, 8. https://oulurepo.oulu.fi/bitstream/handle/10024/48348/nbnfioulu-202403192308.pdf.

295 Harvey, J. F., Steer, M. B., & Rappaport, T. S. (2019). Exploiting high millimeter wave bands for military communications, applications, and design. IEEE Access, 7, 52350-52359.

296 Kaushal, H., & Kaddoum, G. (2017). Applications of lasers for tactical military operations. IEEE Access, 5, 20736-20753.

### Extended Reality (XR)

*Extended Reality* (XR, sv. utökad verklighet) är ett samlingsbegrepp för teknologier som kombinerar verkligheten med det virtuella.[297] De former som sannolikt får störst användning inom ledning är *Augmented Reality* (AR, sv. förstärkt verklighet) och *Virtual Reality* (VR, sv. virtuell verklighet). *Augmented Reality* innebär att digital information överlagras på den verkliga världen i realtid, vilket gör det möjligt att interagera med den digitala informationen. Genom att använda exempelvis AR-glasögon får användare tillgång till digital information direkt i sitt synfält. Inom ledningsområdet kan AR användas för att skapa dynamiska lägesbilder genom att projicera information och objekt på befintliga pappersbaserade kartor. Dagens AR-teknik bygger i stor utsträckning på glasögon, vilket innebär ett antal utmaningar. Framtida AR kan istället baseras på hologram, vilket möjliggör tredimensionella visuella representationer. En särskilt intressant tillämpning inom militär ledning är holographic telepresence, där användare kan delta i möten på distans i form av hologram. *Virtual Reality* skapar digitala världar där användare kan interagera med både information och andra användare. Till skillnad från AR innebär VR att användare är frikopplade från den fysiska miljön. Det vill säga användare ser endast den bild som visas i glasögonen och inte något av den fysiska omgivningen.

### Digitala tvillingar

Digitala tvillingar är virtuella kopior av verkliga företeelser. Förutom att den digitala tvillingen speglar verkligheten i nära realtid, kan den även manipuleras, vilket i sin tur kan påverka dess fysiska motsvarighet.[298] Inom ledningsområdet är en av de mest intressanta tillämpningarna en digital tvilling av ett operationsområde.[299] Vid en sådan tillämpning kan den digitala tvillingen fungera som en avancerad form av lägesbild, där den inte bara skulle beskriva den aktuella situationen utan även möjliggöra utvärdering av olika inriktningar och planer. Dessutom kan den digitala tvillingen användas för att verkställa beslut och därefter följa utvecklingen i realtid.

### Ledningsplatser

Ledning sker från ledningsplatser, vilka kommer att skilja sig åt i utformning beroende på tilldelade uppgifter, vilka förband och funktioner som ska ledas samt den operativa situationen. Detta avsnitt beskriver sex typiska ledningsplatser med egenskaper som framtida ledningsplatser förutsätter. Faktiska ledningsplatser kommer

297 Alnagrat, A., Ismail, R. C., Idrus, S. Z. S., & Alfaqi, R. M. A. (2022). A review of extended reality (XR) technologies in the future of human education: Current trend and future opportunity. Journal of Human Centered Technology, 1(2), 81-96.

298 Juarez, M. G., Botti, V. J., & Giret, A. S. (2021). Digital twins: Review and challenges. Journal of Computing and Information Science in Engineering, 21(3), 030802.

299 Korkmaz, M., Zulfikar, A., & Demirkesen, S. (2024). Leveraging Digital Twins as a Common Operating Picture for Disaster Management: Case of Seismic Hazards. ISPRS International Journal of Geo-Information, 13(12).

anta egenskaper av en eller flera av dessa stereotyper. De typiska ledningsplatser som beskrivs är flexibla, digitala, mobila, dolda, spridda, och virtuella ledningsplatser. Främst bidrar flexibla och digitala ledningsplatser till ökad agilitet, medan de mobila, dolda, spridda och virtuella ledningsplatserna främst bidrar till resiliens.

*Flexibla ledningsplatser*

Flexibla ledningsplatser är flexibla avseende ledningsförmåga, då dessa anpassas efter situationen. Ledningen anpassas till uppdraget, men framförallt med hänsyn till vilka behov av ledning som finns hos de resurser som ska ledas. Förändring i uppdrag och situationen samt vilka resurser som leds kan kräva justeringar av ledningsplatsens kapacitet, kompetens och ledningstempo. Ett förändrat ledningstempo kan innebära ett behov av att anpassa ledningsplatsen avseende ledningsmetod, kompetens, tekniska stödsystem och organisation.

*Digitala ledningsplatser*

Digitala ledningsplatser erbjuder avancerade digitala verktyg för att förbättra informationsinhämtning, situationsförståelse, beslutsfattande och kommunikation. De digitala verktygen används även för att sammanställa, lagra, bearbeta, analysera och visualisera information. Digitala assistenter är ett viktigt gränssnitt till de digitala verktygen. För att öka situationsförståelsen vid ledningsplatsen, för vad som sker och vad som kan komma att hända, projiceras dynamiska lägesbilder på bord och väggar, i 2D- eller 3D-format. Dessa lägesbilder möjliggör för stabspersonalen att samlas kring och gemensamt analysera situationen. Lägesbilderna gör det även möjligt att testa alternativa genomföranden. Den digitala ledningsplatsen kräver en resilient digital infrastruktur för att säkerställa tillförlitlig delning och lagring av information. Utöver ytorna för samverkan har all stabspersonal tillgång till egna skärmar och digitala assistenter för det egna arbetet.

*Mobila ledningsplatser*

Mobila ledningsplatser kan snabbt omgrupperas geografiskt. Förmågan att leda upprätthålls även under förflyttningar. Förutsättningar för mobila ledningsplatser är väl utrustade ledningsfordon och robust trådlöst samband mellan ledningsplatsens samtliga fordon. Ledningsfordonen erbjuder chefer och stabsmedlemmar en god komfort, för att säkerställa deras uthållighet. Tekniska beslutsstöd är anpassade så att de kan nyttjas fullt ut även under tiden då ledningsfordonen är i rörelse och att de kan tas med om ett fordon måste överges. Interaktion med beslutsstöd kan ske via tal vilket kan minska risken för åksjuka.

*Dolda ledningsplatser*

Dolda ledningsplatser etableras för att vara svåra att upptäcka och lokalisera, vilket minskar risken för påverkan från motståndare, exempelvis genom fysiska attacker, telekrigföring eller cyberangrepp. Detta innebär en strävan efter att minska såväl

den fysiska som den digitala och elektromagnetiska signaturen. Ett alternativ är att skapa ledningsplatser som smälter in i befintlig omgivning. Sådana kan exempelvis döljas i existerande byggnader och använda kommunikationstekniker som inte kan särskiljas från civila system.

*Spridda ledningsplatser*

Spridda ledningsplatser är uppdelade på geografiskt skilda platser. Detta för att minska risken för upptäckt samt vid upptäckt minska risken för utslagning av hela ledningsförmågan. Stabsmöten och andra sammankomster sker via videokommunikation och lägesbilder delas i realtid. Den geografiska spridningen av ledningsplatser förutsätter en resilient digital infrastruktur som medger säker kommunikation och dataöverföring mellan ledningsplatsens olika delar.

*Virtuella ledningsplatser*

Virtuella ledningsplatser är integrerade i det digitala nätverket och innehåller samma ledningsstödsystem som fysiska ledningsplatser.[300] Istället för att fysiskt närvara på en plats ansluter sig stabspersonal och chefer via datorer, mobiler, VR/AR-headset och andra enheter. Virtuella ledningsplatser utformas utifrån aktuella behov, vilket omfattar utseendet och möbleringen av de virtuella rummen, samt tillgången till datorstöd och information. Detta möjliggör skapandet av tillfälliga digitala samlingsplatser där chefer och stabspersonal kan samarbeta för att lösa specifika uppdrag och uppgifter. En fördel är att experter, som normalt inte befinner sig vid ledningsplatsen, kan ansluta sig digitalt. En annan viktig resurs är de digitala assistenterna, vilka stödjer och effektiviserar ledningsarbetet. För att virtuella ledningsplatser ska fungera krävs robusta och säkra kommunikationslösningar, resilient digital infrastruktur samt anslutningspunkter och enheter som möjliggör för chefer och stabspersonal att ansluta sig.

## Påverkan på militär förmåga

Förmågan att genomföra militära operationer enskilt eller tillsammans med andra är beroende av ledningsförmåga. Att ha en ledningsförmåga som är överlägsen motståndaren ger asymmetriska fördelar. Detta då tillgängliga resurser kan nyttjas effektivare för att med hög precision åstadkomma eftersträvansvärda effekter i rätt tid och på rätt plats. En aktuell och relevant situationsförståelse ger dessutom förutsättningar att reagera snabbare och förekomma motståndaren. Detta skapar även förutsättningar för att nyttja andra verkansmedel än rent militära.

300 Levin, B., Nilsson, S., Herkevall, J., Alenljung, Z., & Granåsen, M. (2023). Virtuella ledningsplatser - Slutrapport 2022 (FOI-R--5406--SE). Totalförsvarets forskningsinstitut.

## Aktörer

Då förmågan att leda är en förutsättning för att bedriva modern krigföring genomför de flesta nationer och allianser ett kontinuerligt utvecklingsarbete med att förbättra denna förmåga. Bland de mest framstående aktörerna finns en förståelse för att den arena som krig kommer att föras på är komplex, föränderlig och svår att överskåda. Detta förutsätter möjligheter att, över domängränser, kunna inhämta och analysera information, fatta välgrundade och snabba beslut samt åstadkomma en precis verkan som ger avsedd effekt. Att kunna nyttiggöra teknisk utveckling, allra tydligast inom AI, skapar förutsättningar för detta.

### Kina

I Kina styrs de militära resurserna, Folkets befrielsearmé (eng. *People's Liberation Army,* PLA), direkt av den högsta politiska nivån genom Centrala militärkommissionen (eng. *Central Military Commission*) och dess *Joint Staff Department*.[301] Ledningsstrukturen är starkt centraliserad, men det finns en insikt om att långa beslutsvägar försvårar ett snabbt och flexibelt agerande. Därför pågår en utveckling mot att införa inslag av uppdragstaktik och olika former av nätverksbaserat försvar, som ska möjliggöra effektivare gemensamma operationer. För att stärka denna förmåga bygger Kina upp en större och mer avancerad ledningsplats, med syftet att förbättra samordningen av komplexa operationer och öka förmågan att effektivt dela information.

Kina har också satt upp tydliga ambitioner för sin framtida krigföring. Man talar om en övergång till *informatized warfare* och därefter *intelligentized warfare*:

- *Informatized warfare* innebär att kunna inhämta, bearbeta och utnyttja information för att genomföra gemensamma operationer i flera domäner inklusive det elektromagnetiska spektrumet.
- *Intelligentized warfare* innebär ett brett användande av artificiell intelligens, kvantdatorer, *big data* och annan avancerad teknik för att förstärka den militära förmågan. Detta innebär omfattande satsningar på att nyttiggöra den civila tekniska utvecklingen för militära ändamål.

Kina arbetar även med att ta fram en egen modell för ledning av multidomänoperationer, kallad *Multi-Domain Precision Warfare*. Den bygger på integrerad ledning, samband, datorkraft, underrättelser och spaning för att snabbt kunna samordna eldkraft över flera domäner.

301 Department of Defense (DoD). (2024). Military and Security Developments Involving the People's Republic of China: Annual Report to Congress: Military and Security Developments Involving the People's Republic of China. https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF.

Liksom flera andra aktörer satsar Kinas militär på en militär *metaverse*, benämnd *battleverse*.[302,303] I denna digitala miljö skulle operatörer bland annat kunna interagera med digitala tvillingar av fysiska objekt på slagfältet.

Slutligen finns även en uttalad ambition att utveckla förmåga till kognitiv krigföring, det vill säga att påverka en motståndares uppfattningar, attityder och vilja att agera.

### Ryssland

Rysslands militära ledning är strikt hierarkisk, med en starkt centraliserad styrning där presidenten är överbefälhavare och initiativ från högre nivåer prioriteras framför lokal flexibilitet.[304] Den ryska krigföringen har traditionellt byggt på denna hierarkiska ledningsstruktur i kombination med massiv eldkraft.

Under kriget i Ukraina har dock denna ansats till ledning visat sig bristfällig. Förband har i många fall inte tillåtits agera självständigt och har då inte kunnat utnyttja uppkomna möjligheter. Resultatet har blivit långa och långsamma beslutscykler, svagt ledarskap och begränsad initiativförmåga på lägre ledningsnivåer, bristande samverkan mellan förband samt otillräcklig förmåga att snabbt överföra och bearbeta data. Detta har lett till svårigheter med att hantera dynamiska situationer på slagfältet.

För att komma till rätta med några av dessa brister satsar Ryssland på att modernisera sitt C4ISR-system (*Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance*). Genom avancerade tekniska lösningar, i många fall baserade på AI, vill man automatisera flera nyckelfunktioner, till exempel lägesuppbyggnad, informationshantering och samordning av operationer. Förhoppningen är att dessa system ska kunna lösa problemen med de annars rigida, hierarkiska och centraliserade beslutsvägarna.

### Nato

Nato strävar efter att utveckla förmågan att genomföra multidomänoperationer (MDO). MDO bygger på konceptet för gemensamma operationer (eng. *joint operations*), men omfattar även samverkan med icke-militära aktörer och inkluderar dessutom domänerna rymd och cyber. För att kunna leda MDO krävs en utvecklad ledningsförmåga, där agil ledning som sträcker sig över domängränserna samt välfungerande samverkan med civila och andra icke-militära aktörer anses vara avgörande.

---

302 Baughman, J. (2024). The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield. The Cyber Defense Review, 9, 29-36.

303 Bodén, R. & During, C. (2025). Digitala tvillingar och metaversum för försvar och säkerhet. FOI Memo 8914.

304 Grisé, M., Cozad, M., Dowd, A. M., Hvizda, M., Kennedy, J., Kepe, M., de Lataillade, C., Marcinek, K., & Woodworth, D. (2025). Russian military after Ukraine: Potential pathways for the postwar reconstitution of the Russian armed forces. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2700/RRA2713-1/RAND_RRA2713-1.pdf.

Ledningskonceptet för MDO benämns *Cross-Domain Command* och är utvecklat för att hantera komplexa och dynamiska händelser. Centralt i konceptet är principen om uppdragstaktik, som ger befälhavare handlingsfrihet att fatta beslut och ta initiativ nära de händelser som behöver hanteras. Konceptet befinner sig fortfarande i utvecklingsfasen, men förhoppningen är att det ska bli en drivkraft för ett framgångsrikt genomförande av MDO.

Natos framtida ledningsförmåga förväntas kännetecknas av distribuerad information, spridda fysiska ledningsplatser, integration av sensorer och underrättelser med verkan över domänerna samt användning av artificiell intelligens (AI) för att stödja situationsmedvetenhet, planering och beslutsfattande. Samtidigt skapar det faktum att Nato består av medlemsnationer med olika traditioner, kulturer och system betydande utmaningar avseende interoperabilitet. För att möta de tekniska utmaningarna utvecklas bland annat en gemensam digital infrastruktur för kommunikation och informationsdelning, *Federated Mission Networking* (FMN).[305]

### USA

I USA har det under en tid arbetats med att utveckla och genomföra konceptet MDO, där *Joint All-Domain Command and Control* (JADC2) ses som den tekniska möjliggöraren. JADC2 syftar till att integrera information från alla domäner för att förbättra beslutsfattandet.[306] Detta sker genom att data från ett stort antal sensorer samlas in och bearbetas med stöd av artificiell intelligens (AI), som används för att identifiera och välja mål samt föreslå lämpliga medel för verkan, såväl kinetiska som icke-kinetiska. En efterföljare är *Combined Joint All-Domain Command and Control* (CJADC2), vilket också innefattar allierade. Trots framsteg kvarstår flera utmaningar för att fullt ut realisera konceptet, inte minst när det gäller teknisk mognad och interoperabilitet.

Parallellt pågår även utvecklingen av *Next Generation Command and Control* (NGC2), ett teknikdrivet initiativ inriktat på en enhetlig, datacentrerad arkitektur som ska möjliggöra sömlös kommunikation och beslutsfattande över alla ledningsnivåer.[307] NGC2 bygger på en öppen arkitektur, agila och adaptiva system, fullständig integration, hög grad av interoperabilitet och skalbarhet.

305 Gubbels, F. (2023). NATO's Interoperability Challenge: is FMN on its own? Annual overview 2022. NATO Command and Control Centre of Excellence. https://c2coe.org/download/natos-interoperability-challenge-is-fmn-on-its-own/.

306 Zohaib Arif, Z. (2024). Command and Control: The Future of US Military Operations. Security lense. https://securitylense.com/2024/08/command-and-control-the-future-of-us-military-operations/.

307 Barrett, K. (2025). From Tactical Edge to Global Reach: The Army's Next Generation Command and Control and Its Role in CJADC2. Signal. https://www.afcea.org/signal-media/tactical-edge-global-reach-armys-next-generation-command-and-control-and-its-role.

## Lästips

Granåsen, M., Hallberg, N., Josefsson, A., & Ivari, J. (2021). Ledningskoncept 2045: Resultat av 2020 års konceptutveckling (FOI-R--5128--SE). Totalförsvarets forskningsinstitut.

Granåsen, M., Herkevall, J., Johansson, B.J.E., Tolt, G., Axell, E., Cohen, M., Josefsson, A., & Bisset, F. (2024). Att skapa en roadmap för framtidens ledning. Slutrapport Framtida ledning och ledningsplatser 2021-2023 (FOI-R--5570--SE). Totalförsvarets forskningsinstitut.

Madison, A., McDowell, K., Goecks, V. G., Hansberger, J., Olney, C. M., Ahern, C., ... & Kelshaw, C. (2025). "New" Challenges for Future C2: Commanding Soldier-Machine Partnerships. https://arxiv.org/pdf/2503.08844.

Nordström, N., Herkevall, J., & Gideskog, M. (2025). Sätt ett mål, tillsätt resurser, stå inte i vägen – Om införande av moderna arbetssätt vid mottagning och integration av IT-system inom Försvarsmakten (FOI-R--5774--SE). Totalförsvarets forskningsinstitut.

van Rijn, M., Saylam, R., Scherrenburg, M., & Dönmez, M. (2025). AI in Military C2-Systems: An Introduction and Recent Advances. NATO C2COE. https://c2coe.org/download/ai-in-military-c2-systems-an-introduction-and-recent-advances-c2coe/.

# Telekrig

*Göran Kindvall och Gunnar Marcusson*

## Inledande beskrivning

Med telekrig avses militär verksamhet som utnyttjar det elektromagnetiska spektrumet för att bekämpa, förvanska eller exploatera motparters inhämtning, bearbetning eller delgivning av information samt skydd mot för oss ogynnsamt utnyttjande av det elektromagnetiska spektrumet av andra (motparter).

En vanlig indelning av området är i elektronisk stödverksamhet (ES), elektronisk attack (EA) och elektronisk protektion (EP).

Den elektroniska stödverksamheten har som syfte att upptäcka, identifiera och lägesbestämma elektromagnetiska signalkällor. Elektronisk attack innebär utnyttjande av elektromagnetisk energi i syfte att nedsätta eller förstöra en motparts systemfunktioner eller stridsförmåga. Med elektronisk protektion menas åtgärder som minskar effekten av motståndarens telekrigföring samt åtgärder för att undvika elektromagnetiska konflikter.

Telekrig brukar också räknas som ett av flera verktyg i informationsmiljön och har därför genom åren inordnats i begrepp som ledningskrigföring, informationskrigföring och informationsoperationer. Bland andra sådana verktyg kan nämnas dator- och nätverksoperationer (ofta används enbart prefixet cyber fristående för dessa aktiviteter), vilseledning och psykologiska operationer.

Internationellt och inom Nato var det gängse begreppet tidigare *electronic warfare*, men nu används inom Nato istället *electromagnetic warfare* för telekrig. Dessutom kombineras telekrig ibland med någon form av cyberförmåga till *Cyber and Electro-Magnetic Activities* (CEMA). Storbritannien har i sin nya *Strategic Defence Review* från 2025 infört en ny domän kallad *Cyber and Electromagnetic Domain* (CyberEM), som inkluderar cyber och telekrig. Detta ska ses som ett sätt att erkänna den stora betydelse dessa områden har i modern krigföring. Britterna beskriver det så här:

> *"The cyber and electromagnetic (CyberEM) domain is at the heart of modern warfare, the enabling domain that integrates all others. It is the only domain contested by adversaries every day."*[308]

Telekrig utvecklas i takt med övrig teknikutveckling men lägger också en begränsning på hur nya tekniskt avancerade system kan nyttjas på stridsfältet. Om funktionen i dessa system störs ut tillför de inget extra värde.

Vi har sett hur både Ukraina och Ryssland har utnyttjat telekrig under den ryska fullskaliga invasionen av Ukraina. Ett omtalat exempel är att Ukraina stört ut

308 Strategic Defence Review – Making Britain Safer: secure at home, strong abroad, MoD 2025. CyberEM beskrivs i section 7.6.

kommunikationen med ryska drönare och att den ryska sidan därför istället har börjat använda fiberkablar för styrning av och kommunikation med sina drönare. Man tar till gamla metoder i väntan på att teknikutvecklingen presenterar nya möjligheter som telekrig inte biter på.

## Trender och exempel

Det elektromagnetiska spektrumet påverkar alla domäner i operationsmiljön – mark, sjö, luft, rymd, cyber. Därför är kontroll av detta spektrum ett viktigt mål för alla aktörer i konflikter.

Utvecklingen inom telekrigföring kan beskrivas som en "katt-och-råtta-lek". Ett exempel på detta kan vara att attacker med drönare leder till användning av motåtgärder som störning, vilket i sin tur leder till utveckling av motåtgärder mot dessa motåtgärder som exempelvis frekvenshoppning eller annan teknik mot störning alternativt funktioner som inte använder radiosignaler. Detta initierar "spiralformade innovationscykler" av medel och motmedel som, särskilt under krigstid, leder till minskande tidsintervall mellan åtgärder och motåtgärder.

Ukraina uppges förutom att kraftigt ha ökat produktionen av drönare och robotar även ha ökat tillverkningen av telekrigutrustning med en faktor 340 gånger och gått från ca tio företag till ca 140.[309] Därutöver uppges att i mitten av 2024 uppgraderades drönare i Ukraina och Ryssland var åttonde till tionde vecka. I maj 2025 uppgavs detta ske varannan till var tredje vecka.[310]

Samtidigt bör vi, i nuvarande och kanske även framtida omvärldsläge, förvänta oss en normalbild av fientlig påverkan på kommunikationssystem, navigeringssystem och andra system med hjälp av en blandning av telekrigåtgärder, cyber och fysiska sabotage. Jämför citatet från den brittiska *Strategic Defence Review* i inledningen till detta kapitel.

Den ökade drönaranvändningen har också drivit på användningen av telekrigåtgärder som ett medel att bekämpa dessa drönare och då bl.a. kommunikationslänkarna och satellitnavigeringssystemen.

Realiseringen av kvantsensorer kommer att ställa nya krav på telekrigföringen för att kunna uppnå effekt mot de allt bättre sensorer som kvanttekniken kommer att medge. Kvanttekniken kommer även att kunna utnyttjas för telekrigföring.

309 Wilderäng., L., Ökad ukrainsk produktion av telekrigsutrustning med 340x – intresset för Rysslands krig i Ukraina viker, https://cornucopia.se/2025/04/uppdateras-okad-ukrainsk-produktion-av-telekrigsutrustning-med-340x-intresset-for-rysslands-krig-i-ukraina-viker/#:~:text=%C3%96kad%20ukrainsk%20produktion%20av%20telekrigsutrustning%20med%20340x%20%E2%80%93,g%C3%A5tt%20fr%C3%A5n%20ca%20tio%20f%C3%B6retag%20till%20ca%20140, 2025-04-13.

310 Electromagnetic (electronic) warfare, POSTnote 749, 10 juli 2025.

I framtiden kommer det också gå att modellera den elektromagnetiska miljön allt bättre. Detta ger fördelar vid utveckling, prov och försök för såväl sensorer och kommunikation som för motmedel i form av telekrigföring.

Utvecklingen av telekrigföring går inte sällan parallellt med utvecklingen inom sensorer och kommunikation. Det gäller till exempel AESA-radar, vilken nämns i sensorkapitlet. En fullt fungerande multifunktionsantenn av AESA-typ bedöms kunna finnas inom en 10-årsperiod, dvs. cirka 2035. En sådan teknisk systemlösning kan samtidigt användas för flera funktioner, till exempel samtidig spaning och telekrigföringsinsats eller samtidig spaning och kommunikation.

Generellt är den samverkan mellan olika funktioner som medges av multifunktionssystem en viktig förutsättning för att uppnå elektromagnetisk överlägsenhet över motståndare. Civil forskning fokuserar framförallt på att kombinera kommunikation och radar. För att integrera även telekrig krävs försvarsspecifik forskning och utveckling.

## Särskilda delområden

Som nämndes i inledningen kan telekrig delas in i elektronisk stödverksamhet (ES), elektronisk attack (EA) och elektronisk protektion (EP).

ES ligger till grund för inhämtning och lägesbild. Utifrån den kan man gå vidare med beslut om egna störinsatser (EA), vapeninsatser eller andra åtgärder. Det inkluderar även motåtgärder för egenskydd, t.ex. när varnardelen i ett spaningssystem har varnat för en hotande vapeninsats. Skyddsåtgärderna kan vara telekrigmotmedel i form av vilseledning eller kan ske genom egen aktiv insats i form av störning (EA). Samtidigt måste vi också säkerställa störtåligheten hos egna system (EP).

### Elektronisk stödverksamhet

I likhet med kommunikationssystemen i sig, är telekrigsystem för verkan mot kommunikationssystem idag mjukvarubaserade och kan kombinera signalspaning och störning i samma system. Signalspaningen mot kommunikationssystem syftar till att utvinna så mycket information som möjligt om motståndarens kommunikation, t.ex. läge och typ av radiosystem. Därutöver är det av intresse att analysera eventuell förbandstyp och struktur hos motståndarens kommunikationsnätverk. Själva innehållet i kommunikationen är givetvis också av intresse men att utvinna sändningens nyttoinformation är signalunderrättelsetjänst och ligger utanför området telekrig. Den allmänna tekniska utvecklingstrenden är att försöka tillmötesgå det ständigt ökande behovet av överföringskapacitet i kommunikationsnät och system. Detta leder till att frekvensomfång och modulationstyper ständigt utvecklas, vilket är en utmaning för signalspaningssystemen.

En utmaning för signalspaning mot radarsystem är framtidens agila sändarsystem. En klassisk radar har några få parametrar som kan varieras och anpassas i måttlig utsträckning, till det syfte som radarn används för. I en framtida radar kan dessa parametrar ändras i mycket större omfattning än tidigare vilket försvårar både upptäckt och klassificering av sändaren. Det finns då inga typiska sändarmönster att jämföra mot. Utmaningen för signalspaningssystemet är att veta vad man letar efter. Här kommer sannolikt framtida ny teknik[311] kunna öka förmågan hos spaningssystemen.

Inom de elektrooptiska områdena kan man spana passivt med olika former av ljuskänsliga sensorer. Även aktiv spaning går att genomföra till exempel vid användning av laser i LIDAR[312] eller i optikspanare, där en laser kan sända med låg effekt för att via retroreflexer upptäcka sikten och andra elektrooptiska system och sedan höja effekten i lasersignalen för att störa ut sensorerna. Utvecklingstrenden av laserteknik pekar mot prestandahöjning inom både precision, styrka och signalbehandling och området har sannolikt en ökande potentiell betydelse även för telekrig.

### Elektronisk attack

För att en signal ska kunna störas måste den först upptäckas. Störningen behöver anpassas efter den utsända signalens egenskaper och mottagarens eventuella störskyddsåtgärder. Klassiska åtgärder är frekvenshopp och direktsekvensspridning, vilka även kan användas för att öka kapaciteten inom ett givet frekvensutrymme. Störning när sådana signaler används kan ske antingen genom att försöka följa frekvenshoppen, eller att störa bredbandigt över en stor del av det potentiella frekvensbandet. När det gäller direktsekvens måste man koda (eller avkoda) signalen för att få störeffekt i mottagaren. Det är mottagaren man stör för att nå sitt syfte. Men med kunskap om sändaren kan man störa mottagaren mer effektivt med en anpassad metod och störsignal än att bara använda en hög störeffekt på ett ineffektivt sätt.

Telekrigföring kan användas för att påverka kedjan från upptäckt av ett mål till bekämpning av detta mål. Med telekrigföring kan man bryta den kedjan på olika sätt. Till exempel kan man påverka spaningssystem så att de får svårare att se målen och kanske även få dem att se andra mål (som i själva verket inte finns). Störning kan ske med kraftfulla störsändare på stort avstånd, men också från den egna plattformen, eller med hjälp av störsändare med relativt låg effekt, som placeras nära den mottagare som ska störas. Målet är alltid att försvåra upptäckt av mål eller att förvilla och vilseleda så att beslutssituationen försvåras.

Skenmål är ett annat sätt att påverka både spaningssystem och målsökare. De klassiska varianterna är remsor som radarmotmedel, facklor som IR-motmedel och skenradio- och radarsändare för att försvåra för signalspaning och målsökare.

311 Detta kan t.ex. vara olika former av djupinlärning m.m.

312 LIght Detection And Ranging, LIDAR.

Remsorna anpassas i storlek efter vilken radarfrekvens de ska påverka (ge radareko) och genom att använda en kombination av remsor med olika längd kan en täckning av ett större frekvensområde uppnås.

Facklor är pyrotekniska system, som genom att emittera i en målsökares våglängdsområde utgör ett skenmål som ska få målsökaren att välja facklan istället för det tilltänkta målet.

Elektrooptiska sensorer kräver fri sikt till målet och därför är det också möjligt att avskärma mål genom användning av rök och vattendimma.

### Elektronisk protektion

Skydd mot störning i sensorer och mottagare kan handla om hur signalen moduleras eller sänds, val av lobformning eller polarisation m.m. Men redan i dag och än mer framöver är tekniska störskydd integrerade i mottagarens signalbehandling. En annan viktig del av skydd mot telekrigåtgärder är metodval och hur materielen används.

## Samverkande och förutsättande förmågor och tekniker

Som nämndes redan i inledningen bedöms telekrig och cyber ha kopplingar och till detta kan också läggas spektrumhanteringen, dvs. planering av användningen av det elektromagnetiska spektrumet för att till exempel undvika telekonflikter.[313] Samtidigt som dessa överlapp existerar finns det mycket verksamhet som är specifikt spektrumhantering, cyber eller telekrigföring. Dock kommer vi sannolikt i framtiden se situationer där integration av telekrigförmåga och cyberförsvarsförmåga (CEMA) kan bli nödvändig.

Exempel på CEMA kan vara att genomföra en cyberoperation för att få radioutrustning att sända med högre uteffekter, vilket underlättar spaning mot, och positionering av, radioutrustningen. Ett annat exempel kan vara att med hjälp av cyberinsatser få tillgång till detaljerad information om motståndarens radiokommunikation som kan användas för att förbättra såväl precision som effekt i signalspanings- och störinsatser. Sammantaget kan både cyberområdet och telekrigområdet generera kunskap om motståndarutrustning som kan möjliggöra och/eller effektivisera insatser med det andra medlet. CEMA innebär således både att nya möjligheter öppnas och att effekten av individuella cyber- och telekriginsatser kan förbättras.

Som skydd för plattformar samverkar signaturanpassningsområdet med telekrigföring. För en plattform som försöker undgå att bli träffad av en målsökarstyrd robot krävs en kombination av signaturanpassning och telekrigföring för att överleva.

313 En plan över inom vilka frekvensområden olika system får sända. T.ex. tilldelningen av radiokanaler inom rundradiobandet 88 - 108MHz; det finns bara en radiostation i varje kanal inom varje sändarområde.

Exempelvis innebär en låg signatur att det är enklare att få effekt av avledande motmedel.

Mycket av telekrigföring handlar om att kunna verka mot sensorer och kommunikation och därför är utvecklingen inom dessa områden central för effekten av telekrigföring och ställer också krav på utveckling av nya och förbättrade telekrigföringsåtgärder.

Ett annat område som har koppling till telekrigföring är elektromagnetiska vapen. Såväl HPM-vapen som laservapen verkar genom elektromagnetisk energi, även om syftet i dessa fall snarare handlar om att förstöra mål än att, som för telekrigföring med EA, att störa och förvilla.

## Påverkan på militär förmåga

Telekrigförmåga är en förutsättning för de flesta grundläggande förmågor. Signalspaning (ES) ger underrättelseunderlag, elektronisk attack är en delmängd i ett system med graderad verkan. Tillsammans med elektronisk protektion bidrar det till att öka skydd och uthållighet såväl för sensor- och kommunikationssystem som för plattformar av alla slag. Ledningsplatser och förband behöver följaktligen ges en låg signatur såväl fysiskt som digitalt och elektromagnetiskt (EP) i syfte att erhålla ett så komplett eller anpassat skydd som möjligt. Kvalificerad telekrigföring är en effekthöjare på bredden genom att skapa en bättre förståelse för motståndarens system och aktiviteter, bidra till att nedsätta dennes förmåga att observera och följa våra förband och plattformar samt skydda våra resurser från motståndarens telekrigföring.

## Aktörer

Telekrigföring är ett område med hög sekretess. Ingen vill alltför tydligt avslöja sin egen förmåga och i ännu mindre grad sina egna sårbarheter. Därför krävs det egen forskning och utveckling för den som vill ha en kvalificerad telekrigförmåga.

En marknadsanalys som genomfördes 2025 identifierade USA, Ryssland och Kina som globala ledare inom telekrigföring. Analys av antalet patent inom området publicerade på engelska mellan 1976 och 2024 rankade USA högst, följt av Kina, Japan, Sydkorea, Israel och Storbritannien. Analys av akademiska publikationer under samma period visade att Kina hade producerat flest artiklar, följt av USA, Indien, Turkiet, Storbritannien och Polen.[314]

Kinesisk militärdoktrin betonar vikten av att integrera telekrigföring, cyberoperationer och fysiska attacker som ett sätt att överväldiga en motståndares informationssystem. Kina har utvecklat flygstörsändare för avståndskontroll, eskortstörsändare

314 Electromagnetic (electronic) warfare, POSTnote 749, UK Parliament, 10 juli 2025.

för örlogsfartyg och vapen med riktad energi med integrerad AI. Kina prioriterar investeringar och kommersialisering av teknik med dubbla användningsområden, som snabbt kan implementeras i militära operationer. Det finns rapporter om att Kinas telekrigföringssystem orsakar frekventa störningar på civila och amerikanska militära plattformar i Sydkinesiska havet och Taiwansundet.

Ryssland har kontinuerligt utvecklat sin telekrigförmåga under de senaste 15–20 åren och integrerat detta med kinetiska, cyber- och psykologiska operationer. Ryssland har demonstrerat förmåga att störa radiofrekvenssystem på långa avstånd (flera hundra kilometer) och har också mobila telekrigenheter som kan störa till exempel UAV-operationer.

USA har omfattande telekrigförmåga, inklusive de system som är utformade för att samla in underrättelser och störa kommunikation, radar- och navigationssystem. USA är en ledande leverantör av avancerad telekrigföringsförmåga till Natoländer, särskilt inom luftdomänen.

## Lästips

FOI orienterar om Telekrig, Totalförsvarets forskningsinstitut (FOI), 2005 (en ny uppdaterad version planeras utkomma under 2026).

Electromagnetic (electronic) warfare, POSTnote 749, UK Parliament, 10 juli 2025.

McDaid, C., Location Tracking on the Battlefield, Enea, januari 2024, https://info.enea.com/tracking_on_the_battlefield_report?pk_vid=0254f-3f200891e54177013748639da30.

# Obemannade och autonoma system

*Martin Hagström*

## Inledande beskrivning

Obemannade system är en etablerad teknologi i militära sammanhang. Vanligtvis avses farkoster men i en utvidgad mening menas fysiska system som till del är datorstyrda, s.k. cyberfysiska system. Att en farkost är obemannad betyder att operatören, det vill säga piloten eller föraren, befinner sig på en annan plats än farkosten. Autonoma system är inte styrda av operatör utan kan agera självständigt.

Obemannade flygplan (*Unmanned Aerial Vehicles*, UAV) har funnits i över hundra år, de används militärt sedan mer än ett halvsekel och används nu i allt fler tillämpningar. Tekniken är idag inte längre förbehållen ett fåtal avancerade stater, utan är tillgänglig på konsumentmarknaden. Den civila marknaden är i flera avseenden drivande för efterfrågan av teknik för obemannade och autonoma system, men militära behov hos kvalificerade aktörer ställer särskilda krav avseende bland annat robusthet och möjlighet att agera i en ostrukturerad och antagonistisk miljö. Det är en avgörande skillnad mellan militär och civil teknikutveckling. Den civila drivs av teknikens möjligheter och marknadens intresse där teknikens svagheter inte behöver avgränsa den möjliga användningen av teknikens styrkor. Militär teknikutveckling, däremot, är hotdriven, kraven sätts inte av användaren utan av motståndaren. En motståndare kommer aktivt söka efter systemets svaga länkar. Militär teknik möter en antagonist som utnyttjar svagheter och brister i tekniken. Detta medför att det kan vara kostsamt att utveckla militära tillämpningar baserade på civilt utvecklad teknik.

Idag finns tekniska system som gör det möjligt att låta farkoster agera autonomt i många situationer där omgivningen är känd och förutsägbar och benämningen autonoma system används i ökande utsträckning. Med ett större beroende av mjukvara kommer också ökade risker för cyberangrepp på systemen. Detta är inte unikt för autonoma system men kommer kräva en ökad uppmärksamhet när sådana system tas i bruk i större omfattning.

Utvecklingen har pågått sedan 1960-talet, både av spaningsfarkoster och beväpnade UAV:er, det som nu kallas patrullrobotar. De första patrullrobotarna togs i bruk av Israel i slutet av 1980-talet och under 1990-talet kom de större flygplans-UAV:erna att användas, och fick stor uppmärksamhet under krigen i Afghanistan, Irak och konflikter i Mellanöstern. I konflikterna i Syrien, Irak, Libyen och Nagorno-Karabach användes beväpnade UAV:er i ökande omfattning. Utvecklingen av sensorer, elektronik och miniatyrisering har gjort mindre UAV:er med bra sensorsystem och god manöverförmåga tillgängliga till relativt låga kostnader i stora mängder. Detta har förändrat förutsättningarna för krigföring på flera sätt, vilket illustreras i Ukraina.

I kriget i Ukraina efter Rysslands storskaliga invasion 2022 har systemen förändrat förutsättningarna på stridsfältet. Sensorerna burna av UAV:er är allestädes närvarande och har etablerat begreppet det transparenta stridsfältet. Med hjälp av sensorerna kan alla rörelser detekteras i en zon några tiotal kilometer från sidornas kontaktlinje. Små beväpnade UAV-system används för att anfalla detekterade mål vilket lett till en förändrad taktisk situation. Rörelse utgör inte ett skydd och det är bara vid dålig sikt eller på natten som förflyttningar kan göras. Den tekniska kapplöpningen mellan medel (UAV:er) och motmedel (Counter UAS) pågår och även om medlen idag vinner över motmedlen är det inte säkert att det övertaget kvarstår i framtiden.

Till sjöss används obemannade ytfarkoster och användningen av markfarkoster ökar. Ukraina har med obemannade, fjärrstyrda, system förnekat Ryssland kontroll över Svarta havet och tillfogar regelbundet Ryssland förluster genom anfall både mot fartyg på havet, mot hamnar och även mot flygplan och helikoptrar. Markstriderna har fått stor uppmärksamhet i media men betydelsen av Ukrainas framgångar i sjödomänen är svåra att överskatta, där obemannade system har haft en nyckelroll. Obemannade markfarkoster har använts sedan första världskriget men de är de svåraste systemen att automatisera. I kriget i Ukraina pågår mycket experimenterande och det finns många försökssystem men ännu är det inte en etablerad verksamhet.

## Trender och exempel

Under konflikter drivs ofta teknikutvecklingen fram i högre takt än annars och kriget i Ukraina är ett tydligt exempel. Både Ukraina och Ryssland har etablerat truppslag med fokus på obemannade system[315] och det pågår en kapplöpning mellan medel och motmedel, vilket påskyndar utvecklingen. Farkoster behöver kunna navigera och satellitnavigeringssystem är idag det naturliga valet för denna funktion. I telestörda miljöer krävs avancerade antenner och gärna militära mottagare för att kunna utnyttja satellitnavigeringssystemen. De är emellertid både dyra och mer utrymmeskrävande än de enklare systemen som används civilt. Därför har många nationer forskningsprogram för att utveckla andra navigeringssystem som inte är beroende av kommunikationslänkar. Idag är de allra flesta obemannade systemen fjärrstyrda med automation i vissa funktioner. Flygande farkoster styrs idag typiskt genom att ange vägpunkter, eller en planerad rutt medan själva styrningen av farkosten är automatiserad.

315 Russia's Unmanned Systems Troops: Grand Plans, Slipping Deadlines https://briefly-news.com/en/russias-unmanned-systems-troops-grand-plans-slipping-deadlines/.
Russia plans to create new branch of unmanned systems, https://militarnyi.com/en/news/russia-plans-to-create-new-branch-of-unmanned-systems/.
Why Ukraine is Establishing Unmanned Forces Across Its Defense Sector and What the United States Can Learn from It https://www.csis.org/analysis/why-ukraine-establishing-unmanned-forces.

Automationen förväntas öka och idag finns system som är helt autonoma i delar av ett uppdrag. För att kunna utföra ett uppdrag helt autonomt, utan direkt påverkan av en mänsklig operatör, krävs att alla, för uppdraget nödvändiga, funktioner har automatiserats. Farkoststyrning, även under varierande väder och omständigheter, är en nödvändig funktion. I komplicerade miljöer kan hinderundvikande och omplanering vara avgörande och för uppdrag under lång tid när risk för fel i system eller delsystem ökar behöver även feldetektion och felhantering kunna omhändertas av systemet. Det kan vara svårt att i förväg bedöma hur komplicerat det är att utveckla alla de funktioner som krävs. Många förutsägelser om hur snabbt teknikutvecklingen kommer gå har visat sig vara felaktiga.

Den första autopiloten för flygplan demonstrerades redan 1914 och idag är det relativt enkelt att genomföra flygning autonomt, medan komplicerade uppdrag i komplexa miljöer är svårare. Motsvarande gäller för undervattensfarkoster, särskilt när risken för att kollidera med andra farkoster i en stor öppen vattenvolym är låg och det finns undervattensfarkoster som kan utföra enklare uppdrag helt autonomt. För ytfarkoster till sjöss och för markfarkoster har utvecklingen inte kommit lika långt. Medan det är relativt enkelt att styra ytfarkoster till sjöss måste hänsyn tas till andra fartyg och kollisioner undvikas, något som inte är tekniskt helt löst även om det finns många utvecklingsprojekt på området. För markfarkoster är utmaningarna fler. I strukturerade och kända miljöer kan fordon köra förarlöst och utvecklingen går framåt även i komplexa miljöer som stadstrafik även om många problem återstår att lösa. De första förarlösa bilarna kunde köra i trafik i slutet på 1990-talet och 2050 kommer de sannolikt finnas i trafiken i betydligt större utsträckning än idag. Militära markfarkoster, *unmanned ground vehicles*, UGV, är idag väsentligen teleopererade. Ostrukturerad och okänd miljö, särskilt i terräng, utgör ännu svårigheter avseende autonom framkomlighet. För specifika och avgränsade tillämpningar kan lösningar utvecklas men för att möjliggöra en bredare användning i olika situationer krävs såväl forskning som omfattande utveckling. Många av dagens utmaningar kommer troligtvis vara övervunna år 2050 och det kommer finnas system som fungerar, om än inte i alla situationer och miljöer, för många olika uppgifter.

## Särskilda delområden

Obemannade system finns i alla domäner, från rymden ner till under vattenytan. Varje domän ställer specifika krav på farkoststyrning och sensorutrusning samt har olika förutsättningar för kommunikation, både mellan olika obemannade system och mellan de obemannade systemen och deras användare och operatörer.

### Autonomi

Automation, eller autonomi, är ett centralt delområde som också det kravställs på olika sätt beroende på tillämpning och uppgift och som varierar mellan domänerna. Det finns fortfarande forskningsfrågor inom farkostautomation som exempelvis

feldetektion och felhantering, farkostnära funktioner som är centrala och viktiga för militära system. Feldetektion är inte ett forskningsområde som är avgränsat till obemannade system, men hur obemannade system autonomt ska kunna hantera felfunktioner och göra omplanering av ett uppdrag är en svår fråga som inte har studerats i någon större omfattning.

Flygfarkoster har redan idag en hög automationsgrad och de utvecklingsprogram som finns syftar mot autonoma system som utför olika typer av flygföretag, från spaning till attackuppdrag, helt autonomt. Några av dessa kommer vara realiserade 2050 men för att de svåraste och mest kvalificerade systemen ska bli verklighet behöver stora resurser avsättas för forskning och utveckling, projekt som storleksmässigt kan rymmas i USA:s och Kinas utvecklingsprogram. För exempel, se kapitlet om plattformar i luftdomänen.

För markfarkoster är autonom rörlighet i varierande terräng och i snö fortfarande forskningsproblem. 2050 kommer det förmodligen finnas system som autonomt kan röra sig i terräng. Vilka lösningar som ger militär nytta i olika situationer är idag inte uppenbart men det finns många uppslag, se kapitlet om markplattformar.

I sjödomänen ser de tekniska utmaningarna olika ut på och under ytan. För kortare uppdrag på begränsade ytor finns det idag demonstrerade förmågor men uppdrag över längre tid och med lång räckvidd ställer krav på, förutom avancerad automation, även energilagring och tillförlitlighet samt för ytfarkoster möjligheten att hantera olika väder. Ukraina har framgångsrikt använt obemannade ytfarkoster, både för bekämpning av fasta mål som Krimbron, och som bärare av korträckviddiga luftvärnsrobotar, där såväl helikoptrar som stridsflyg blivit nedskjutna.[316] För exempel, se kapitlet om plattformar i sjödomänen.

Uppdragsautonomi, förmågan att taktiskt planera och omplanera en militär uppgift utifrån en befälhavares intentioner och behov, är ett område som får allt större uppmärksamhet i forskningsprogram världen över. Ett exempel är svärmteknik, hur en självorganiserande grupp farkoster på ett effektivt sätt ska lösa en uppgift utan att en operatör ger detaljerade instruktioner till var och en. Ett exempel kan vara att genomföra ett spaningsuppdrag genom en avvägd utspridning av sensorer över ett intressant område, mäta in mål från flera håll för att nå hög precision i inmätning och fördela målföljningsuppdrag mellan farkoster så att uppdraget löses så väl som möjligt. För enklare uppgifter är detta möjligt att realisera i närtid men för mer komplexa uppdrag kommer det dröja men till stor del finnas tillgängligt närmare 2050.

316 Kosta Gakk and Eve Brennan, ‘Ukraine claims it destroyed Russian fighter jet using seaborne drone for the first time’, CNN, 4 May 2025, https://edition.cnn.com/2025/05/04/europe/ukraine-destroyed-russian-jet-seaborne-drone-first-intl. Boldizsar Gyori, ‘Ukraine downed 2 Russian helicopters in sea drone attack, HUR says’, Kyiv Independent, 2 January 2025, https://kyivindependent.com/ukraine-downs-2-russian-helicopters-in-sea-drone-attack/; and David Axe, ‘One Of Ukraine’s Drone Boats Just Shot Down A Russian Helicopter’, Forbes, 31 December 2024.

### Samverkan mellan operatörer och autonoma system

Relationen mellan människa och system är viktig för styrning av obemannade system och kommer vara det även för autonoma system. Metoder för att leda och använda autonoma system i olika militära tillämpningar behöver utvecklas i takt med att teknikens utveckling leder till att nya funktioner införs. Användaren kan vara allt från en operatör i en ledningscentral som övervakar en svärm av spaningsfarkoster till en operatör i ett stridsfordon där styrning av en spanings-UAV bara är en av flera kritiska uppgifter. Hur gränssnitten och kommunikationen mellan system och operatör ska utformas för att maximera situationsmedvetandet och minimera den kognitiva belastningen är frågor som är uppmärksammade men relativt nya i forskningen. Forskningsfrågorna inkluderar utvecklingen av nya mätmetoder, som ett komplement till klassisk psykofysiologisk mätteknik. Ett exempel är användningen av icke-invasiva metoder för att styra farkoster med tankekraft. År 2050 kommer systemen och interaktionsprinciperna vara betydligt mer utvecklade än idag. Det kommer finns exempel på realiseringar av begreppet *human-machine-teaming*, obemannade autonoma system som samverkar med bemannade system på ett intuitivt och i många avseenden effektivt sätt.

### Juridik

Ny teknik ställer ibland tidigare utvecklade regelverk i nytt ljus. Många av dagens regelverk innehåller explicita krav eller outtalade antaganden om människans roll i planering och genomförande av militära operationer, inkluderat vid användning av tekniska system. Detta gäller såväl internationell som nationell rätt. Med en ökande grad av automation behöver regelverken studeras och analyseras. Sådana studier kan säkerställa, dels att teknikutvecklingen inriktas mot system som kan användas rättsenligt, dels att hela det rättsliga handlingsutrymmet kan nyttjas, och därmed undvika att bristfällig förståelse av regelverken resulterar i opåkallade förmågebegränsningar. Om betydande och omotiverade begränsningar av användande av obemannade system finns i svensk rätt kan förslag på förändringar lyftas. Om motsvarande begränsningar finns i folkrätten är ändringar inte enkla att realisera, men i vissa fall kan nya och förtydligande tolkningar som svarar mot regelverkens syften och krav underlätta införandet av nya förmågor.

## Samverkande och förutsättande förmågor och tekniker

För att automatisera funktioner krävs a) sensorer, som kommunicerar och omvandlar fysikaliska parametrar till mätvärden (digital information), b) en modell av omvärlden farkosten befinner sig i, dvs. en matematisk beskrivning av hur den fysiska omvärlden fungerar, c) beslutsalgoritmer (AI eller autonomi) som baserat på mätvärdena och tillståndet systemet befinner sig i beräknar vilka åtgärder som ska vidtas, t.ex. om hur hjulen eller flygplansrodren ska vridas samt slutligen d) aktuatorer, de mekanismer i exempelvis en farkost som fysiskt verkställer den åtgärd

som ska vidtas, som att vrida på hjul eller roder. Dessa teknik- och tillämpningsområden sammanfattas ofta med termen robotik men innehåller flera delområden såsom djupinlärning för bildigenkänning, signalbehandling, automation, farkostsstyrning, optimeringslära, navigering m.fl.

Obemannade farkoster innefattar i sig många teknikområden och som nämnts ovan är robust navigering och kommunikation två centrala tekniker som inte är unika för obemannade farkostsystem. En högre grad av automation, eller autonomi, minskar behovet av kommunikation till användaren men robust navigering i telestörda miljöer kommer alltid vara ett kritiskt behov.

Utöver dessa så kommer utvecklingen av andra för plattformsutvecklingen relevanta områden att vara av betydelse. Det handlar om material- och energiteknik, som kan skapa förutsättningar för miniatyrisering och längre uthållighet, samt sensorteknik och informationsteknologi i stort. För att realisera en autonom funktionalitet för komplexa situationer krävs komplex programvara med hög tillförlitlighet. Hur sådan ska utvecklas är ett viktigt forskningsområde i sig.

## Påverkan på militär förmåga

Obemannade system har redan visat sig oundgängliga i militära tillämpningar. De har förändrat förutsättningarna på stridsfältet, dels genom att möjliggöra en konstant sensornärvaro, dels som bärare av verkansdelar och därmed göra precisionsbekämpning tillgängligt i en stor mängd. Det pågår en kapplöpning mellan medel och motmedel och den obalans dem emellan, till framförallt flygfarkosternas fördel, som kan ses exempelvis i kriget i Ukraina, kan se annorlunda ut i framtiden. Precis som det militära flyget genomgick en snabb utveckling under första världskriget utvecklas nu kunskapen om, och användningen av, obemannade system. Det senaste decenniet har tekniken utvecklats men under de senaste konflikterna, framför allt efter Rysslands storskaliga invasion av Ukraina, har det skett en snabb utveckling av taktik och hur systemen bör användas. Många nationer stärker nu sin forskning för att utveckla ny kunskap som kan stärka teknikutvecklingen. Att obemannade system med hög grad av autonomi kommer påverka den militära förmågan stort är utom tvivel, men vilka förmågor som kommer bli dimensionerande och kritiska i framtiden är ännu inte avgjort.

## Aktörer

Många länder har en aktiv utveckling av autonoma system och obemannade farkoster. De mest aktiva aktörerna har tidigare varit USA, Israel och Ryssland men många andra länder har utvecklingsprogram där vissa, som Kina, inte är lika öppna om sin forskning och teknikutveckling som t.ex. USA. Turkiet har sedan slutet på 1980-talet använt UAV:er, framförallt anskaffade från Israel och USA. Landet gjorde stora satsningar på sin egen industri efter att ha blivit nekade att köpa större

UAV:er av USA i mitten på 00-talet och är idag en av de främsta tillverkarna och exportörerna. Ukraina har efter snart 4 års fullskaligt krig etablerat en inhemsk produktion av mindre UAV:er med en årsproduktion 2025 som överstiger 4 miljoner enheter.[317] Ukraina utvecklar hela sin försvarsindustri i vilket det internationella stödet har en viktig roll.[318] Ukrainas stora satsning på obemannade system kommer sannolikt betyda att den typen av produkter får en stark ställning i landets försvarsindustri. Med ett starkt utländskt stöd, framförallt från Storbritannien och länder i EU, är det möjligt att Ukraina blir en av Europas starkaste aktörer inom området.

## Lästips

Appelgren, J., Beran, T., Musco Eklund, A., Hagström, M., Autonoma vapensystem - dagens debatt och en väg framåt Tekniska, legala och etiska aspekter, FOI Memo 6953, 2022.

Clement, S. Mastering the future of uncrewed Warfare, Sub-committee on technology trends and security, 2025-10-12 ,NATO Parliamentary Assembly, https://www.nato-pa.int/document/2025-uncrewed-warfare-report-clement-023-stctts.

Litnarovych, V., Ukraine Plans to Deploy 15,000 Combat Robots to the Frontline in 2025, United24, 2025-03-31. united24media.com/latestnews/ukraine-plans-to-deploy-15000-combat-robots-to-the-frontline-in-2025-7200.

Rantakokko, J., Nygårds, J. Obemannade farkoster för markstriden - erfarenheter från Ukraina, FOI-R--5723--SE, Juli 2025.

Rantakokko, J., Tekniköversikt autonoma och obemannade system - Del 1: Historik, FOI-R--4680--SE, 2019.

Sutton, H.I., Ukraine Has World's First Navy Drone Armed With Anti-Aircraft Missiles, Naval News, 2024-05-21 www.navalnews.com/navalnews/2024/05/ukraine-has-worlds-first-navy-drone-armed-with-anti-aircraftmissiles/.

Svenmarck, P., Melbi, A., Pestrea, A., Oskarsson, P-A., Andersson, A., Winther, P., Konsekvenser för ledning av autonoma samverkande system: Slutrapport, FOI-R--5525--SE, 2023.

317 Game of drones: the production and use of Ukrainian battlefield unmanned aerial vehicles, https://www.osw.waw.pl/en/publikacje/osw-commentary/2025-10-14/game-drones-production-and-use-ukrainian-battlefield-unmanned.

318 Russia's War Transforms Ukraine into a World-Leading Military Producer, https://jamestown.org/program/russias-war-transforms-ukraine-into-a-world-leading-military-producer/ The transformation of Ukraine's arms industry amid war with Russia https://www.sipri.org/commentary/topical-backgrounder/2025/transformation-ukraines-arms-industry-amid-war-russia Ukraine's Drone Industry The role of volunteerism and policy in building an emerging UAV Industry, https://entreprenorskapsforum.se/wp-content/uploads/2025/08/WP_74.pdf.

Watling, J., Emergent approaches to combined arms manoeuvre in Ukraine, RUSI, 2025-10-23, https://www.rusi.org/explore-our-research/publications/insights-papers/emergent-approaches-combined-arms-manoeuvre-ukraine.

# Vapensystem

*Martin Hagström*

## Inledande beskrivning

Verkanseffekt är ofta i fokus när vapen diskuteras. Mer verkan, eller rätt verkan, är centralt för vapen samtidigt som precision, hastighet och räckvidd också är kritiska egenskaper för att nå avsedd verkanseffekt. Teknikutvecklingen på vapenområdet drivs på under militära konflikter och konflikternas karaktär styr inriktningen. Under kalla kriget skedde en kapprustning på många områden med långsiktiga utvecklingsprojekt vilka ofta fokuserade på extrem prestanda för strid mellan kvalificerade motståndare. Kriget i Ukraina präglas snarare av tillämpning av existerande teknik, med korta utvecklingscykler och en hög grad av taktikanpassning och improvisation.

Det finns flera inriktningar inom teknikutvecklingen på vapenområdet. En sådan är kvalificerade vapen för strid mot kvalificerade motståndare, där hög hastighet, lång räckvidd, verkan och precision är nyckelord. En annan innebär automation, interoperabilitet och hög grad av systemintegration. Båda dessa inriktningar bär mot system av system med komplex kravställning av många ingående delsystem. Förutom de ingående vapnen integreras även sensor- och ledningssystem, vilket innebär att de totala kostnaderna brukar bli höga för sådana projekt.

Försörjningssäkerhet för ingående komponenter, såsom sprängämnen och krut, samt robusthet och redundans i produktion, är också faktorer som är kostnadsdrivande. Hur länge väpnade konflikter pågår är svårt att förutse. Kriget i Ukraina har pågått i tolv år och där tydliggörs behovet av robusthet och uthållighet i produktion och lägre kostnader för vapen, ammunition och förbrukningsmateriel. Låga kostnader med möjlighet till långa serier i anpassningsbar produktionstakt är troligen en nödvändig utvecklingsväg framåt, men för traditionella försvarsindustrier ett nytt och ovant tillvägagångssätt.

## Trender och exempel

### Övergripande trender

Inriktningen på vapenutvecklingen drivs av tekniska möjligheter, hotutvecklingen samt av ekonomisk och politisk styrning. Med låg politisk acceptans för egna förluster riktas utvecklingen mot teknik för skydd av soldater och mot förmågor för att skydda samhället från en högteknologisk fiende. Detta kräver avancerade vapen för vilka en hög anskaffningskostnad kan accepteras. Långvariga konflikter ställer krav på låga styckekostnader och robusthet i produktion och leverans. Vilken teknikutveckling som bedrivs beror således både på politiska vägval och på omvärldens

utveckling. Kriget i Ukraina präglades under den första perioden 2014 – 2022 av lågintensiva strider där båda sidor använde begränsade resurser. Kriget efter 2022 handlar däremot om intensiva strider där teknikutvecklingen, eller olika tillämpningar av teknik, drivs fram i en ständigt pågående duellsituation med korta utvecklingscykler. Produktionskapacitet har stor påverkan på parternas förmåga. Både Ukraina och Ryssland har på relativt kort tid byggt upp en stor produktionsförmåga av mindre UAV:er för att bära vapen och sensorer. Produktion av avancerade vapen, kvalificerade system och ammunition är svårare att öka på kort tid men Ryssland med sin historiskt starka försvarsindustri ser ut att ligga före Ukraina. Detta pekar på vikten av etablerade forskningsinstitut och industrier.

Vilka som är de bästa vapensystemen beror på typ av konflikt. Operationsområdets miljö styr kravbilden där avstånd, väderförhållanden och motståndarens utrustning är faktorer som styr vilka förband och vapensystem som ger lämplig effekt. Vapen, och skyddssystem, som är anpassade för ett scenario är inte självklart lämpade för ett annat. Precisionsvapen med stor effekt mot ett befäst mål med liten utbredning är dyra och ineffektiva mot ett mindre skyddat mål utspritt över en större yta, medan yttäckande vapen avsedda för oskyddade mål har liten effekt mot befästa anläggningar. Vapen som är utformade för att användas i öppen terräng kan fungera sämre över skogbeklädda ytor. På ett glest slagfält med stora avstånd, t.ex. Nordkalotten, blir logistiken en viktig faktor. Vapensystem med möjlighet att skjuta flera olika typer av vapen/ammunition, t.ex. från drönare och robotar till artillerigranater, kan öka möjligheterna att med samma resurser verka på flera avstånd och mot olika mål.

I likhet med andra teknikområden sker inom vapenområdet en ökad systemintegration där många delar sätts samman till komplexa system med prestanda som vida överstiger tidigare generationers enklare system. För vissa system görs detta av leverantören, men i många fall omfattar systemet både personal och delsystem från flera leverantörer. Detta gör systemintegration i en vidare bemärkelse oundgänglig även för den organisation som ska utveckla, producera, förbandssätta eller använda systemet, som Försvarsmakten och andra försvarsaktörer såsom FMV. För att ett komplext högnivåsystem ska nå den prestanda som eftersträvas när delsystemen sätts samman måste dessa ofta anpassas. Det innebär att viss systemutveckling måste ske. Att anpassa färdiga system kan i många fall vara dyrare än att nyutveckla. Komplexa system på hög systemnivå och med höga prestanda är dyra att utveckla, och krav på tillförlitlighet, tillgänglighet och kommunikationsmöjligheter är ytterligare fördyrande och försvårande faktorer. Avancerade system medför ofta även högre krav på användarna med ökade utbildnings- och träningsbehov till följd. Kunskapen om och förmågan till systemintegration behöver öka i omfattning om utvecklingen inom enskilda områden ska kunna nyttiggöras.

## Tekniska trender

Högre precision, snabbare vapeninsats och längre räckvidd har alltid varit viktiga egenskaper vid utveckling av vapensystem. De senaste decenniernas teknikutveckling inom elektronik och datorer har gjort det möjligt att göra sensorer och datorer små, energieffektiva och samtidigt mer kraftfulla. Teknikutvecklingen under samma period har inte på motsvarande sätt underlättat att flyga fort och långt. För det har det hitintills krävts kvalificerad militär forskning och avancerade anläggningar.

### *Precision och manövrering*

Precisionsvapen var tidigare synonymt med robotar, vilka är relativt stora och dyra vapen avsedda för kvalificerade mål. Den allmänna teknikutvecklingen har i dag gjort det möjligt att även tillföra precisionsförmåga till mindre och relativt billiga system. Mindre, fjärrstyrda, drönare utrustade med stridsdelar används nu frekvent i kriget i Ukraina. Utvecklingen går mot en ökad automation och det som för robotvapen har kallats *fire and forget*, dvs. automatisk styrning mot utpekade mål, finns som prototyper även för de mindre drönarvapnen. I ett mer industriellt utförande finns från flera leverantörer så kallade patrullrobotar. De är system som utnyttjar flexibiliteten hos obemannade (FPV-)drönare och som används för att spana, söka efter mål och angripa mål med verkansdelar.

Precision innebär att träffa ett mål med den noggrannhet som eftersträvas. För att åstadkomma det krävs både förmåga till navigering, dvs. att systemet kan mäta sin egen position relativt målet, beräkna en bana mot en tänkt plats där verkan avses ske och göra målinmätning med en sensor, och förmåga att manövrera för att till slut träffa målet. Mot framtiden kan detta göras mer autonomt än med dagens i stort obemannade tillvägagångssätt.

Positionering kan göras på olika sätt. Satellitnavigering har möjliggjort helt nya tillämpningar men är, liksom all radiobaserad teknik, känslig mot störning och andra telekrigsåtgärder. Det pågår därför mycket forskning kring alternativa tekniker. Tröghetsnavigering påverkas inte av yttre störningar men det finns ännu inga sensorer med tillräcklig prestanda som är billiga och små nog. Utvecklingen av sensorer för målinmätning går framåt. Kvalificerade sensorer i radar- och infraröda våglängdsområdet är fortfarande relativt dyra medan enklare bildalstrande sensorer är billiga och små, till stor del tack vare civil teknikutveckling. Behov som drivs av militära tillämpningar resulterar emellertid inte nödvändigtvis i billiga produkter.

Mindre farkoster är relativt enkla att manövrera i låga hastigheter men för vapen som flyger i mycket höga, hypersoniska (dvs. över fem gånger ljudhastigheten), hastigheter är det tekniskt komplicerat att utforma system för att styra dem. Det är i många avseenden en forskningsfråga som kräver kunskap, avancerade anläggningar och möjligheter till prov.

Vad som är tillräcklig precision beror på målet och vilken typ av verkansdel som används. Ett exempel på en tillämpning som kräver mycket hög precision är luftvärnsrobotar som är avsedda att i hög hastighet träffa målet nos mot nos, en s.k. direktträff. Ett stridsfordon är ofta väl skyddat men det finns delar som är svåra att ge fullt skydd och stor effekt kan nås om dessa sårbara delar kan träffas. Detta kräver emellertid centimeterprecision. Att träffa en svag punkt i en befästning, som en lucka till en radarstation, kräver en träff inom någon meter och för att slå ut en känslig del i en grupperad ledningsplats med en artillerigranat eller motsvarande kan det räcka med en träff inom några meter från målet. Ett rörligt mål är mer komplicerat att träffa än ett fast mål och ställer högre krav på sensorer och ledningssystem för att kunna styra precist i slutfasen, men kravet på precision är detsamma.

Avancerade siktes- och avfyrningssystem som tidigare endast fanns på större plattformar, finns idag tillgängliga på soldatnivå. Automatkarbiner kan t.ex. utrustas med sikten där automatiserad bildbehandling hjälper skytten eller rentav styr avfyrningen för att förbättra träffsannolikheten.

I en nära framtid kan miniatyrisering av mekanik och elektronik möjliggöra små robotar och styrbara projektiler. Det finns idag exempel på styrbara artillerigranater, men lösningarna är baserade på satellitnavigering vilket kan göra dem sårbara i telekrigssituationer och dessutom mycket dyrare än traditionellt artilleri. Högre precision på längre avstånd, till låg kostnad, bedöms vara en viktig förmågehöjande egenskap hos artilleriet och därmed en sannolik utveckling, t.ex. raketartilleri med lång räckvidd och hög precision.

*Hastighet*

Hög hastighet ger både kort flygtid till målet, vilket är viktigt för tidskritiska mål, och kort tid för eventuella skyddssystem att motverka ett hot. Vad som är hög hastighet beror på situation och uppgift. För vissa tillämpningar kan vapensystem med hög underljudshastighet vara en utmaning för motmedelssystem medan det betraktas som låg hastighet i andra situationer. Teknik för att flyga i hög underljudshastighet är väl utvecklad, likaså för överljudshastighet även om det gör systemen dyrare.

Ett begrepp som förekommer ofta i den militärtekniska debatten är så kallade hypersoniska system, system som flyger i över fem gånger ljudhastigheten. Den militära effekten av att kunna använda hypersoniska system bedöms kunna vara mycket stor. Det är emellertid fortfarande svårt att utforma sådana om de ska kunna manövrera under sin färd. Redan de tyska V2-robotarna nådde hypersoniska hastigheter i delar av sin bana liksom interkontinentala ballistiska robotar, robotar som flyger i en, förutbestämd, ballistisk bana. Med hypersoniska vapen avses oftast system som kan manövrera under färd, framförallt i atmosfären. Det finns två huvudtyper av system, dels hypersoniska glidfarkoster som skjuts upp som en ballistisk robot och som sedan glidflyger i de övre atmosfärslagren, och kryssningsrobotar som flyger på höga höjder. Flera länder utvecklar nu hypersoniska vapensystem med

manöverförmåga. Dessa vapensystem kommer sannolikt att vara mycket svåra att bekämpa med dagens luftförsvarssystem. Detta på grund av att de kan flyga med hög hastighet på lägre höjder än interkontinentala robotar med en ballistisk bana (glidfarkosterna kan flyga på en höjd av 40–50 km istället för höjder på 100-tals kilometer), och därmed är svårare att upptäcka med markbaserade radarsystem. De kan även manövrera, vilket gör det svårt att förutse deras banor och planerade nedslagsplatser. Kina, Ryssland och USA har alla utvecklingsprogram för sådana system. Inom det europeiska försvarsforskningsprogrammet, EDF, utvecklas motmedelssystem mot sådana hot. Detta kräver omfattande utvecklingsinsatser både avseende luftvärnsrobotarna och för inmätning och ledningssystem. För att ha en kapacitet att detektera hot på långt håll kommer satellitbaserade sensorer att behövas, kombinerat med markbaserade system. För att utveckla hypersoniska system krävs också omfattande forsknings- och utvecklingsprojekt som ännu inte har tagit form inom EU, även om det finns initiativ som kan leda mot sådana, bl.a. ett franskt program.

*Lägesbild och ledning*

Övertag i räckvidd gentemot en motståndare är en uppenbar fördel. Direktriktad eld har en begränsning i räckvidd men med indirekt eld, antingen artilleri eller robotvapen, kan en motståndare angripas på långa avstånd. Detta kräver emellertid inmätning av målets position och överföring av den informationen till skjutande plattform. I över 100 år har flyget burit spaningssensorer men den mängd sensorer som förekommer i Ukraina, där båda sidor använder drönare i mycket stor omfattning, är omvälvande. Det har förändrat stridsfältet genom att göra det transparent. Drönarna bär sensorer som ständigt övervakar hela stridsområdet och de används också för vapenleveranser. Rörelse var tidigare ett skydd men med en ständig bevakning syns alla rörelser. Övervakningen gör att soldater eller fordon i rörelse upptäcks omedelbart och utsätts för bekämpning, antingen via klassisk indirekt eld eller med hjälp av drönarburna verkansdelar. Verkansdelarna som används är traditionella men de ingår i ett system som har drag av tidigare framtidsvisioner om ett nätverksbaserat försvar med övervakning, samverkande system och precisionsvapen.

*Räckvidd*

Beroende på vapensystem räknas räckvidd från meter till tusentals kilometer. Direktriktad eld kan nå ett mål på flera kilometers avstånd men kräver fri sikt till målet. Artilleri är begränsat till några tiotals kilometer men kan med raketdrift komma över 100 km.

För farkoster, robotar eller drönare, är den räckviddsbegränsande faktorn framförallt mängden drivmedel och större farkoster har längre räckvidd. Räckvidderna för de små drönarsystemen på stridsfältet i Ukraina kan räknas från enstaka till några

tiotal kilometer. Ryssland använder glidbomber (räckvidd ca 50–150[319] km), taktiska ballistiska robotar (räckvidder upp till omkring 500 km), drönare (enklare kryssningsrobotar, räckvidder upp till ett par tusen kilometer), traditionella kryssningsrobotar (räckvidd från 500 km och uppåt) och ett mindre antal medeldistansrobotar (räckvidder upp till några tusen kilometer). Ukraina har använt enklare system som också kan flyga långt men har efter några år även utvecklat flera långräckviddiga system. Långa räckvidder är inte en utmaning ur ett enskilt tekniskt utvecklingsperspektiv, men möjligtvis i kombination med höga hastigheter, precision och möjlighet till kommunikation med farkosten.

För att kunna nyttiggöra system med räckvidder på 100-tals kilometer krävs sensorsystem som kan mäta in målets position på sådana avstånd och ledningssystem som kan exekvera beslut inom relevanta tidsrymder. Satellitbaserade sensorsystem spelar en viktig roll redan idag men för tidskritiska mål kan det vara svårt att ha god sensortäckning på rätt plats. Förmågan till inmätning och ledningssystem som möjliggör korta beslutscykler kommer att vara en viktig del av framtida långräckviddiga bekämpningssystem. Dessa kommer också troligen att vara förhållandevis kostsamma vad avser utveckling och underhåll.

## Samverkande och förutsättande förmågor och tekniker

### Automation och samverkande system

Sedan mitten på 1990-talet har framförallt USA, och delvis även Ryssland, utvecklat förmågan att samverka med militära system. Genom att skapa en tillfällig men tät sammankoppling av vapen, sensorer och plattformar erhålls ett mycket kvalificerat bekämpningssystem. Begreppet ”system i samverkan” har hittills främst inbegripit luft- och sjöstridskrafter. För markstridskrafterna ses en motsvarande ökad integration av olika system. I kriget i Ukraina finns många exempel på hur system som obemannade flygplan, artilleri och stridsfordon integreras, för att tillsammans nå en högre stridseffekt än de skulle göra var och en för sig. Det ger också en robusthet och flexibilitet om olika skjutande system kan ersätta varandra.

Pansarvärnsvapens effektivitet har demonstrerats under kriget i Ukraina. En intensifierad utveckling av skyddssystem mot den typen av vapen är nu att vänta. Kvalificerade staters framtida stridsfordon och stridsvagnar kommer därför sannolikt att vara skyddade med avancerade system, som kan motstå många av de idag förekommande vapensystemen. En hög grundskyddsnivå gör också att sådana system blir mindre sårbara för olika splitterstridsdelar, som artillerigranater. Stridsvagnar kommer att bli ännu dyrare system men svåra att slå ut. Detta kommer att ställa nya krav på vapenutvecklingen.

319 Det finns rapporter om att räckvidden för glidbomber ökar och upp till 200 km har provats, https://kyivindependent.com/russias-new-long-range-glide-bombs-aim-to-terrorize-civilians-not-win-battles-experts-say/.

## Civil teknik, tillgänglighet och tekniskspridning

Den civila teknikutvecklingen skapar en ekonomisk asymmetri mellan hot och skydd. Civil teknikutveckling har lett till en bred spridning av teknik, som bara för ett par decennier sedan var förbehållen högteknologiska staters försvarsprogram. Fjärrstyrda eller helt autonoma farkoster, såsom exempelvis drönare, är numera konsumentprodukter. Även små jetmotorer finns på hobbymarknaden. Med relativt små medel kan därmed enklare typer av kryssningsrobotar byggas. Små fjärrstyrda flygfarkoster utgör i dag ett reellt hot i många sammanhang, såväl spanande som beväpnade. De används aktivt i flera pågående konflikter av såväl icke-statliga väpnade grupper som av båda parterna i kriget i Ukraina. Detta medför en breddad hotbild, eftersom brett tillgänglig teknik ger fler aktörer möjlighet att utveckla och bygga relativt avancerade vapen samtidigt som den förra generationens militära kvalificerade vapensystem finns alltmer tillgängliga.

De hot som kan förverkligas med modern civil teknik möter ofta inte de krav på tillförlitlighet eller robusthet som normalt ställs på militära system. Den civila teknikutvecklingen ger inte samma möjligheter för dem som vill utveckla försvarssystem, som den ger dem som vill utveckla hotsystem. Att bygga försvarssystem, som för att nå effekt behöver ha en hög tillförlitlighet, för att möta även enklare högteknologiska hot, innebär kostsam utveckling och systemintegration. Den civila teknikutvecklingen skapar därmed en asymmetri mellan hot och försvar. Ett exempel på detta är mindre obemannade flygfarkoster (*Unmanned Aerial Systems, UAS*) som kan bära både vapen och sensorer, men som är svåra att motverka på relevanta avstånd. Tekniken för motmedel mot sådana system (*Counter UAS)* ligger för närvarande efter i utvecklingen, något som kan ses i Ukraina. Det görs stora ansträngningar för att möta detta hot genom metod- och taktikutveckling samt med satsningar på teknisk utveckling av konventionellt luftvärn och laser- och mikrovågsvapen *(High Power Microwave, HPM)*. Det övertag de obemannade systemen verkar ha i dag bör vara utjämnat i framtiden.

Högteknologisk vapenutveckling kräver etablerad industri, forskning och en hög teknisk nivå. USA dominerar fortfarande vapenutvecklingen, men flera länder i Asien, med Kina i ledningen, har höga ambitioner och satsar stort på att utveckla forskning och industri. Förutom att höja det egna landets militärtekniska nivå, är de asiatiska staternas ambitioner sannolikt starkt marknadsdrivna. När ett fåtal länder med USA i spetsen ledde utvecklingen, var spridningen av sådana vapen möjlig att kontrollera. Nu har flera länder tillägnat sig förmågan att utveckla högteknologiska precisionsvapen, som därmed kan bli tillgängliga på en större marknad. Detta kan få säkerhetspolitiska konsekvenser och påverka maktbalanser. Turkiet har gjort stora ansträngningar och under de senaste 20 åren har landet kraftigt expanderat sin försvarsindustri vilken i dag är mångdubbelt större än vid millennieskiftet. Efter att i slutet av 00-talet ha misslyckats med att teckna avtal med USA om köp av de större obemannade flygsystemen MQ-1 Predator och MQ-9

Reaper, intensifierades den inhemska utvecklingen. Turkiets försvarsindustri är i många avseenden lika avancerad som Europas och USA:s, och landet är i dag en stor leverantör av det obemannade flygsystemet Bayraktar TB2. Detta system fick stor uppmärksamhet i konflikten i Nagorno-Karabach och har använts framgångsrikt av Ukraina i kriget mot Ryssland. Kina har i dag en teknikнivå som inte är långt efter de stora västerländska staternas och utbildar nu fler ingenjörer än USA, Ryssland och EU tillsammans. På ett teknikområde har västländerna fortfarande ett försprång, nämligen avancerade jetmotorer.

### Robust, billig och uthållig materielförsörjning

Kriget i Ukraina har pågått sedan 2014 och med intensiva strider sedan februari 2022. Ammunitionsförbrukningen i ett långvarigt och intensivt krig är mycket hög och det finns ett stort behov av att producera ny ammunition i den takt den förbrukas. Det ställer krav på infrastruktur, kontinuerlig produktion och transportmöjligheter till de stridande förbanden. Likaså visar förlusterna hos båda sidorna i kriget att soldater, vapen och fordon också måste ersättas i stor omfattning. Huruvida försvarsindustrierna i väst har möjligheter att skala upp produktionen av kvalificerade vapen-, flyg- och fordonssystem är inte uppenbart.

Den traditionella vapenindustrin karakteriseras inte av automatiserade produktionslinor utan snarare av korta serier, mycket manuellt arbete och skickliga montörer. Ukraina har lyckats att höja produktionsförmågan av små drönare och har nu en ganska signifikant produktion (över 4 miljoner förväntade enheter 2025) men det är inte en enhetlig kvalitetskontrollerad industri utan distribuerad och med produkter av varierande kvalitet och egenskaper. En del av dessa drönare blir vapen men tillverkningen av verkansdelarna till dessa är svår att skala upp. Användningen var inledningsvis till stor del improviserad, med stora personella risker som följd. Hög kvalitet och tillförlitlighet är vanligtvis förenat med höga kostnader. Huruvida lägre tillförlitlighet fast till mycket lägre kostnad respektive mycket större antal är något som måste accepteras eller om det är möjligt att skapa en högkvalitativ produktion som ger hög tillförlitlighet utan kostnadsökningar är en central fråga som behöver drivas av köparna av vapensystem och plattformar, dvs. stater.

Civil utveckling kan leda till både billigare och dyrare vapen. Civilt driven teknikutveckling (miniatyrisering, kraftelektronik, materialteknik m.m.) gör tekniska systemlösningar, som tidigare var dyra, lätt tillgängliga och billiga (t.ex. drönarutveckling i form av enkla precisionsvapen). Vapenteknologi har av flera skäl, såsom begränsande regelverk och behov av specialistkompetens, varit ett område med få aktörer. Med civilt tillgänglig teknik, stor efterfrågan och medföljande finansiella resurser och allmän kompetensspridning kan nya aktörer ta plats och erbjuda exempelvis precisionsvapen. Det finns exempel på företag som har sitt ursprung i IT-branschen, för att sedan börja utveckla små drönare och som nu också har robotar

i produktportföljen. Mjukvaruföretag har erfarenhet av komplex systemutveckling och är kanske de som kommer att vara ledande aktörer i framtidens försvarsindustri.

Förändringar i civil industri kan också leda till att vapen blir dyrare att tillverka. Olika kritiska komponenter som hittills har kunnat produceras i, eller som råvaruförsörjts från, en civil industribas riskerar att i framtiden inte finnas tillgängliga. Exempelvis begränsas möjligheten till produktion av vissa kemiska substanser av den europeiska REACH-förordningen och det finns även andra ämnen som bly som har en begränsad civil användning.

### Standarder, modularitet och systemintegration

En framtida inriktning som förespråkas av såväl industrier som användare (stater) är avancerade system av system, dvs. sammanfogade system som ger en överlägsen effekt jämfört med de enskilda systemen. Det kräver integration av flera olika system, något som är komplicerat och arbetskrävande. Om system från olika tillverkare ska integreras i ett system behöver det finnas tydliga gränssnitt och förhandlingar avseende kontrakt mellan leverantörer krävs. Ett sätt att hantera detta är att utforma standarder för systemens gränssnitt och som köpare ställa krav på att systemen ska uppfylla dessa. Genom att skapa modulära system av system kan delsystem bytas ut eller uppgraderas. Det finns exempel på sådana standarder i dag där industrier och stater gemensamt utvecklar dem för att möjliggöra flexibilitet och en anpassningsbar systemarkitektur. Modularitetsprincipen återfinns även på lägre systemnivåer, som modularitet i vapen och verkansdelar. Standarder behövs för alltifrån informationsutbyte till gränsytor för infästningar för raketer och robotar på plattformar.

## Aktörer

Utveckling av komplexa system tar tid. Med stora satsningar kan utvecklingstiden kortas men komplexa system är svåra att utveckla snabbt. Under ett krig pågår en implementering och användning av teknik med hög omsättningstakt. I Ukraina tillämpas existerande teknik i nya former men det syns inte några effekter på produktion och utveckling av kvalificerade vapensystem. Vilken militär teknik som kommer utvecklas beror på vilka politiska beslut som fattas. De politiska besluten kommer antagligen att se olika ut i olika politiska sfärer.

För de flesta aktörer kommer det ökade lufthotet sannolikt att leda till stora ansträngningar för att stärka luftförsvaret, från de minsta plattformarna och objekten som behöver aktiva skyddssystem till yttäckande skydd av städer. Eftersom det i dag råder en asymmetri mellan hot och skyddssystem så kan en möjlig utveckling vara att produktionen av bl.a. luftmålsrobotar effektiviseras. Robotarna till det israeliska systemet *Iron Dome* är förhållandevis billiga och produceras i helautomatiska anläggningar.

På motsvarande sätt är det rimligt att förvänta sig en utveckling mot billiga kryssningsrobotar och artilleri med hög precision och lång räckvidd.

Natos förmåga att planera och genomföra extremt komplexa, samordnade anfall bygger till stor del på USA:s militära förmågor. De europeiska staterna kan komma till slutsatsen att den förmågan behöver finnas även i en rent europeisk kontext. Behovet av möjligheten till avancerad strid med samverkande system är stort och kräver utveckling av tekniska system som ännu främst finns som koncept och visioner. Såväl utvecklingen av tekniken som av taktik och metoder för användning kommer att kräva samordnade satsningar med långsiktiga åtaganden från flera stater.

Försvarsindustrin verkar på en reglerad marknad med exportkontroll, få kunder och få aktörer. För några typer av enklare produkter finns en viss konkurrens om kunder men för avancerade system så är stater, ensamma eller i grupp, de enda köparna på en marknad som har en eller ett par leverantörer. Upphandling är en komplicerad process där tillgången till kompetens inom de olika högteknologiska områdena är begränsad vilket gör processen för kravställning och prestandakontroll till en utmaning för många stater.

## Lästips

Magnus Evestedt, Ulrik Edh, Intercepting Hypersonic Glide Vehicles, 2024-11-08, FOI-D--1345--SE.

Anton Åkesson, Magnus Evestedt, Samverkande robotar – Omvärldsbevakning, 2025-09-22, FOI Memo 8955.

Magnus Evestedt, Boban Pavlovic, Styrda vapen – Omvärldsbevakning, 2023-12-11, FOI-R--5517--SE.

Christopher Weidacher Hsiung, Cecilia During, Oscar Almén, Ivar Ekman, Peter Stenumgaard och Annica Waleij (eds.), Strategic Outlook 10: China as a Global Power, FOI-R--5620--SE, juni 2024.

Jack Watling, The Arms of the Future: Technology and Close Combat in the Twenty-First Century, 2023-09-07, Bloomsbury Publishing.

# Kärnvapen

*Mattias Waldenvik*

## Inledande beskrivning

Med ett kärnvapen avser vi i detta kapitel ett vapen med en verkansdel som är en kärnladdning.

I all väsentlighet fungerar kärnvapen som vilken stridsdel som helst. Det är särskilt tydligt för vapenbärare med dubbla användningsområden, det vill säga vapensystem som kan skjuta både konventionella stridsdelar och kärnvapen. När vapenbäraren väl har bestyckats med kärnvapen så fungerar den i grova drag på samma sätt som en konventionellt bestyckad. Detsamma gäller operationer med kärnvapen. Detta innebär exempelvis att om strategiskt bombflyg ska genomföra ett kärnvapenanfall, kommer det att behöva kompletteras på samma sätt som ett konventionellt anfall, med avseende på resurser som lufttankning, jaktskydd, förbekämpning av luftförsvar och så vidare.

Den militära nyttan av kärnvapen kommer framför allt från den ögonblickliga och mycket stora energiutvecklingen per massenhet. Ett exempel är att en enstaka fullt bestyckad tung rysk interkontinental ballistisk robot kan medföra stridsspetsar som tillsammans har en större sprängstyrka än de allierades bombningar under hela andra världskriget, 1939–1945.

Enligt Icke-spridningsavtalet (NPT) finns det fem kärnvapenstater som har rätt att inneha kärnvapen. Det är USA, Storbritannien, Frankrike, Kina och Ryssland. Utanför avtalet står Indien, Pakistan, Israel och Nordkorea. Vi skiljer på de två grupperna genom att referera till dem som *de jure* respektive *de facto* kärnvapenstater.

Energin i en detonerande kärnladdning kommer från kärnreaktioner i en så kallad kedjereaktion där det utvecklas oerhört höga energinivåer under mycket korta tider. En enstaka kärnreaktion är i allmänhet flera storleksordningar mer energetisk än en enstaka kemisk reaktion. Den höga energimängden gör att ett kärnvapen skiljer sig i verkansform från vapen baserade på konventionellt explosivämne. Fram till och med bråkdelar av en sekund efter explosionen är kärnvapnet väsentligen en mycket stark röntgenkälla. I atmosfären absorberas röntgenstrålningen i luften och omvandlas till en luftstötvåg. Kärnvapnets höga temperatur ger upphov till värmestrålning som kan orsaka brännskador och bränder på stora avstånd från explosionspunkten och kärnreaktionerna ger upphov till den gamma- och neutronstrålning som går under namnet initialstrålning. De olika verkansformerna har skalningslagar, dvs. förhållanden mellan varandra, som beror på laddningsstyrka. Detta innebär att ett mindre kärnvapen med en sprängstyrka på enstaka kiloton har initialstrålning som den starkaste verkansformen medan värmestrålningen dominerar för större laddningsstyrkor. Ett vapen avsett att användas mot ett mål där initialstrålningen

är den dimensionerande verkansformen kommer därför i allmänhet ha en lägre laddningsstyrka än till exempel ett kärnvapen avsett för att slå ut oskyddad trupp över en större yta. Således torde ett land vid ett eventuellt nyttjande välja det kärnvapen och den storlek som ger önskad verkan och nytta.

Källan till ett eventuellt radioaktivt nedfall, den så kallade kvarvarande strålningen, är de klyvningsprodukter som genereras av kärnklyvningen. Om explosionen sker en bit ovanför markytan kommer klyvningsprodukterna följa med svampmolnet upp i de högre delarna av atmosfären där de över tiden sprids ut över åtminstone det aktuella halvklotet. Om detonationen i stället sker på så låg höjd att partiklar från marken kommer i kontakt med klyvningsprodukterna kommer de ge upphov till ett nedfall runt explosionspunkten och över tid i vindriktningen, där partiklarna följer med vinden och så småningom faller till marken.

## Kärnvapen som strategiskt instrument

Ett centralt begrepp avseende kärnvapen är avskräckning, ett begrepp som kan vara svårt att exakt definiera men som de flesta nog påstår sig kunna känna igen när de väl ser det.

Ett sätt att se på kärnvapen och avskräckning är den militärstrategiska relevansen. Det är den hänsyn som militärstrategiskt behöver tas till de förmågor som motståndarens beslutsfattare har tillgång till. Det omfattar inte bara kärnvapnen i sig utan även hur de har operationaliserats, och hur relevanta förband övas. Det vill säga trovärdigheten i kärnvapenförmågan, och konsekvenser av denna: har aktören de facto förmåga att genomföra kärnvapenoperationer där allt som saknas är ett beslut för att de ska kunna genomföras i det närmaste omedelbart?

Det som framförallt synliggörs och kommuniceras strategiskt är kärnvapnet som verktyg för olika slag av politiska påtryckningar. Rädslan för kärnvapen, baserad på okunskap eller faktiska omständigheter, utnyttjas för att påverka politiskt beslutsfattande direkt eller indirekt. Det senare till exempel genom att försöka påverka folkopinionen. Kärnvapnens nyttjande som påverkansinstrument bör konceptuellt hållas isär från avskräckningen som den beskrivs ovan, det vill säga förmågan att verkligen kunna använda kärnvapen. Likaså ska inte kärnvapen och dess effekter blandas samman med attack mot kärnkraftsindustri eller smutsiga bomber.

Kärnvapen är specifikt utvecklade och den tekniska utvecklingen hänger ihop med den doktrinära utvecklingen. Kärnvapendoktriner beskriver vad en part vill åstadkomma med sina kärnvapenstyrkor och under vilka omständigheter det ska ske. Kärnvapendoktrinen är trovärdig när den faktiska förmågan till att genomföra operationer motsvarar beskrivningen i doktrinen.

Under det Kalla kriget rådde en global kärnvapenavskräckning. Den doktrinära utvecklingen har efter det kalla krigets slut, med Ryssland som exempel, i mycket grova drag inneburit att den globala avskräckningen kompletterats med regional

avskräckning. Det har utvecklats medel och metoder för att kringgå ett framtida dimensionerande västligt robotförsvar. I skenet av detta är det inte konstigt att utvecklingen i huvudsak sker, och har skett, inom områdena vapenbärare och plattformar. Ett ryskt exempel på detta är kärnvapenbestyckning av den aeroballistiska[320] roboten Kinzjal.

Teknikutvecklingen i Ryssland de senaste decennierna kan alltså sägas vara driven av utveckling dels av den regionala avskräckningen, dels för att säkerställa att den globala avskräckningen fortsätter att vara trovärdig i skenet av ett av motståndaren utvecklat robotförsvar.

I skenet av det pågående kriget i Ukraina går det att argumentera för att den regionala avskräckningen fungerat i den mån att ingen tredje part har blandat sig i stridigheterna. Därutöver har det stöd som har givits till Ukraina till stora delar varit förknippat med restriktioner som sannolikt syftar till att begränsa konfliktens omfattning, om inte annat så geografiskt. Däremot har kärnvapen ännu inte spelat någon roll i de faktiska striderna.

Den 19 november 2024 publicerade Ryssland på Kremls hemsida en uppdaterad doktrin, "Grunderna för den Ryska federationens politik inom området kärnvapenavskräckning".[321] Vad denna innebär återstår att se. Det gäller både avseende utvecklingen av faktiska förmågor samt en därmed förändrad avskräckning, och genom prismat politiska påtryckningar.

## Trender och exempel

### Utvecklingen av kärnladdningar

Kärnladdningen är en del av det större kärnvapnet och områden som på sikt kan förändras är laddningens sprängstyrka, behov av provsprängning, fissionsfri fusion och en typ av vapen med en konstruktion som skulle kunna förenkla förvaring och logistik vid eventuell användning. Den grundläggande konstruktionen för kärnladdningar är begränsad av fysikens lagar. Banbrytande i sammanhanget skulle vara fissionsfri fusion, det vill säga fusionsvapen som inte behöver en fissionsladdning för att initiera fusionsreaktionerna. Möjligheten att använda kärnisomerer för att åstadkomma detta har diskuterats i litteraturen, se referenslistan i slutet av kapitlet, men bedöms idag inte vara en framkomlig väg.

Dagens utveckling av nya kärnladdningar är baserad på konstruktioner som har provats i fullskaliga kärnvapenprov. Men, behovet av provsprängning och utveckling av kärnladdningar kan förändras framgent. Med tillgång till provsprängningsdata, en mer komplett kännedom om materialegenskaper vid höga tryck och temperaturer

320 En aeroballistisk robot är en ballistisk robot som avfyras från ett flygplan. I det här fallet kan Kinzjal ses som en Iskanderrobot som avfyras från en MiG-31.

321 Presidentukas 991, Ryska federationen den 24 november 2024.

samt erforderliga beräkningsmodeller, kan det bli möjligt att utveckla nya konstruktioner utan att provspränga. En annan möjlig utveckling är att behovet av en ny konstruktion, och resultat från modellering och simulering, föranleder att provsprängningar återupptas.

Kärnladdningar finns i olika storlekar. Det stora utrymmet för utveckling av nya konstruktioner omfattar troligen kärnladdningar med relativt små sprängstyrkor, eller med befintliga laddningsstyrkor men med ett mer effektivt utnyttjande av det fissila materialet. Med små laddningsstyrkor avses här sprängstyrkor av storleken motsvarande tiotals ton konventionellt explosivämne. Denna utveckling kan leda till nya tillämpningar

Antagandet om lägre laddningsstyrkor är baserat på följande resonemang. Det förefaller vara så att, givet tillgång på relevanta material, lämpliga isotoper av uran och plutonium, men utan fullständig förståelse för detaljerna i explosionsförloppets tidsutveckling, så blir laddningsstyrkan för kärnladdningen av ungefär samma storleksordning som de kärnvapen som användes mot Japan under det andra världskrigets slutskede, det vill säga något eller några tiotals kiloton. För att göra laddningsstyrkan mindre krävs en mer detaljerad förståelse för detonationsförloppet. Dylika kunskaper har traditionellt erhållits genom kärnvapenprov och annan experimentell verksamhet, men skulle möjligen kunna erhållas genom datorsimuleringar, givet god kännedom om de ingående materialens egenskaper under höga tryck och temperaturer. Sammanfattningsvis är resonemanget baserat på iakttagelsen att det är tekniskt mer komplicerat att på ett förutsägbart sätt åstadkomma små laddningsstyrkor. Samtidigt finns det stridsekonomiska fördelar om till exempel en flygbomb på 250 kilo skulle ha en sprängverkan motsvarande tio ton.

En annan väg för utvecklingen är laddningar som förenklar logistiken. I det fall kärnladdningen är avsedd att utgöra verkansdelen i ett vapensystem med dubbla användningsområden, för såväl konventionella operationer som kärnvapenanvändning, behövs ett logistiksystem som kan para ihop verkansdel med vapenbärare under fältmässiga förhållanden. Laddningskonstruktioner som förenklar det förfarandet, till exempel genom en förenklad hantering, skulle kunna medföra en förmågehöjning som inte har med den egentliga vapenprestandan att göra. Särskilt i skenet av de speciella kontrollbehov som krävs mot oavsiktlig användning av kärnvapen och för säkerställandet av avsiktlig användning.

### Utvecklingen av nya kärnvapen

Med utvecklingen av nya kärnvapen avses här utvecklingen av hela vapensystem. Vi kan från avsnittet ovan konstatera att den utvecklingen i huvudsak avser utvecklingen av andra komponenter än själva kärnladdningen, framför allt vapenbärare.

Det är ett rimligt antagande att det vid framtagningen av en ny typ av kärnvapen finns en tänkt uppgift och ett tänkt mål som dimensionerar kravställningen på hela

systemet. Detta gäller avseende till exempel användbarhet, räckvidd, precision och laddningsstyrka. Det är systemet sammantaget som skall leva upp till kravställningen.

Vikten av vapenbärare och plattformar – hela vapensystemet – illustreras väl av hur antalet kärnvapenstridsspetsar hanterades i Startavtalet. Eftersom det av olika skäl betraktades som omöjligt att komma fram till en tillförlitlig rustningskontroll, med tillhörande verifikationsregim, för de faktiska kärnladdningarna fokuserade man istället på (kärn)vapenbärare och plattformar. Ett exempel på hur detta gestaltade sig är att tillvägagångssättet för att minska arsenalen med tio stridsspetsar var att, i ett förfarande verifierat av motparten, förstöra en vapenbärare avsedd att bära tio stridsspetsar och den för (kärn)vapenbäraren avsedda plattformen, till exempel en silo. De tio stridsspetsarnas, dvs. kärnvapnens, vidare öde, oavsett om det var faktiska stridsspetsar eller det nominella antal som motsvarade vapenbärarens prestanda, spelade i sammanhanget ingen roll.

Utvecklingen idag med vapenbärare som manövrerar, är hypersoniska eller rent av drivna av en kärnreaktor, pekar på den uppenbara vikten av att kärnladdningen tar sig till det tänkta målet. Utvecklingen av kärnladdningar är i det sammanhanget av sekundär betydelse.

En viktig parameter avseende utvecklingen av nya kärnvapen är den industriella infrastrukturen för tillverkning och hur den är tänkt att fungera. Här råder det stora skillnader mellan USA och Ryssland, med Kina bedömt någonstans däremellan men med viss osäkerhet i bedömningen. Mot bakgrund av ett rådande *de facto* provstopp förefaller de olika parterna ha valt olika strategier för att vidmakthålla sina befintliga arsenaler. I grova drag har Ryssland satsat på att behålla sin infrastruktur för tillverkning av komponenter i uran och plutonium medan USA har valt att istället underhålla befintliga komponenter förvarade i lager eller i den aktiva arsenalen. Antingen ser man till att veteranbilen är i gott skick genom att byta ut delar utsatta för åldring och slitage, eller så bygger man med jämna mellanrum en ny bil efter i det närmaste samma ritning, för att försöka sig på en liknelse.

Båda strategierna förefaller fungera för vidmakthållande av arsenalerna, men de skiljer sig åt vad gäller potentialen för tillverkning av nya konstruktioner i större skala för en möjlig expansion av antalet kärnstridsspetsar eller för tillverkning av nya konstruktioner. Här befinner sig USA i en process av återtagande av produktion av komponenter av framför allt plutonium.

Kina är svårbedömt bland annat eftersom utvecklingen i landet är allt annat än transparent. Av allt att döma är dock Kinas arsenal under utveckling och kommer sannolikt påverka utvecklingen av nya kärnvapen under perioden fram till 2050.

## Särskilda delområden

### Kärnreaktioner och kärnfysik

Kärnreaktionerna delas in i två grupper, fission och fusion. I fissionsreaktioner, eller kärnklyvning, delas en tung kärna i ett fåtal lättare kärnor – så kallade klyvningsprodukter. En fusionsreaktion är istället en sammanslagning av lätta kärnor.

Den största återhållande faktorn för anskaffning av kärnvapen är tillgång till och bearbetning av råvarorna uran och plutonium.

De fysikaliska förloppen för kärnreaktioner är väl utforskade i den mening att det med stor sannolikhet saknas alternativa, mer lättillgängliga, material än de som används idag som skulle förenkla tillverkningen.

I en kärnladdning baserad på fission sker kärnklyvningen genom att en neutron träffar en atomkärna, som därmed klyvs till lättare kärnor och ett antal neutroner. De senare kan sedan i sin tur klyva flera kärnor och så vidare. Den således beskrivna kedjereaktionen kan bara ske under förutsättning att kärnorna är fissila, vilket i praktiken begränsar urvalet till en isotop[322] av uran, nämligen uran-235 och en isotop av plutonium, närmare bestämt plutonium-239. Även i en kärnreaktor kommer energiutvecklingen från kärnklyvningar som genomgår en kedjereaktion. Skillnaden är dock, att upprätthållandet av en kedjereaktion i en kärnreaktor måste utnyttja neutroner från processer som sker på en tidsskala som är väsentligt långsammare än explosionsförloppet i en kärnladdning.

Fusionsreaktioner kan bara ske om de kärnor som skall slås samman har tillräckligt hög relativ hastighet för att de elektriskt repellerande kärnorna skall komma tillräckligt nära varandra för att den starka kärnkraften[323] skall verka till sammanslagningen. För att åstadkomma höga relativa hastigheter hos partiklarna i makroskopiska mängder material krävs mycket höga temperaturer. Det finns i dagsläget endast en känd metod för att åstadkomma detta i ett vapen och det är att tillföra den erforderliga mängden energi med hjälp av en fissionsladdning. Därmed faller även fusionsladdningen under kravet på industriell framställning av de fissila materialen.

I praktiken finns det en rad ingenjörsmässiga problem som behöver bemästras för en aktör som vill tillverka kärnvapen. Ett signifikant problem är att materialegenskaperna för uran-235 och plutonium-239 under de höga temperaturer och tryck som de utsätts för under explosionsförloppet är komplicerade och teoretiskt

322 En atomkärna består av protoner och neutroner. Vilket grundämne som kärnan tillhör motsvaras av antalet protoner. Kärnor av samma grundämne, till exempel uran med 92 protoner, men med olika antal neutroner kallas för *isotoper*. Kemiskt sett är isotoperna snart sagt identiska men dess kärnreaktioner kan skilja sig radikalt. Ett givet grundämne har i normalfallet både stabila och radioaktiva isotoper.

323 Den starka kärnkraften, även kallad stark växelverkan, är en av fyra fundamentala krafter inom fysiken och är den kraft som håller samman en atomkärna. Kraften verkar endast på mycket korta avstånd.

svårtillgängliga. Det är författarens uppfattning att mycket av den forskning och utveckling som genomförs idag, i länder med kärnvapen, går ut på att få bättre modeller för dessa material, modeller som möjliggör att datorsimuleringar i allt högre grad kan användas för att vid behov utveckla nya designer av kärnladdningar. Bedömningen är att idag sker utvecklingen av nya kärnladdningar i huvudsak baserad på komponenter med egenskaper kända från tidigare provsprängningar. Det eventuella behovet av att genomföra provsprängningar diskuteras nedan.

### Provsprängningar

Avtalet CTBT, som förbjuder provsprängningar av kärnvapen, träder i kraft först när ett antal nyckelstater både har skrivit under och ratificerat avtalet. Poängen med detta är att ett avtal inte skulle bli stabilt om inte alla nyckelaktörer så att säga är med på båten. På grund av att den till avtalet hörande verifikationsregimen trots det har byggts upp under flera decennier kan avtalet dock sägas fungera ändå, men på en rättsligt svagare grund.

Relativt nytillkomna stater med kärnvapen, har sannolikt ett större behov av att provspränga för att verifiera att deras kärnladdningar fungerar som det är tänkt under olika omständigheter. Avtalet CTBT hämmar förmodligen den tekniska utvecklingen av kärnladdningar för aktörer som vill eller nyss har utvecklat kärnvapen. USA och Ryssland har å andra sidan genomfört ett stort antal provsprängningar och kan utnyttja dessa erfarenheter för att vidmakthålla sina arsenaler. Själva vidmakthållandet skiljer sig dock avseende produktionskapacitet. I skenet av detta kan CTBT ses som ett avtal som är tänkt att inte bara förhindra spridning av kärnvapen till nya aktörer utan även försvåra för *de facto* och *de jure* kärnvapenstater att utveckla sina befintliga arsenaler.

I korta drag är det författarens bedömning att Ryssland vidmakthåller sin arsenal genom att tillverka nya komponenter baserade på en konstruktion som en gång i tiden genomgått fullskaligt kärnvapenprov. Komponenterna används sedan, tillsammans med befintliga data från proven, för att till viss del utveckla nya kärnladdningar.

USA å andra sidan, har inte haft kapacitet att tillverka komponenter i uran eller plutonium, utöver enstaka exemplar. Här har man istället satsat på vetenskapligt baserade metoder för att säkerställa att befintliga komponenter fortfarande kommer att prestera så som de en gång i tiden gjorde i ett eller flera kärnvapenprov. Utvecklingen av ökad kapacitet för tillverkning är dock under utveckling i USA.

Kina är även här problematiskt att bedöma. I jämförelse med USA och Ryssland har Kina genomfört avsevärt färre kärnvapenprov och borde därmed rimligen sakna den databas av erfarenheter som vi antagit att USA och Ryssland lutar sig mot för att vidmakthålla och till viss del utveckla sina arsenaler. Behovet att provspränga borde med andra ord vara relativt stort för Kina, särskilt mot bakgrund av bilden att de faktiskt expanderar sin arsenal inte bara i numerär utan även vad

gäller förmågor. Till exempel kan utvecklingen av robotar som bär flera stridsspetsar som var och en kan styras mot olika mål, antas vara beroende av förmågan att bygga kärnladdningar av relativt liten storlek, något som förutsätter kunskaper om explosionsförloppet.

Diskussionen om kärnvapenprov begränsas i detta kapitel till kärnvapenprov som genomförs av vad vi kan kalla ingenjörsmässiga behov. Kärnvapensprängningar med andra syften, som till exempel politiska markeringar, tas inte upp.

## Samverkande och förutsättande förmågor och tekniker

Som nämnts ovan är de drivande faktorerna för teknikutvecklingen inom området grundade i problemet med att vapenbäraren skall nå målet med tillräcklig precision, givet alla till buds stående motmedel. Det som i slutändan driver denna utveckling är kravet att under alla omständigheter kunna avskräcka motståndaren genom förmågan att potentiellt kunna tillfoga motståndaren en för motståndaren oacceptabel skada. Vid fjärrbekämpning är förstås kärnvapen underkastade samma problem som konventionella vapen med att upptäcka och identifiera mål och sedan bekämpa dessa innan de till exempel har omgrupperat till en annan plats eller försvunnit ut ur vapensystemets porté.

Räckvidd är en faktor av stor vikt. Man kan analysera konsekvensen av räckvidd på olika sätt. En grundläggande fråga för oss i Sverige är till exempel under vilka omständigheter ett vapensystem kan användas mot vårt land. En annan aspekt, som kanske har mer att göra med hur ett vapensystem skulle kunna användas mot Sverige, har att göra med var i motståndarens organisation som ett givet vapensystem finns och på vilken nivå insatsplaneringen görs. Ett exempel på detta är en sjömålsrobot, där fartygschefen, först efter bemyndigande att använda kärnvapen, använder roboten när det finns ett mål i sikte, varför roboten i fråga framför allt är ett hot mot svenska fartyg involverade i någon form av sjöstrid.

Förmåga att penetrera motmedel, framför allt i formen av robotförsvar i olika former, bedöms vara en starkt drivande faktor för utvecklingen av både vapenbärare och olika former av telekrigssystem.

Det kanske mest extrema uttrycket för denna trend är den utveckling av en kryssningsrobot respektive en torped med nukleär framdrift som sker i Ryssland. Den nukleära framdriften medför att så fort reaktorn har startat utgör vapenbäraren, utöver allt annat, en transport av radioaktivt avfall. Även provverksamhet med sådana plattformar är i någon mån skarpa eftersom en reaktor med utbränt radioaktivt bränsle behöver hanteras vid varje tillfälle. Den nukleära framdriften ger åtminstone i teorin en i det närmaste oändlig räckvidd. Det är inte själva energikällan utan hela systemets tålighet mot mekanisk, termisk och radioaktiv påverkan som är gränssättande. De system som idag är under utveckling har en strategisk

karaktär men när, och om, tekniken bemästras i praktiken skulle det kunna finnas en frestelse att använda den i andra sammanhang.

Om det mål man vill bekämpa skall bekämpas med stötvågsverkan finns det för varje laddningsstyrka en optimal höjd för detonationen. Vid planeringen av en insats behöver man därför ta hänsyn till felmarginalerna både i uppskattningen av höjden för detonationen och för kärnladdningens laddningsstyrka. Osäkerheten i laddningsstyrkan kan bero dels på felmarginalerna vid mätningar på provsprängningar, dels på den faktiska konstruktionen. Det senare gäller särskilt om kärnladdningen är konstruerad från komponenter som inte har provats tillsammans. Förbättringar i vapenbärarens stödsystem, precisionen i alla dimensioner, kan alltså leda till ett mer effektivt vapen för den vapenverkan man vill uppnå i målet. Stridsdelar som är markpenetrerande är ett annat exempel på vapenbärare som kan förbättra ett kärnvapens förmåga till verkan i målet.

Förmågan att upptäcka rörliga mål, planera en insats, fatta ett beslut och sedan genomföra insatsen innan målet har flyttat sig ur sikte är en förmåga som i allra högsta grad påverkar kärnvapenområdet, och den tidigare nämnda logistiken gör det inte mindre komplicerat. Ökad förmåga för insatser mot rörliga mål med kärnvapen är något som definitivt påverkar mängden värdiga[324] mål för bekämpning med kärnvapen. Därmed påverkas den militära förmågan vilket diskuteras vidare i nästa avsnitt.

## Påverkan på militär förmåga

Områdets påverkan på militär förmåga kan komma att förändras radikalt de närmaste decennierna. Som förhoppningsvis redan framgått av texten så beror det varken på att området i sig eller utvecklingen av kärnladdningar kommer att förändras radikalt. Snarare kan synsätt på reglering och konventionella vapens utveckling påverka området. En aspekt som kan komma att påverka militär förmåga är om Ickespridningsavtalet (NPT) faller samman och de stater som har förmågan finner att egna kärnvapen är en förutsättning för den egna säkerheten.

Så vitt det är allmänt känt är idag interkontinentala strategiska robotar baserade till lands och till sjöss bestyckade med kärnladdningar. Övriga kärnvapen är förvarade i förråd och hanteras och bevakas i särskild ordning. Förfarandet behöver vara sådant att kärnvapen under inga omständigheter förloras eller bringas att detonera utan auktorisering. Vidare behöver kärnvapnen göras tillgängliga för skjutande förband när väl auktorisering föreligger.

Militär förmåga kan i allra högsta grad påverkas av utvecklingen av nya vapenbärare. Ett aktuellt exempel är den ryska medeldistansroboten Oresjnik som provsköts

324 Med värdiga mål avses här mål där användandet av kärnvapen möjliggör eller avsevärt förenklar bekämpningen under de omständigheter som råder vid tillfället för insatsen.

med konventionella stridsspetsar mot mål i Ukraina 2024. Robotkomplexet är troligen en variant mycket snarlik robotkomplexet Rubezj vars utvecklingsprojekt möjligen var slutfört när projektet av någon anledning lades på is någon gång runt 2017. Skillnaden mellan den ringa uppmärksamhet som Rubezj rönte för mindre än tio år sedan, och den uppmärksamhet Oresjnik fått fram till idag är slående och illustrerar väl att den tekniska förmågan, där Oresjnik och Rubezj förefaller snarlika, eller rent av identiska, kan uppfattas på väldigt olika sätt beroende på den egna uppfattningen om världsläget, och synsätt på användning av kärnvapen.

Utöver vapenbärare kan den militära förmågan inom kärnvapenområdet komma att förändras av andra faktorer, som liksom området vapenbärare också påverkar konventionella vapen. Dit hör ledningssystem, insatsplanering och logistik. Dessa områden är särskilt komplicerade inom kärnvapenområdet så länge det finns en önskan från den politiska ledningen om att den skall kontrollera kärnvapnens användning och att de därför är konstruerade för att förhindra icke-auktoriserad användning och säkerställa att de kommer till användning endast när beslut om detta föreligger.

Den gängse uppfattningen idag är att ryska icke-strategiska kärnvapen förvaras i förråd underställda det 12:e huvuddirektoratet vid försvarsministeriet (12 GUMO). Innan de kan användas av fartyg, flygplan eller markrobotförband, de skjutande förbanden, behöver en logistisk fas genomföras. Särskilt komplicerat förefaller hanteringen vara för fartyg som behöver angöra en kaj i anslutning till en kran som kan lyfta ombord robotar eller andra vapenbärare bestyckade med kärnvapen. All utveckling som förenklar denna hantering, eller åtminstone förkortar den tid det tar, kommer att ha en påverkan på militär förmåga. Det är också värt att notera att vapenbärare och plattformar som kan bära både kärnvapen och konventionella vapen tas i anspråk vid förberedelser för kärnvapenanvändning, vilket medför att de inte samtidigt kan genomföra konventionella operationer.

Tempot för genomförandet av insatser och den ovan nämnda förmågan att upptäcka, följa och bekämpa rörliga mål med plattformar och vapenbärare som är svåra att bekämpa på vägen mot målet är allmängiltiga förmågeaspekter som är giltiga även inom kärnvapenområdet.

## Aktörer

Enligt inledningen är USA, Storbritannien, Frankrike, Ryssland och Kina de fem kärnvapenstaterna som enligt Icke-spridningsavtalet (NPT) har rätt att inneha kärnvapen. Indien, Pakistan, Israel och Nordkorea anses ha kärnvapen men står utanför avtalet och är i den meningen inte kärnvapenstater som det definieras i avtalet.

I egenskap av Sovjetunionens arvtagare inom kärnvapenområdet, är Ryssland tillsammans med USA det land som genomfört flest provsprängningar och också den

nation som kan sägas vara mest beroende av kärnvapen i sin säkerhetspolitik. Det är dessutom det land som har flest typer av kärnvapen i sin aktiva arsenal.

Det finns ett antal stater som kan betecknas som tröskelstater i den mening att de har stora delar av den industriella kärntekniska infrastruktur som behövs för ett kärnvapenprogram. Dit skulle man kunna räkna Tyskland, Japan och Iran även om det bara är den sistnämnda som, på goda grunder, betraktas som ett politiskt problem idag. Ett Iran med kärnvapen skulle starkt påverka både den regionala balansen och undergräva förtroendet för Icke-spridningsavtalet för de parter som har gått med som icke-kärnvapenstater. Det är svårt att säga något om utvecklingen fram till 2050 utöver att det sannolikt kommer att bli komplicerat. Det är förmodligen ett risktagande att under perioden fram till 2050 ta Icke-spridningsavtalet för givet.

Vi har tidigare nämnt den kinesiska utvecklingen av arsenalen, och inom perioden fram till 2050 är faran överhängande att den kommer upp i samma storleksordning som de arsenaler USA och Ryssland har. Det sista existerande avtalet, det Nya startavtalet (eng. *New START Treaty*) löpte ut 5 februari 2026 och därmed saknas idag rustningskontrollerande regimer inom området. Dynamiken mellan dessa tre parter förefaller svår att förutsäga med mer än att det sannolikt kommer att bli ett komplicerat triangeldrama. I det sammanhanget kan det vara värt att nämna att trots dagens spända relation mellan USA och Ryssland har de båda parterna en lång erfarenhet av att leva tillsammans med kärnvapen och en doktrin om ömsesidig garanterad förstörelse. Kina har inte den erfarenheten eller den relationen, men har också haft förmånen att från sidan betrakta utvecklingen av relationen mellan USA och Ryssland under många årtionden. De behöver med andra ord inte genomgå samma våndor som har präglat utvecklingen av relationen mellan kärnvapenstaterna USA, Ryssland och när det begav sig Sovjetunionen.

Avslutningsvis behöver vi lyfta möjliga händelser som inträffar mer eller mindre plötsligt och som kan komma att rita om kartan över en natt. I det här sammanhanget skulle en sådan händelse vara att ett eller flera kärnvapen faktiskt används i ett skarpt läge. Utfallet av en sådan utveckling är svårt att förutsäga, bland annat eftersom det finns så många faktorer att ta hänsyn till, såsom exempelvis militära, politiska och psykologiska. Dessutom finns ett stort utfallsrum över de omständigheter där en sådan händelse skulle kunna inträffa och en mängd olika händelseförlopp som potentiellt skulle kunna leda fram till att ett sådant beslut fattas. Ett första steg mot att förbereda sig för det oväntade i detta sammanhang kan vara att inte av automatik eller gammal vana *a priori* förutsätta att kärnvapen inte kommer att komma till användning.

## Lästips

Standardverket för kärnvapenverkan är Lars Wigg, Handbok för kärnvapenverkan, FOA-R--96-00378-4.1SE, 1996. Ett mer tillämpat exempel på kärnvapenverkan finns att läsa om i Martin Goliath et al., Kärnvapenscenario för räddningstjänst, FOI-R--5131--SE, 2021.

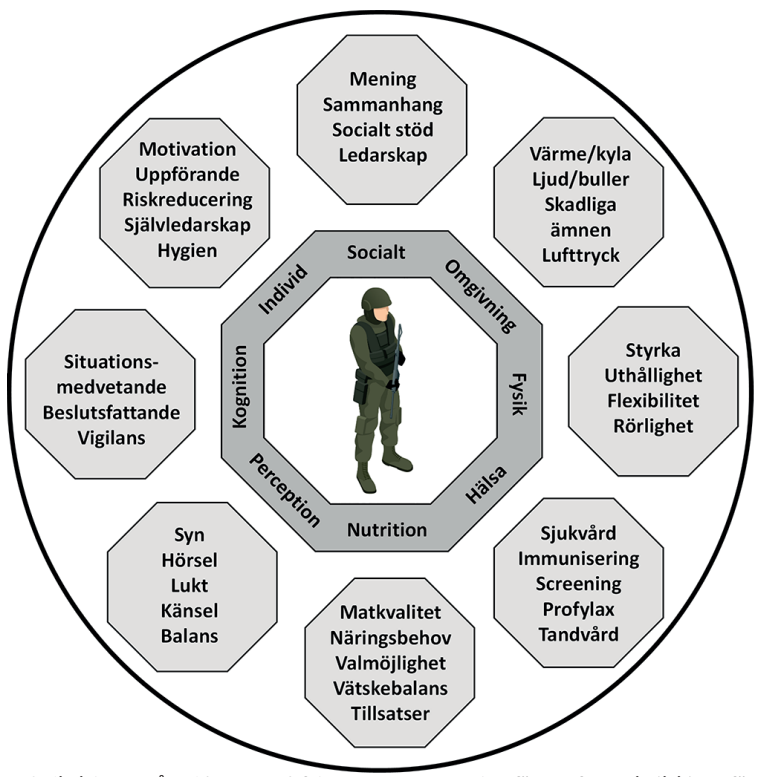
En bra introduktion till rysk kärnvapendoktrin är Kristina Melin, Russia's Updated Principles for Nuclear Deterrence A Broom for all Corners?, FOI Memo 8829, 2025. En introduktion till avskräckning finns i Karl Sörenson, Kort om avskräckning, FOI Memo 8204, 2023.

# Soldatsystem

*Britta Levin, Hans Kariis, John Ottosson, Wilhelm Sahlén och David Bergström*

## Inledande beskrivning

Soldatsystemet inkluderar individ, med dess utbildning och färdighet, och materiel såsom personlig utrustning, befattningsspecifik utrustning och av soldaten buren grupputrustning. Soldaten ingår som en del av en grupp där varje individ har en tilldelad uppgift/roll som måste samspela med resten av gruppen för att skapa en funktionell enhet. Detta ställer krav på effektiv kommunikation och interaktion mellan individer inom såväl som mellan grupper. Sett ur ett ledningsperspektiv ingår soldaten som en nod i en större helhet och bidrar med interaktion mellan nivåer som pluton och kompani. Att individen är en del av systemet innebär att soldatens prestation, i form av kognitiv och fysisk förmåga, påverkar systemets möjlighet att skapa effekt. Förutom tillgång till teknik i form av diverse utrustning är soldatens prestation i fält beroende av fysisk komfort, ergonomi, näringstillförsel och vila såväl som träning och förberedelser inför insatsen, såsom illustreras i figur 10.




**Figur 10** En holistisk syn på soldaten med faktorer som samverkar för att forma individens förmåga och motståndskraft.

## Trender och exempel

Det går att se ett antal övergripande trender inom området. Exempel på trender är ansatser inom interoperabilitet, material, autonomi, konnektivitet, människa-maskin-gränssnitt och inte minst inom energiförsörjning där ett antal exempel ges. Området är både brett och tvärvetenskapligt och påverkas av utvecklingen inom många andra i antologin beskrivna områden. De exempel som tas upp i detta kapitel utgör enbart ett axplock och kapitlet kan med fördel läsas som ett komplement till det som skrevs i Militärteknik 2045.[325]

### Övergripande trender

Det finns ett ökat fokus på interoperabilitet som inte minst aktualiserats med tanke på det rådande omvärldsläget. Interoperabiliteten är kritisk för förmågan att verka effektivt i en nationell såväl som internationell kontext. Det kommer bli än viktigare att olika militära system och nationer kan utbyta information, resurser och taktik smidigt. För den framtida soldaten innebär detta en ökad teknisk kompatibilitet (genom standarder) och möjligheter till en organisatorisk samsyn på hur till exempel träning ska bedrivas. Utmaningar inkluderar att balansera innovation med standardisering, samt hantera cybersäkerhet i ökad digitalisering.

#### *Material*

Det har länge uttryckts stora förhoppningar om möjligheter med smarta material. Teknikutvecklingen inom smarta material, och additiv tillverkning i 3D såväl som 4D, har visat potential till banbrytande möjligheter inom militära sammanhang. Med 4D-printing kan strukturer programmeras att förändras över tid och anta nya former när de utsätts för stimuli som temperatur, ljus eller andra yttre faktorer. Bland viktiga områden ses material som reagerar på externa stimuli (som temperatur, ljus eller tryck), material som reparerar sig självt efter skador, möjlighet till tillverkning av diverse materiel vid behov och effektiv återvinning.

#### *Autonomi*

I framtiden kommer möjligheterna till nära samverkan mellan människa och maskin att öka, där balansen mellan mänsklig kontroll och maskinell autonomi är en viktig fråga. Utvecklingen av autonoma eller semiautonoma system som kan samverka med soldaten förväntas ha stor inverkan på soldatsystemets behov av förändring. Autonoma system kan assistera soldaten vid genomförande av olika uppgifter, till exempel genom att agera observatör, leverera en vapeninsats, minska soldatens burna vikt samt sköta transporter.

325 Kindvall, G. och Lindberg, A.(red.), Militärteknik 2045 – Ett underlag till Försvarsmaktens perspektivstudie, FOI-R--4985--SE, november 2020.

*Konnektivitet*

Den moderna soldaten förväntas operera i komplexa nätverksbaserade system där snabb datadelning, beslutsstöd och samordning är avgörande för taktisk överlevnad och framgång. I USA finns redan trådlösa kommunikationslösningar med kort räckvidd framtagna, för till exempel *Rapid Target Acquisition*, där bilden från ett IR-sikte trådlöst överförs och visas i ett huvudburet NVG-system (*Night Vision Goggles*). Sensorfusionen snabbar i detta fall upp tiden från upptäckt till skott och möjliggör förmågor som att skjuta utan att vara i skottställning eller från en skyddad position.

*Människa-maskin-gränssnitt*

I takt med att digitaliseringen av stridsmiljön intensifieras, blir behovet av sömlösa övergångar mellan olika gränssnittskomponenter allt viktigare. Framtidens soldatsystem förväntas integrera displayytor, sensorflöden och beslutsstödsystem i en sammanhängande och adaptiv helhet. Målet är att skapa en användarupplevelse där information flödar fritt mellan enheter – från kroppsburna skärmar och visir till röststyrda kommandosystem och haptisk återkoppling – utan att störa soldatens fokus eller tempo.

## Exempel på teknik

Det går att dela in soldatrelaterade teknikområden i förutsättningsskapande förmåga och militär förmåga. Kapitlet tar upp exempel på tekniker inom områden som avancerad databearbetning och AI, energiförsörjning, kommunikation och nätverkslösningar, verkan, kamouflage, sensorer och människa-maskin-gränssnitt.

I vissa fall kan en och samma teknik användas på olika sätt. Den snabba utvecklingen inom materialteknik, nanoteknik och mikroelektronik har gjort det möjligt att skapa robotar i millimeterskala – med egenskaper som liknar biologiska insekter. Ett exempel är en flygande mikrorobot som efterliknar insekters rörelsemönster med hög smidighet, robusthet och precision.[326] Med en vikt på under ett gram och ett lyftkraft-till-vikt-förhållande på 2,2 kan roboten ta mer än sin dubbla vikt i nyttolast. Den är utrustad med fyra vingar som rör sig oberoende av varandra, vilket ger exceptionell manöverförmåga i luften. För att uppnå snabb och effektiv rörelse använder roboten piezoelektriska aktuatorer – komponenter som fungerar likt biologiska muskler och möjliggör snabb och responsiv styrning.

*Avancerad databearbetning och AI*

Nya beräknings- och signalbehandlingsmetoder är avgörande för tekniker som baseras på analys av stora datamängder. Ett exempel är neuromorf teknik som är ett framväxande forskningsfält som syftar till att efterlikna hjärnans struktur och

326 Kim, S., Hsiao, Y. H., Ren, Z., Huang, J., & Chen, Y. (2025). Acrobatics at the insect scale: A durable, precise, and agile micro–aerial robot. Science Robotics, 10(98), eadp4256.

funktion i elektroniska system. Genom att designa hårdvara och algoritmer inspirerade av biologiska neuroner och synapser möjliggör tekniken energieffektiv och adaptiv informationsbearbetning. Neuromorfiska komponenter, såsom spikande neurala nätverk och specialiserade chip (till exempel Intel Loihi och IBM TrueNorth), används för att förbättra kognitiva funktioner i tillämpningar som robotik, sensorisk bearbetning, *edge computing* och självlärande AI-system.

*Energiförsörjning*

Med nya batterikemier som fastfasbatterier finns en potential att nå dubbla energidensiteten jämfört med nuvarande celler. Det finns fortfarande flera utmaningar, inte minst att utveckla batterier som klarar många laddcykler utan att tappa prestanda. Samtidigt pågår mycket forskning inom området, både på företag och universitet.

För extrema miljöer, sett till värme och kyla, finns det battericeller/kemier som är relativt nära kommersialisering. Det skulle kunna bli aktuellt för soldaten att ha med sig olika celler beroende på var den ska verka.

Linköpings universitet har utvecklat ett batteri som består av plast och lignin och förväntas kunna integreras i elektronik på helt nya sätt. Batteriet kan formas fritt som tandkräm och sträckas ut till sin dubbla längd med bibehållen prestanda. Nyckel till den goda prestandan är flytande elektroder.[327]

Det finns flera exempel på tekniker för att utvinna energi ur olika typer av närliggande energikällor och på så sätt förse soldater med elektricitet. Bland exempel finns sätt att utvinna elektricitet med hjälp av mjuka och töjbara material[328], från människokroppen i form av värme och rörelse[329], samt luftfuktighet.[330] Flertalet lösningar befinner sig dock på en låg TRL och bedöms kräva betydande utvecklingsinsatser innan de kan användas praktiskt.

*Kommunikation och nätverkslösningar*

Förutom kommunikation mellan soldater och olika ledningsnivåer finns behov av data- och informationsöverföring såväl mellan burna system och sensorer som med mindre obemannade plattformar. Kraven på tillgänglighet, räckvidder och datatakter varierar över tiden. Adaptiva radiosystem som flexibelt kan välja mellan olika vågformer och frekvenser utgör viktiga möjliggörande tekniker för den

327 Mohammadi, M., Mardi, S., Phopase, J., Wentz, F., Samuel, J. J., Ail, U., ... & Rahmanudin, A. (2025). Make it flow from solid to liquid: Redox-active electrofluids for intrinsically stretchable batteries. Science Advances, 11(15), eadr9010.

328 Vallem V, Sargolzaeiaval Y, Ozturk M, Lai YC, Dickey MD. Energy Harvesting and Storage with Soft and Stretchable Materials. Adv Mater. 2021 May;33(19):e2004832. doi: 10.1002/adma.202004832.

329 Zhou, M., Al-Furjan, M. S. H., Zou, J., & Liu, W. (2018). A review on heat and mechanical energy harvesting from human–Principles, prototypes and perspectives. Renewable and Sustainable Energy Reviews, 82, 3582-3609.

330 Liu, X., Gao, H., Ward, J.E. et al. Power generation from ambient humidity using protein nanowires. Nature 578, 550–554 (2020). https://doi.org/10.1038/s41586-020-2010-9.

önskade sömlösa kommunikationsförmågan. Dessa system kombinerar kompakta multiantennsystem med möjlighet till lobformning, diversitetsvinster eller spatiell multiplexing, med relänoder och multihoppfunktionalitet i självkonfigurerande och självläkande nät.

*Verkan*

Soldatburna verkans- och skyddssystem bedöms även i framtiden vara avgörande för vissa militära uppgifter där tyngre och mer långräckviddiga system inte är lämpliga med hänsyn till bristande effektivitet eller tredjepartsrisk. Över tid bedöms dock högteknologiska aktörer i ökande grad kunna avlasta soldater genom robotiserad logistik- och verkansförmåga och i kombination med sensorer och moderna metoder för beslutsstöd göra soldaten till en taktisk beslutsfattare.

En mindre riskaversiv logistikkedja kommer troligen att möjliggöra snabbare och större logistikflöden vilket möjliggör att tyngre vapen kan frambringas för att kompensera för motståndarens skydds- och vapenutveckling. Det vill säga, om robotar tar över logistiken kan materiel transporteras genom mer riskfyllda områden utan att personal utsätts för fara. Detta möjliggör att tyngre och mer omfattande beväpning kan föras fram närmare fronten än vad som annars hade varit möjligt. En avgörande fråga bedöms vara hur kostnadseffektivitet och agilitet i motmedelsutvecklingen kan erhållas.

Viktiga utmaningar bedöms inkludera:

- Optimering av balansen mellan verkan, skydd och rörlighet utifrån hotutvecklingen och tekniska landvinningar. Kontinuerlig analys och jämförelse mellan olika verkans- och skyddsstrategier. Rationell teknisk värdering av faktisk förmåga (mobilitet, verkans- och sårbarhetsvärdering).
- Kostnadseffektivitet, motståndskraft mot motmedel som t.ex. aktiva skydd och telekrig och vikts-/volymseffektivitet för ostyrda såväl som styrda vapen och kroppsskydd.
- Anpassade system för verkan/skydd mot obemannade hotsystem av såväl fjärrstyrd som autonom typ.

*Kamouflage*

För att möta hotet från nya sensorteknologier och förändrad flora av sensorbärare (drönare) utvecklas ny signaturanpassningsteknik. Utveckling inom civil materialvetenskap kan där komma till nytta såsom tunnfilmsdisplayer, olika tvådimensionella material, spektralt designade fotonkristaller, ledande polymerer och cellulosabaserade material.

Inspiration kan hämtas från naturen (biomimetik), till exempel fjärilar och skalbaggar med fotonkristaller eller bläckfiskar och kameleonter med adaptivt kamouflage.

Soldatmaskering kan i högre grad komma att tillverkas av naturliga material såsom cellulosa, ull, viskos, lin, hampa. Dessa har fördelarna att råvaran är nedbrytbar i naturen och tillgänglig i Sverige.

Soldatens termiska signatur (skenbar temperatur) kan minskas genom inblandning av lågemissiva material (t.ex. metallnanotrådar) i textilier. Den faktiska temperaturen på soldaten kan regleras med hjälp av fasövergångsmaterial (PCM). Dessa material är några av de som för närvarande studeras i EU-projektet ACROSS (eng. *Adaptive camouflage for soldiers and vehicles*).

### *Sensorer*

För NVG-system sker en kontinuerlig förbättring av prestanda (eng. *Figure Of Merit*, FOM) hos bildförstärkarrören, där upplösningsförmågan successivt kunnat ökas genom minskning av hålstorlekar i de mikrokanalplattor som förstärker de fotokonverterade elektronerna. Hållfastheten hos de millimetertunna plattorna börjar dock numera nå en gräns där hålstorlekar inte kan göras mindre på grund av begränsningar i använda glasmaterial och tillverkningsmetoder. Forskning och utveckling pågår därför kring alternativa tillverkningstekniker (såsom laserborrning), men också på att helt ersätta mikrokanalplattor med tunna membran av halvledarmaterial som inte har samma fysikaliska begränsningar.

Inom 4–5 år förutspås FOM-värden (i median) kunna ökas från dagens ca 2500–2700 till åtminstone 3500–4000 genom dessa förbättringar, vilket kommer innebära ökad räckvidd och/eller NVG-system med bredare synfält än dagens konventionella $40^0$. Introduktion av halvledarkomponenter banar också väg för en ny era av digitala bildförstärkartekniker, där utläsning av signal kan göras med liknande tekniker som används i moderna kamerasystem, vilket skapar ökade förutsättningar för inbyggd och mer avancerad signal- och bildbehandling i form av bildkvalitetsförbättring och autonom detektion och igenkänning. Den digitala bildförstärkartekniken skapar också förutsättningar för bildinformation att enklare kunna lagras och delas mellan olika enheter i stridande nätverk.

IR-tekniken som används i soldatburna sensorsysten genomgår också en kontinuerlig utveckling, där reducering av pixelstorlek förväntas öka pixelupplösningen hos IR-system. Likt utvecklingen av bildförstärkare kan ökad upplösning resultera i längre räckvidder hos system och/eller till ökade synfält med en bättre täckningsförmåga. Eftersom pixelstorlekar dock redan nu börjar närma sig diffraktionsgränsen (skalan av våglängd) är det att förvänta att denna utveckling så småningom kommer att avstanna och att fortsatt utveckling snarare kommer handla om andra egenskaper så som ökad känslighet, snabbare respons, multispektral förmåga och mer avancerad och inbyggd signalbehandling. En tydlig trend på senare tid är multiband eller multifärg, där en och samma pixelmatris kan registrera samtidig bildinformation från två eller flera separata våglängdsband. Multispektrala EO-system får antas bli allt vanligare i perspektivet 10–15 år, då dessa skapar förutsättningar för

förbättrad upptäcktsförmåga genom att till exempel göra det svårare för en motståndare att vidta erforderliga signaturanpassningsåtgärder.

*Människa-maskin-gränssnitt*

I takt med att mängden tillgänglig information ökar, uppstår en växande utmaning: att filtrera, prioritera och presentera rätt data vid rätt tidpunkt för varje användare. Det räcker inte längre med statiska menyer eller enkla skärmar – framtidens gränssnitt måste vara intelligenta, kontextmedvetna och situationsanpassade. Ett sätt att möta detta behov är multimodala gränssnitt som kombinerar olika modaliteter (såsom gester, tal, blickriktning med flera) med automatisering. Genom att tolka användarens beteende, miljö och intention i realtid kan systemet anpassa sin respons – exempelvis genom att visa relevant information, dölja störande element eller föreslå nästa steg. Ett exempel på ny typ av informationsöverföring är en elektronisk skjorta som detekterar skador och meddelar status via soldatstödsystemet.[331]

## Samverkande och förutsättande förmågor och tekniker

I takt med att utvecklingen inom energiförsörjning har gått snabbt framåt har bristen på standardisering blivit alltmer påtaglig, vilket medför flera praktiska och operativa utmaningar. En ökad grad av standardisering skulle underlätta för soldater, både nationellt och internationellt, att dela energi med varandra eller att ansluta till gemensamma energikällor och lagerlösningar. Detta skulle i sin tur bidra till ökad interoperabilitet, effektivare resursanvändning och förbättrad operativ förmåga i fält.

NVG-system börjar redan idag integreras allt mer med AR, där egenposition, målpositioner, navigationspunkter och annan användbar taktisk information kan överlagras i bildförstärkarens display. I allt större utsträckning integreras dessa med olika TAK (eng. *Team Awareness Kit*)-applikationer för uppdragsplanering, nätverkskommunikation och förbättrad geospatial situationsmedvetenhet mellan olika stridande grupper. Fusionerade NVG-system är också på stark frammarsch, där en termisk IR-bild optiskt överlagras bildförstärkarbilden, vilket bidrar till en snabbare upptäckt av varma hotobjekt i terrängen. I framtiden är det önskvärt att kunna fusionera information från flera olika typer av sensorer.

Ett annat exempel på samverkande förmågor är kroppsnära sensorer och nätverkslösningar. Forskare vid MIT har utvecklat en ihålig fiber som kan förses med mikrokomponenter i form av minne, processorer och enheter för trådlös kommunikation.[332] Den mjuka och töjbara fibern kan vävas in i textilier utan att förlora sin funktionalitet, vilket möjliggör distribuerad databehandling direkt i kläder.

331 South, T., Smart shirt could detect, and one day treat, fatal wounds. ArmyTimes, 11 Oktober 2022

332 Gupta, N., Cheung, H., Payra, S. et al. A single-fibre computer enables textile networks and distributed inference. Nature 639, 79–86 (2025). https://doi.org/10.1038/s41586-024-08568-6.

## Påverkan på militär förmåga

Framtidens adaptiva gränssnitt förväntas vara dynamiska, kontextmedvetna och skräddarsydda efter individens roll, uppgift och kognitiva belastning. Gränssnittet blir inte längre en passiv kanal för information, utan en aktiv medspelare som förstår användarens behov och anpassar sig därefter – oavsett om det handlar om visuell presentation, haptisk återkoppling eller röststyrning. Denna typ av teknologisk symbios mellan människa och system kan i förlängningen förbättra reaktionsförmåga, precision och samverkan på slagfältet.

Smarta material kan integreras med sensorer som detekterar kemiska ämnen, strålning eller rörelse. En uniform med inbyggda nanosensorer skulle kunna varna för hot i realtid, medan 4D-printade antenner anpassar sig för optimal signalstyrka, vilket är avgörande för samordning i komplexa operationer. Dessa innovationer kan inte bara öka soldaters säkerhet och effektivitet utan också transformera logistik, underhåll och taktisk anpassningsförmåga.

Det är troligt att dagens stora militärtekniska problem i form av drönare förr eller senare kommer att lösas med för ändamålet utvecklade motmedel, varpå kapplöpningen mellan medel och motmedel fortsätter. Segrande i den militärtekniska kapplöpningen kommer även i framtiden vara den som snabbast och bäst kan sammankoppla relevanta underrättelser om motståndarens aktuella och framtida förmågor, en strukturerad och lösningsorienterad process för framtagning av ändamålsegna motåtgärder i intim samverkan med slutanvändaren, kostnadseffektiv och robust materielproduktion och en fungerande process för snabb fältsättning och anpassad utbildning och träning. Sist och inte minst kommer områdets utveckling att påverkas av möjligheterna till att både utvinna och lagra energi på effektiva sätt.

## Aktörer

Flera större nationer har utvecklat och fortsätter att vidareutveckla egna soldatsystem. Eftersom dessa system består av många olika komponenter och bygger på tvärvetenskaplig forskning, återfinns aktörerna inom vitt skilda sektorer. Delkomponenter som verkan, skydd och sensorer drivs främst av försvarsindustrier och forskningsinitiativ med militär inriktning, medan framväxande teknologier som AR, talinteraktion, användning av AI och biosensorer i stor utsträckning utvecklas inom den civila sektorn. Organisationer som EU (inom bland annat EDA och EDF) och Nato (inom *Science and Technology Organization*, STO) bedriver verksamhet som bland annat syftar till att ta fram underlag för standardisering. Målet är att effektivisera materielanskaffning och öka möjligheterna till utbytbarhet, energiförsörjning och interoperabilitet mellan olika nationers system.

Kriget i Ukraina har blivit en katalysator för innovation – särskilt på taktisk nivå, direkt bland soldaterna vid fronten. I takt med att konflikten utvecklats till en adaptiv stridssituation, som kräver kontinuerlig anpassning av både taktik och

teknik, har behovet av snabba och kreativa lösningar blivit avgörande för stridsteknisk överlevnad och framgång. Detta har lett till en våg av teknologiskt och taktiskt nytänkande som har förändrat hur krigföring bedrivs på soldatnivå. Den ökade kreativiteten kan delvis förklaras av bristen på kvalificerad materiel, och i vissa fall brist på samordning hos såväl motståndare som egna förband (till exempel luftsamordning), vilket har tvingat fram nya lösningar i en akut situation. Ur ett framtidsinriktat perspektiv framstår dock fortfarande förmågan att tänka i system som en avgörande framgångsfaktor. Ett helhetsgrepp med fokus på integration och systemarkitektur skulle kunna lägga grunden för en mer effektiv och samordnad utveckling av framtidens soldatsystem. Genom att tillämpa ett övergripande systemperspektiv skapas förutsättningar för att optimera samverkan mellan teknik, taktik och individ – vilket i sin tur stärker den operativa förmågan på alla nivåer.

MIT:s *Institute for Soldier Nanotechnologies* (MIT-ISN) är ett samarbete mellan MIT, USA:s armé och flera industriföretag. Forskningscentrets mål är att revolutionera soldaters skydd, utrustning och operativa stöd genom banbrytande nanotekniklösningar. Forskningen är bred och omfattar användning av nanoteknik inom strategiska områden såsom medicin, fotonik, bioteknologiska material och energisystem. Exempel på applikationer är snabba diagnosverktyg, smarta bandage, material för extrema miljöer, multifunktionella material, detektion av farliga ämnen, kamouflageteknik samt kompakta och effektiva energikällor.[333]

Ett exempel på en explorativ ansats är den internationella tävling, *xTechHumanoid*, som den amerikanska armén har utlyst med målet att identifiera och påskynda utvecklingen av prototyper för militariserade humanoider. En militariserad humanoid definieras som en teknisk replik av en stridande människa vad gäller utseende, funktion och kapacitet som kan arbeta tillsammans med soldater i varierande operativa miljöer. När de är fullt utvecklade förväntas de erbjuda alternativa stridskrafter som möjliggör ett brett spektrum av kostnads- och resurseffektiva metoder för krigföring. Syftet är att humanoiderna ska komplettera och samverka med – snarare än ersätta – soldater och andra stridande befattningar. Åtgärden bedöms ha potential att reducera operativa risker och minimera personalens exponering i högriskmiljöer.

## Lästips

Kim, S., Hsiao, Y. H., Ren, Z., Huang, J., & Chen, Y. (2025). Acrobatics at the insect scale: A durable, precise, and agile micro–aerial robot. Science Robotics, 10(98), eadp4256.

Kudithipudi, D., Schuman, C., Vineyard, C.M. et al. Neuromorphic computing at scale. Nature 637, 801–812 (2025). https://doi.org/10.1038/s41586-024-08253-8 .

333 https://isn.mit.edu/major-transitions, hämtad september 2025.

Gupta, N., Cheung, H., Payra, S. et al. A single-fibre computer enables textile networks and distributed inference. Nature 639, 79–86 (2025). https://doi.org/10.1038/s41586-024-08568-6.

# Mänsklig förstärkning

*Britta Levin*

## Inledande beskrivning

Mänsklig förstärkning är samlingsnamnet för tekniker och metoder som syftar till att öka eller bibehålla nivån på mänsklig prestation. Begreppet kan delas in *HPO* (eng. *Human Performance Optimization*) och *HPE* (eng. *Human Performance Enhancement*). Delområdet HPO omfattar strategier för att öka prestationen inom det som anses ”biologiskt normalt” för populationen genom till exempel urval, utbildning, träning, nutrition, vila, läkemedel och ledarskap. HPE handlar om att skapa nya och utökade förmågor genom yttre såväl som inre modifikation av kroppens strukturer och funktion. Detta kan uppnås genom till exempel kirurgiska ingrepp, genetisk förändring, farmakologiska substanser, nervstimulering, implantat, exoskelett och proteser.

Begreppet är brett och omfattar användningen av en mängd olika tekniker och metoder. På senare tid har begreppssfären utökats till att även omfatta tillstånd där människans prestation minskas, degenerering, såväl som återställs från ett dylikt tillstånd. Samtliga dessa begrepp ryms inom paraplybegreppet mänsklig modifiering.[334]

Begreppet Försämring av mänsklig prestation, *HPD* (eng. *Human Performance Degradation*) innebär en minskning av individens prestationsförmåga jämfört med tidigare nivåer. Minskningen kan vara orsakad av fyra huvudsakliga faktorer: 1) daglig variation genom normalt leverne och utförda uppgifter, 2) omständigheter såsom olycksfall och sjukdom, 3) brister i systemsäkerhet relaterat till biverkningar och reliabilitet, 4) fientliga aktioner som direkt syftar till att skada individen eller nyttja svagheter i systemen. Alla fyra varianterna påverkar individen negativt men konsekvenserna är olika. En positiv förändring inom den dagliga variationen (från måttlig degenerering) kallas återhämtning medan att återta förmåga från övriga fall av degenerering kallas återställning av mänsklig prestation (*HPR*, eng. *Human Performance Restoration*).

HPR avser metoder och strategier för att hjälpa individen att återgå till sin ursprungliga prestationsnivå efter att denna tillfälligt eller permanent har försämrats. HPR omfattar ett brett spektrum av tekniker och metoder som syftar till att återställa individens fysiska, kognitiva och emotionella funktioner. Som exempel ses behandling av posttraumatiskt stressyndrom (PTSD), avancerad protesteknik med sensorisk feedback, 3D-printade biologiska strukturer för vävnadsersättning (hud, brosk, organ), exoskelett som stöd vid rehabilitering och hjärnimplantat för vissa neurologiska funktionsnedsättningar.

334 MCDC. (2021). Information Note of the MCDC HPO/HPE Cycle 19/20. MULTINATIONAL CAPABILITY DEVELOPMENT CAMPAIGN (MCDC), March 2021.

Området är tvärvetenskapligt och det finns överlapp med andra i rapporten beskrivna områden som bioteknik och soldatsystem.

## Trender och exempel

Det går att se ett antal övergripande trender som kan påverka utvecklingen av tekniker och metoder för mänsklig förstärkning. Bland dessa trender ses ett ökat samhälleligt intresse för träning, självmedicinering, teknikutveckling mot kroppsnära teknik (biosensorer och hjärn-datorgränssnitt), användning av AI, bioteknik och inte minst möjligheter till ökad individanpassning. Tekniskt sett kan en indelning göras i yttre applicerad utrustning (objekt utanpå kroppen), implantat (artificiellt eller biologiskt objekt som sätts in i kroppen), substanser (läkemedel, näringsämnen etc.), genetisk modifiering och träningsmetoder.

### Övergripande trender

När en stor mängd olika varianter av data samlas in från individer och analyseras med hjälp av AI uppstår oanade möjligheter att identifiera hittills okända samband. Intresset för träning och hälsa främjar produkter som baseras på biosensorer och medicinska självtester. Det går att se en utveckling mot hybridlösningar där kroppssensorer kombineras med AI som tolkar olika typer av data i realtid. Kroppsnära teknik passar för breda tillämpningar inom träning, hälsa, prestationsutvärdering och för att kartlägga omgivningsfaktorer.

Möjligheter med hjärn-datorgränssnitt (ofta refererat till som BCI, eng. *brain-computer interface*) diskuteras ofta. BCI-tekniken utvecklas snabbt och visar lovande resultat för att återställa funktioner hos personer med neurologiska funktionsnedsättningar. I nuläget arbetas med att förbättra taktila upplevelser, så att användare kan känna beröring via proteser eller robotarmar – en avgörande faktor för effektiv kontroll och livskvalitet.

Framtida BCI-system förväntas bli mer intuitiva, trådlösa och mindre invasiva, vilket kan öppna för bredare användning även utanför medicinska tillämpningar. Det är troligt att framtida kroppsburna sensorer och BCI kommer att komplettera varandra. Till skillnad från motoriska kommandon (som att röra en hand), är kognitiva processer som minne, uppmärksamhet och beslutsfattande mycket mer abstrakta och diffusa. De involverar flera hjärnregioner samtidigt, vilket gör det svårt att isolera tydliga signaler som kan användas i ett BCI-system. Det som däremot har visat potential är möjligheten att avläsa tankar för att använda som ett sätt att snabba upp kommunikation. Ett neuralt nätverk har till exempel lyckats syntetisera tal med hjälp av *Electrocorticography* (ECoG), dvs. utgående från nervcellers aktivitet som registreras med hjälp av elektrodmatriser placerade direkt på hjärnbarken. På senare tid har dock icke-invasiva tekniker gått framåt. Med tanke på medicinska

risker med invasiva implantat samt andra osäkerheter och komplikationer bedöms de icke-invasiva teknikerna ha störst potential för den framtida soldaten.

Individanpassning kommer bli möjlig i takt med att kunskap och system tas fram som underlättar detta**.** Anpassad nutrition handlar om att säkerställa tillräckligt och gynnsamt näringsintag för den enskilde individen. Med nya mätmetoder och kunskap om biologiska system skulle anpassningen av nutrition kunna förbättras än mer på individbasis. Träning och coachning syftar till att göra soldater bättre rustade för kommande påfrestningar. Skräddarsydda träningsprogram ökar fysisk förmåga samtidigt som förslitningar orsakade av överbelastning på grund av felaktig träning undviks. Fysisk aktivitet bidrar också till att höja den kognitiva förmågan genom att stimulera bildandet av nya nervceller i hippocampus.

Regenerativ medicin syftar till att reparera, ersätta eller återställa skadade celler, vävnader och organ och beskrivs även i kapitlet bioteknik. Inom biomedicinsk forskning ses stamcellsteknik och regenerativ medicin som revolutionerande för att adressera allvarliga skador, kroniska sjukdomar och brist på transplantationsorgan.

## Exempel på teknik

Det finns ett antal forskningsområden vars framsteg och innovationer utgör en grund för utvecklingen av framtida, användbara produkter.

### *Miniatyrisering och nanoteknologi*

När optik och sensorteknik miniatyriseras skapas sensorer som är små, lätta och som kräver minimalt med energi. Detta möjliggör på sikt integration med människans egna sinnen (till exempel i form av sensorer som är känsliga för dofter, ett brett elektromagnetiskt spektrum och ljud). Ett exempel från nanoteknologi är försök på möss som visat att synceller belagda med nanopartiklar kan ge förmåga att se frekvenser i det infraröda spektrat.

### *Avancerad databearbetning och AI*

Nya beräknings- och signalbehandlingsmetoder är avgörande för tekniker som baseras på analys av stora datamängder. Metoder inom artificiell intelligens (AI) såsom maskininlärning är väsentliga för att uppnå tillräcklig funktion hos system som baseras på data från biosensorer. Ett exempel på aktör inom området är företaget Cerebras Systems som specialiserat sig på att bygga datorsystem som är optimerade för komplexa AI-applikationer inom djupinlärning. Företaget är känt för sin innovativa teknologi *Wafer Scale Engine*,[335] som integrerar ett stort antal processorkärnor på ett enda chip, vilket avsevärt förbättrar träning och inferens av AI-modeller. Ett annat exempel är forskning vid MIT som har utnyttjat principen att radiosignaler reflekteras från människokroppar och möjliggör detektering

335 Lie, S. (2024). Inside the cerebras wafer-scale cluster. IEEE Micro, 44(3), 49-57.

av subtila förändringar utan att det krävs bärbara sensorer. Genom att analysera data från en hel natts sömn – såsom andning, hjärtfrekvens och sömnstadier (t.ex. REM-sömn) – har de kunnat identifiera samband med tillstånd som Parkinsons sjukdom, Alzheimers och andra kroniska sjukdomar.[336]

*Farmaka och droger*

Olika typer av substanser har använts för att förstärka den mänskliga förmågan inom en rad olika områden. Användbarheten varierar beroende på individens fysiska och mentala utgångsläge, och i vissa fall förekommer oönskade bieffekter samt risk för tillvänjning och beroendeproblematik. Nootropa läkemedel (eng. *smart drugs*) påverkar kognitiva funktioner såsom mental skärpa, minneskapacitet och vakenhet. Många av dessa substanser finns redan tillgängliga idag, och nya är under utveckling. Ett exempel är Modafinil som ger ökad uppmärksamhet och minskat sömnbehov och nyttjas av vissa försvarsmakter genom reglerad användning.

*Materialteknik och syntetisk biologi*

Forskning och produktutveckling inom bioteknologin kan ge biologiska eller icke-biologiska material med skräddarsydda egenskaper. Dessa kan användas i eller utanpå kroppen och ha en bättre slitstyrka eller friktion, utformas för att få bättre acceptans av kroppens vävnader och mindre beläggning av oönskade ämnen, och på sikt kopplas till nervceller eller stärka leder och skelett.

*Medicinsk teknik inklusive BCI*

Inom området ses nya metoder för interaktion mellan människan och teknik. Exempel på teknisk lösning för läkemedelsadministration är en tablett som vecklar ut sig till en stjärna när den når magsäcken och därefter utsöndrar den verksamma substansen i lagom takt under flera veckor.[337] Ett annat område som kan leda till stora förändringar är sjukvård och hälsoövervakning på distans. Möjlighet att ställa diagnos, eller utföra medicinsk behandling, baserad på (bio)sensordata, skulle i framtiden kunna förhindra och återställa skador och sjukdomsutbrott.

Närliggande till mänsklig förstärkning är ambitionen att bevara kroppen ung, bota sjukdomar eller förhindra att de uppstår. Gränsdragningen mellan behandling och förstärkning är ibland oklar, och frågan är i vilken utsträckning metoder som används för att bota eller förebygga sjukdomar även kan tillämpas för att förstärka friska individer. Även om effekten finns, kanske den inte är påtaglig eller kan medföra oönskade biverkningar. Ett exempel är forskning som visat att patienter som utsätts för ljus- och ljudpulser med en frekvens på 40 hertz – en frekvens som förknippas med hjärnrytmer inom gammaområdet – uppvisar förbättrad

336 https://theconferenceforum.org/editorial/how-mits-dr-dina-katabi-is-developing-a-next-generation-of-invisible-remote-monitoring, hämtad september 2025.

337 Tarita, T. This Star-Shaped Pill Stomach Could Transform Schizophrenia Treatment. Health, Neurology, News, 20 juni 2025.

hjärnaktivitet. Kliniska studier tyder på att tekniken kan bromsa hjärnatrofi och förbättra kognitiva funktioner hos Alzheimerpatienter.[338] Samtidigt krävs fortsatt forskning för att förstå de bakomliggande mekanismerna och för att utveckla teknikens terapeutiska potential.

BCI är ett exempel på gränssnitt för kommunikation mellan hjärnans nervceller och tekniska enheter på sätt som kan vara mer eller mindre invasiva. Synchron är ett neuroteknikföretag som utvecklar ett BCI kallat Stentrode.[339] Det är ett nätliknande elektrodimplantat som placeras i hjärnans motoriska cortex via jugularvenen. Hjärnans signaler registreras och överförs trådlöst till en extern enhet via en mottagare implanterad i bröstet. Tekniken är mindre invasiv, betydligt säkrare och mer tillgänglig än traditionella neuroimplantat. Ett annat exempel är systemet AlterEgo som är icke-invasivt och fungerar på ett helt annat sätt än tidigare nämnda BCI.[340] Enheten avläser inte hjärnaktiviteten som sådan, utan förutspår vad bäraren vill säga utifrån signaler som produceras i de muskler som användaren använder för att tala. Kommunikationen blir tyst genom att den bara utgår från de neuromuskulära signalerna.

*Bio-mekatronik*

Området omfattar utveckling av exoskelett och bioniska proteser (robotproteser). Exoskelett är en yttre struktur som stöttar det mänskliga muskel-skelettsystemet, ofta i syfte att öka styrka och uthållighet. Framtagningen av tekniska lösningar drivs främst av behoven av att avlasta operatörer från fysiskt tunga eller monotona arbetsmoment, och därmed undvika skador, samt möjligheten att ersätta förlorade kroppsfunktioner kopplat till armar och ben.

*Genteknik*

Utvecklingen inom genomredigeringsteknik har påverkat och underlättat möjligheten att göra riktade förändringar i arvsmassan. Metoden kan användas för att manipulera utvalda gensekvenser genom att stänga av, ta bort, reparera eller ersätta genetiskt material. Detta för att uppnå en önskad förändring eller förbättring. För att nå önskade effekter måste även andra forskningsområden som ger kunskap om biologiska system utvecklas.

338 Park, Jung M., and Li-Huei Tsai. "Innovations in noninvasive sensory stimulation treatments to combat Alzheimer's disease." PLoS Biology 23.2 (2025): e3003046.

339 https://synchron.com/.

340 Simms, C. (2025) The 'near-telepathic' device that puts AI in your head. Nature News. 18 Sep 2025. doi: 10.1038/d41586-025-03000-z.

*Individanpassning*

Personlig medicin bygger på ett flertal teknikområden. Genom förståelse för och kartläggning av individens biologi såsom genetik, proteomik och tarmflora, kan medicinsk behandling skräddarsys. Ett exempel är individuellt anpassad dosering av prestationshöjande medel och läkemedel utgående från individens egenskaper.

*Additiv tillverkning*

Tekniken för additiv tillverkning utvecklas ständigt och framöver ses nya möjligheter med att generera avancerade geometrier, mjuka material och möjlighet att kombinera med printad elektronik. När dessa tekniker kombineras med scaffoldmaterial (till exempel hydrogeler eller nanofibriller), skapas en tredimensionell miljö där celler kan växa och återskapa komplexa biologiska strukturer. Ett exempel på tillämpning är 3D-utskrift i biokompatibla material, vilket gör det möjligt att utveckla implantat och medicinska lösningar som kroppen kan acceptera. Ett konkret användningsområde är bioskrivare som kan skriva ut hudceller direkt på sår. Denna metod kan påskynda läkningsprocessen och samtidigt minska behovet av traditionella hudtransplantationer.

*Sensorer*

Genom att transformera sensorinformation till mänskliga spektra kan individen förses med förmågor som supersyn (till exempel att kunna se genom väggar, att uppfatta detaljer på långt håll eller i låg belysning), superhörsel (till exempel att kunna uppfatta ljud med låga nivåer med tydligare riktning och brusreducering) och superkänsel (till exempel att uppfatta låga vibrationer och farliga ämnen). Ett exempel på teknik är smarta kontaktlinser för överlagring av termisk information direkt i ögat.[341]

## Samverkande och förutsättande förmågor och tekniker

Till skillnad från många andra militära teknikområden har mänsklig förstärkning ett tydligt humanperspektiv. Tekniken ska inte bara användas av människan utan i vissa fall även vara en del av henne. Den civila utvecklingen inom området dominerar med en intressesfär som omfattar individ, organisation och samhälle. Detta innebär att diskussioner kring potential och möjligheter måste inkludera en mångfald av perspektiv: den globala tekniska utvecklingen, användbarhet och säkerhet i praktiken, kort- och långsiktiga effekter, synen på mänsklig förstärkning, etiska ställningstaganden samt legala förutsättningar såväl civilt som militärt. Dessa faktorer kommer sannolikt att vara avgörande för hur omfattande, och i vilken takt, olika typer av förstärkning implementeras. Militärt sett kommer utvecklingen

341 Ma, Y., Chen, Y., Wang, S., Chen, Z. H., Zhang, Y., Huang, L., ... & Xue, T. (2025). Near-infrared spatiotemporal color vision in humans enabled by upconversion contact lenses. Cell, 188(13), 3375-3388.

dessutom att kräva fältmässighet. Tekniken måste inte bara ge operativ effekt utan också fungera under realistiska och ofta extremt utmanande förutsättningar.

Området består av en mängd olika tekniker och metoder där förutsättningarna för framtida införande varierar och förstärkningen kommer infrias allteftersom möjligheterna med respektive teknik och metod så medger. I vissa fall finns uppenbar potential medan det i andra fall fortfarande är oklart om, eller när, tillräckliga effekter kommer uppnås. Kopplingen mellan teknikområden gör det mycket svårt att förutsäga utvecklingen på längre sikt än fem till tio år. Vilka applikationer som kommer tas fram beror både på den tekniska utvecklingen i sig och på den idégenerering som föregår produktframtagning – en process som ofta involverar flera samverkande teknikfält.

Potentialen att uppnå förstärkning förväntas vara betydligt större med HPE samtidigt som dessa metoder generellt sett är mer invasiva och därmed förenade med större risker och fler etiska dilemman. Tekniken blir kontroversiell när risken för skador är hög och bieffekter på lång sikt inte kan bedömas. Det är också så att en överdriven rädsla för att bedriva forskning på tekniker och metoder innebär att fullt rimliga lösningar inte ges en chans. Dessa insikter har bland annat adresserats av forskningsaktiviteten NATO STO HFM RTG 365 (*Human Capability & Survivability Enhancement: Augmenting people to deliver an enhanced and more resilient capability for defence*) som tagit fram ramverk för att underlätta framtagning av processer för införande av HPE. Etiska och legala ramverk är en nödvändighet, vilket bland annat uppmärksammats i samband med Natos ökade intresse för strategier för området.

## Påverkan på militär förmåga

Sätten människan kan förstärkas på kan primärt delas in i fysik, sensorik, kognition och resiliens (förmågan att motstå, återhämta sig från och anpassa sig till förändringar, kriser eller påfrestningar). Fysisk förstärkning omfattar olika sätt att skydda människan mot omgivningen samt att öka uthållighet och skadetålighet (till exempel via förstärkning av hud och senor). Sensorisk förstärkning inkluderar tekniker för att skapa nya eller förbättrade sinnen. Det handlar dels om att tillvarata den information i omgivningen som normalt inte kan uppfattas av människans sinnen, dels om nya metoder för kroppsnära informationspresentation. Kognitiv förstärkning avser olika sätt att öka den kognitiva prestationsförmågan. Förstärkt kommunikations- och interaktionsförmåga omfattar bland annat sätt att automatiskt avläsa en människas intention.

## Aktörer

Den tekniska utvecklingen inom den civila sektorn visar på framväxten av nya aktörer, ledda av entreprenörer som investerar egna resurser i högriskprojekt med fokus på innovation inom olika områden. Företag som Google, Amazon, Meta (Facebook), Neuralink och Apple driver avancerade projekt inom neuroteknik, AI, biomekanik och gränssnitt mellan människa och maskin.

Amerikanska DARPA står för bredd inom forskning och satsar på banbrytande explorativ utveckling för militära syften. Ett exempel är programmet *ADvanced Acclimation and Protection Tool for Environmental Readiness* (ADAPTER) med avsikt att utveckla system som ger individen större kontroll över sin egen fysiologi. Programmet kommer att integrera konstruerade celler och biokemiska ämnen i en intern, bioelektronisk bärare som den stridande kan aktivera vid behov. Denna bärare ska kunna producera och frisätta behandlingar som antingen eliminerar den huvudsakliga orsaken till resediarré – patogena bakterier – eller reglerar dygnsrytmen som störts av uppdragskrav eller jetlag.

Karolinska Institutet bedriver ledande forskning inom neurovetenskap, med särskilt fokus på expertisens och kreativitetens neuropsykologi. Forskningen syftar till att förstå de neurala mekanismer som möjliggör hög prestation efter långvarig och målinriktad träning. Genom avancerade hjärnavbildningstekniker och tvärvetenskapliga metoder kartläggs hur hjärnans struktur och funktion förändras i takt med att individen utvecklar expertis, samt hur kreativitet uppstår och formas i samspel mellan kognition, erfarenhet och motivation.

## Lästips

Park, Jung M., and Li-Huei Tsai. Innovations in noninvasive sensory stimulation treatments to combat Alzheimer's disease. PLoS Biology 23.2 (2025): e3003046.

NATO STO HFM TR 365 Human Capability & Survivability Enhancement: Augmenting people to deliver an enhanced and more resilient capability for defence (bedömd utgivning 2026).

How MIT Developed Invisible Remote Monitoring to Enhance Research https://theconferenceforum.org/editorial/how-mits-dr-dina-katabi-is-developing-a-next-generation-of-invisible-remote-monitoring.

# Del 4 – Syntes

*Anna Lindberg, Cecilia During och Göran Kindvall*

## Inledning

För tredje gången ger vi ut en publikation om framtida militärteknik.[342] Det är en omfattande produkt som denna gång namnsatts till antologi. I denna del återkopplar vi till antologins inledande delar, diskuterar teknikutvecklingen ur olika perspektiv och redovisar avslutande tankar om arbetet med teknik mot framtiden. Vi inleder med texter om säkerhetsstrategier och framtidens försvar. Antologins tidigare delar sammanfattas under rubriken Observationer från Del 1-3 och under Diskussion lyfts aspekter och områden vi ser som relevanta i arbeten med teknik och framtida försvarsförmåga. Under rubriken Avslutande kommentarer reflekterar vi över vilken betydelse teknik kan ha för framtida militär förmåga och hur utveckling kan te sig i relation till försvarets uppgifter.

Det kan tyckas att huvuddelen av den tekniska framsynen som presenteras i Del 2 och 3 borde vara relativt oförändrad jämfört med tidigare rapporter då vår blickpunkt ligger långt fram i tiden. Det finns likheter med tidigare utgåvor, men också skillnader. Antologin är skriven i en tid av snabb förändring. Försvarsgrenarna stärks och växer, materielsystem med långa livslängder kombineras med nya innovativa lösningar och behöver anpassas till en snabb förändringstakt inom informations- och kommunikationsteknik (IKT). Viss teknisk utveckling rusar framåt medan annan går betydligt långsammare. Produktionen av militär materiel och förband effektiviseras samtidigt som den säkerhetspolitiska och aktörsdrivna händelseutvecklingen är högst oförutsägbar, nästintill nyckfull.

Den främsta förändringen sedan tidigare rapporter är militärteknikens ökade betydelse, vilket lyfts under Observationer från Del 1. De senaste fem åren har inneburit stora skiften som en följd av den värld och kontext som teknikutvecklingen bedrivs i. Det finns en tilltro till framtida teknik och en stark investeringsvilja i en tid där teknikutvecklingen går snabbt framåt och behovet av militär förmåga är stort.

Teknikmässigt genomsyrar de senaste årens otroligt snabba framsteg inom AI-området underlagen i Del 2 och 3, då intelligenta system driver forskning och tillämpningar framåt. I antologins texter om kärnvapen och rymdsystem finns förändringar rörande

342 De bägge tidigare rapporterna är:
Kindvall, G. och Wiss, Å. (red.), Militärteknik i ett tjugoårigt perspektiv: Underlag till Försvarsmaktens Perspektivstudie 2017, FOI-R--4462--SE, november 2017.
Kindvall, G. och Lindberg, A., (red.), Militärteknik 2045 – Ett underlag till Försvarsmaktens perspektivstudie, FOI-R--4985--SE, november 2020.

militärt nyttjande. Jämfört med tidigare militärteknikrapporter har antalet kapitel utökats för att ge en bredare beskrivning av teknikutvecklingen.

Generellt finns antaganden om digitalisering, AI-tjänster och IKT i författarnas texter och flera av kapitlen bidrar därför till en fördjupning av området IKT. Syftet är att redovisa en mer fullständig bild av de teknikområden som är nödvändiga för att fullt ut genomföra den digitalisering av militär verksamhet som både förmodas och krävs inom en inte alltför lång framtid. Ytterligare nya områden i denna utgåva är bioteknik, materialteknik, energi, telekrig och vapenteknik. Kapitlen om bioteknik och materialteknik visar både hur dessa områden kan bidra in mot andra forskningsfält och hur de kan påverka framtida militär förmåga i egen rätt.

Vi täcker dock inte in allt. Områden som fått förnyat intresse är exempelvis logistik, sjukvård, CBRN och produktionstekniker för effektivare materielförsörjning. Dessa beskrivs till del i antologins texter, men är inte föremål för egna kapitel.

En ständig utmaning vid beskrivning av potentiella framtider är att inte fastna i nutida tankemönster. Samtidigt hänger det historiska, befintliga och framtida samman. Förändring tar tid men snabbas på i tider av krig i en ständig cykel av medel och motmedel. Det gamla och befintliga används tillsammans med det nya. Militärt utvecklad teknik blandas med sådan av civilt ursprung. Därutöver kan det finnas helt nya möjligheter, det disruptiva och science fiction-liknande.

Dagens förändrade kontext, där snabb upprustning och både militära och civila teknikområden bidrar till militär förmåga, kombinerat med ett växande antal nationella strategier, aktörstyper och utvecklings- och produktionsparadigm, skapar fler alternativa sätt att lösa militära uppgifter, där tekniker och tillämpningar inte är bundna till försvarsgrenar och funktioner. Detta gör att vi här finner det mer relevant att belysa större förändringar än att ge exempel på enskilda kombinationer av tekniker och materielsystem mot framtiden.

## Säkerhetsstrategier och försvar mot framtiden

Det finns många ursprung till konflikter mellan och inom stater, såsom naturresurser och ekonomi, geografiska områden och platser, inflytande över populationer och ideologi, eller tillgång till kunskap och information. Teknik nyttjas för olika ändamål och säkerhetspolitiska syften. Frågan är vad stater väljer att utveckla och införa mot framtiden samt varför. Tekniken tillämpas och ger såväl nya möjligheter som nya hot. Idag, liksom i framtiden, står människan i centrum och väljer till vad och hur tekniken ska användas. Vi inleder med en retorisk frågeställning om vad framtida försvarsförmåga ska användas till. Vad ska försvaras och värnas, vilka är aktörerna och vilka hot kan leda till konflikter?

I regeringens nationella säkerhetsstrategi[343] pekas på tre fokusområden för nationell säkerhet. Det första omfattar skyddet mot yttre hot; att bibehålla ett säkert Sverige genom utrikes-, säkerhets- och försvarspolitiken. I detta område, som benämns Ett säkert Sverige, omhändertas Natointegration, försvar och den regelbaserade världsordningen. Det andra fokusområdet, Ett tryggt, öppet och sammanhållet Sverige, innebär bland annat att värna fri- och rättigheter, rättsstatens principer och att bekämpa systemhotande organiserad brottslighet. Det tredje området, Ett motstånds- och konkurrenskraftigt Sverige, beskriver åtgärder för att stärka motståndskraft, konkurrenskraft och försörjningsberedskap. Sammantaget behövs arbete inom samtliga områden för arbetet med nationell säkerhet. Teknikerna som beskrivs i föreliggande antologi kan användas inom alla dessa tre områden, men tillhör traditionellt främst det första området.

Partnerskap och bilaterala avtal har funnits sedan lång tid tillbaka men att vara allierad i Nato utgör en omvälvande förändring. Även det utvecklade försvarssamarbetet inom EU utgör en omslagspunkt. Natomedlemskapet innebär omfattande förändringar av styrning och uppgifter för Försvarsmakten i fred och vid åberopande av Artikel 5 i Natofördraget. Medlemskapet i Nato påverkar utformningen av det svenska försvaret, idag och mot framtiden. Förutom att försvara Sverige mot väpnat angrepp ska vi även kunna verka inom det kollektiva försvaret inom Nato samt delta i Natos operationer och andra aktiviteter för avskräckning och försvar. I detta ingår bland annat värdlandsstöd, ett större operationsområde samt att placera förband i andra länder.

Status avseende Nato år 2050 väljer vi att inte hantera i antologin, inte heller andra typer av samverkan eller avtal. Vi förutsätter att bilaterala och multilaterala avtal fortsatt är centrala för svensk säkerhet och försvarsteknikområdet.

## Försvar mot framtiden i tider av snabb förändring

Vår förmåga att föreställa oss förändring, att se alternativ och att mentalt hantera den stora och komplexa osäkerheten, är fortsatt central för att fatta så bra beslut som möjligt. Vi lever i en tid av snabb förändring och får inte låta oss förblindas av det vi ser här och nu i de konflikter som pågår idag, i mitten av 2020-talet.

Krigföring anpassas till de mål som ska uppnås och de förutsättningar som råder i form av exempelvis operationsmiljöer och militärgeografier, inblandade aktörer samt styrkeförhållanden. Mot 2050 utökas paletten av tillgänglig teknik avsevärt samtidigt som den geopolitiska miljön, både globalt och i vårt närområde, kan utvecklas i olika riktningar som idag inte kan förutspås.

343 Regeringskansliet Statsrådsberedningen (2024), Nationell säkerhetsstrategi. https://www.regeringen.se/contentassets/fa7bceced8a548ada27f45b24f611714/nationell-sakerhetsstrategi.pdf.

Försvarsförmåga är en verksamhet som inriktas och byggs långsiktigt, men som också behöver vara snabb och dynamisk. Allt fler system införs löpande och det finns inom vissa områden behov av flexibel teknikutveckling och snabbt produktinförande. De uppgifter som försvaret har att lösa mot både en nära och lång framtid är, tillsammans med dagens verksamhet, utgångspunkt för val om framtida militär teknik och materiel. Försvar består dock inte enbart av teknik. Organisation, processer och människor driver utvecklingen framåt. I inriktningen mot framtiden är det därför nödvändigt att reflektera över de möjligheter och utmaningar som teknikutvecklingen kan medföra för försvaret, för att öka förutsättningarna att ta rätt beslut i rätt tid.

Legalitet och etik återkommer genom flera texter. Det råder osäkerhet avseende reglering och användning av den nya teknik och materiel som framtiden kan erbjuda. Förhållningssättet kan skilja markant mellan aktörer, något vi behöver beakta.

# Observationer från Del 1-3

## Observationer från Del 1

Antologins Del 1 redovisar den absolut främsta förändringen jämfört med tidigare utgåvor, nämligen militärteknikens ökade betydelse för säkerhet. Det råder krig i Europa, Sverige är tillsammans med Finland medlem i Nato och nationell samverkan mellan försvarsmyndigheter, näringsliv och akademi har återuppstått. Totalförsvar, nationers rådighet och försörjning är centrala krafter i den utveckling som pågår med att snabbt rusta för ett möjligt krig. Teknik existerar i en kontext, den påverkar och påverkas av globala händelseutvecklingar. Natomedlemskapet utgör en omvälvande förändring. Sveriges operationsområden och uppgifter är både i princip desamma som tidigare och avsevärt förändrade i och med medlemskapet i Nato.

Del 1 beskriver osäkerheten i den globala utvecklingen, en allt större konkurrens om teknik, kritiska råvaror och globala värdekedjor. Det pågår en utveckling där teknik, kunskap, råvaror och innovation är geopolitiska verktyg för militär kapacitet, säkerhet, inflytande, styrka och makt. Multilateralt arbete och samsyn efterfrågas av vissa, samtidigt som polarisering separerar och minskar de globala tekniska utbytena och samförstånden. Militärt viktiga tekniker, som vi i antologin kallar nyckelteknologier och integritetskritiska områden, har sedan en tid tillbaka getts allt större prioritet. Behovet av kontroll och rådighet genomsyrar de militärtekniska områdena, samtidigt som nyttjandet av civil teknik visar hur traditionell militär metod och materiel kan förbättras och utmanas idag och mot framtiden.

Det pågår en snabb teknikutveckling. Försvarsinnovation och teknikens roll i konflikter är på gemene mans radar. Vi slås av den tilltro som finns till de möjligheter framtida teknik kan ge samt till hur civil teknik kan anpassas för militärt bruk.

För en hållbar och beboelig planet är grön omställning och klimatåtgärder kritiska, även för försvaret. Flertalet större plattformar och materiel är fossilberoende och har driftskrav som skiljer sig från det civila. Samtidigt kan en omställning bidra till nya möjligheter för verkanssystem, logistik och andra delar av försvarets verksamhet.

## Observationer från Del 2 och 3

Intelligenta system, kommunikation, data, information och beräkningskapacitet är fundament för dagens och framtidens totalförsvar där lägesbilder och situationsförståelse är vanligt använda begrepp för efterfrågade tjänster. Intelligenta system och digitalisering driver upp takten på forskning, utveckling, produktifiering och verksamheters genomförande. Detta förändrar Försvarsmakten och dess organisation.

Utvecklingen går snabbt och drivs framförallt av civila aktörer, men det finns även verksamhet inom den militära sektorn. Drivkrafterna är många och kan sammanfattas med att genomföra verksamhet smartare, bättre och enklare. Det är en mycket snabb, evolutionär utveckling där teknik för IKT successivt införs i system och de redan komplexa infrastrukturerna. Militärt är Natos koncept för multidomänoperationer (MDO) och gemensamma operationer en stark drivkraft, medan regelverk och rådande processer för bland annat styrning, säkerhet och ekonomisk planering kan motverka önskad takt för införande.

Artificiell intelligens (AI) påverkar alla andra teknikområden och tjänster. Redan idag ser vi till exempel hur AI kan bidra till snabbare framtagning av lovande material och läkemedel med unika egenskaper. Artificiell generell intelligens (AGI) som motsvarar eller till och med överträffar den mänskliga intelligensen (artificiell superintelligens) måste diskuteras i en tidsram mot 2050. Forskare har skilda uppfattningar angående när, eller om, en sådan utveckling blir möjlig och vad det i så fall skulle kunna betyda för samhället i stort och för försvaret.

En gemensam nämnare som ger möjlighet till banbrytande tillämpningar är utvecklingen av AI-modeller och verktyg. I grunden består dessa av algoritmer och beräkningar, samt nyttjande av enorma datamängder. Datorer och beräkningskraft finns integrerat överallt. Det enorma beroendet av beräkning, mjukvara och hårdvara är ett faktum, från små processorer i mindre materielsystem till stora nätverk för ledning.

Förbättringar kan göras i verksamhet genom prediktivt underhåll och erfarenhetshantering avseende materielprestanda. Digitalisering är också en förutsättning för övergång till alltmer semiautonoma och autonoma farkoster samt digitala agenter och assistenter i nätverken. Digitala tjänster kan stödja arbetet med att utforma och följa upp organisation och metod.

Framtida behov och tekniska trender för informationsteknikområdet är högre hastighet i beräkningar, energieffektivitet i hårdvara och beräkningar längre ut i nätverken. Gränsen mellan central respektive distribuerad databehandling och lagring

suddas ut. *Edge computing* (beräkning längst ut på linan), *fog computing* (beräkning i mellanlager) och centrala (moln)lösningar innebär en distribuerad hantering av data. I kvalificerade plattformar såsom nyare stridsflyg och soldatsystemet implementeras redan idag sådana lösningar för att minska fördröjning, möjliggöra nätverkstrafik och säkerställa behovet av kommunikationens tillgänglighet utanför den egna plattformen och enskilda informationssystem.

Mängden data och information ökar explosionsartat och måste hanteras. Trots den överväldigande mängden data är tillgången till data med höga informationsvärden fortsatt begränsad. Därutöver finns särskilt skyddsvärda data såsom biologiska data, planer, vissa algoritmer, signaturer samt data för att träna system. Resonemanget gäller såväl rena data som metadata. I en splittrad värld med skilda perspektiv avseende integritet är det oklart om det kan förutsättas att *open source*-data fortsatt är en lika tillgänglig och användbar resurs mot framtiden.

Att skilja på data, dvs. avgöra om den är verklig eller syntetisk, äkta eller falsk, blir allt svårare. Detta ställer krav på teknisk infrastruktur och på informationssystemen. Människan behöver hjälp av tekniken. Vi behöver även hjälp med att ifrågasätta våra egna förutfattade meningar och få alternativ till lösningar. Även här kommer AI-verktyg att kunna bistå.

Tekniken möjliggör hybrida hot i form av exempelvis påverkan, störning och subversion. Hoten från informationspåverkan ökar och att särskilja autentisk information från AI-genererat innehåll blir avgörande när fientliga aktörer enkelt kan sprida sitt narrativ i form av exempelvis röstkloning och syntetiska videor (*deepfakes*). Informationsoperationer påverkar både barn och vuxna, i såväl fred som under krig. Icke-fungerande GPS kan ge mycket stora effekter på civil verksamhet redan idag. Samhället påverkas genom störningar i flöden, förstörelse av samhällskritisk infrastruktur och organiserad brottslighet. Datainsamling av fientliga aktörer samt cyberhändelser är hot mot både individer och samhälle. Det väpnade kriget är en del av konfliktspektrumet, men det finns omfattande verksamhet och militära tekniker som kan användas utan att nå över tröskeln till krig men ändå orsaka stor skada på samhället och nationens skyddsvärden.

Automatisering, robotik och nya tillverkningsmetoder ger bättre produktionsförutsättningar. Att tillräckligt snabbt utveckla och tillverka produkter bedöms även fortsättningsvis vara en utmaning. Det är en industriell fråga men också en forskningsrelevant och politisk frågeställning som går utöver den tekniska forskningen. Det handlar exempelvis om att snabbare omsätta forskningsresultat till produktion, att effektivisera validering och verifiering och om att säkerställa en tillräcklig produktionskapacitet.

Mot 2050 finns än fler sensorer i alla militära domäner, men också i samhället i stort. Sensorerna är placerade närmare de verkande systemen, är multifunktionella och finns även på en hög och strategisk informationsnivå. Transparensen är troligen

här för att stanna, liksom de medel som försöker påverka och modifiera andra aktörers lägesbilder. Duellen mellan medel och motmedel blir allt mer komplex och kan, särskilt under konflikter, ha ett mycket högt tempo.

Samtidigt finns det motkrafter till sensorutvecklingen, till exempel i form av utvecklingen av nya material som kan ges unikt anpassade egenskaper som kan bidra till att minska systems signaturer. En del av denna utveckling går ut på att dra lärdomar från lösningar i naturen, så kallad biomimetik. Andra är att dölja sig i brus, att störa system samt att aktivt förmedla falsk information.

Trots ett överflöd av sensorer och information kan det därför bli svårt att veta vad som faktiskt händer. Artificiell intelligens finns i princip överallt för att hantera informationsflödet och ge mänskliga beslutsfattare en hanterbar situation utan kognitiv överbelastning. Eller helt enkelt för att fatta beslut utan mänsklig inblandning i de situationer där detta kan ses som etiskt acceptabelt. Gränserna för detta kan skilja mellan olika aktörer.

Redan idag är rymdbaserade förmågor centrala och integrerade med andra domäners förmågor genom system för spaning, kommunikation och navigering. Mot 2050 utvecklas rymddomänen till att bli en än mer integrerad och nödvändig del av krigföringen. Det finns exempel på verkan mot rymd, från rymd och inom rymd och allt tyder på att alla dessa former kommer att bli vanligare i framtiden. På lång sikt kan också mänskliga kolonier etableras och utvinning av råvaror i rymden bli en realitet. Det går inte att utesluta existensen av baser på månen 2050 och inte heller bemannade rymdfärder till Mars och kanske ännu längre bort i rymden. År 2050 kan den så kallade GEOINT-singulariteten ha uppnåtts, vilket innebär att varje punkt på jordytan kan observeras när som helst. Detta tillsammans med omfattande utveckling inom sensorområdena i domäner andra än rymd, datafusion och smart beräkning av sensordata är en anledning till att transparensen skulle kunna bli ett normaltillstånd på det framtida stridsfältet.

Det saknas idag egentlig reglering avseende rymden som krigföringsdomän. Mot 2050 har troligen fler aktörer än idag tillgång till rymdförnekande system såsom mikrovågsvapen, cyber, laserbländning, telekrigföring, manövrerande satelliter och ballistiska robotar. Rymdens betydelse ökar också för övriga domäner och rymddomänen blir en än mer integrerad del av operationsmiljön.

Arbete har redan idag inletts mot att uppfylla behoven av egen svensk rådighet i rymden, genom utveckling av rymdbaserade system och rymdbaserad förmåga. Till rymddomänen räknas ofta även höghöjdsplattformar i gränslandet mellan satellit och flyg. De har betydelse för positionering, navigering och tid (PNT), kommunikation och spaning. Samtidigt kommer beroendet av rymdbaserade tjänster för PNT (GNSS) sannolikt bli mindre då särskilt kvantteknik kommer att medge högre noggrannhet hos tröghetsnavigering, en noggrannhet som dessutom kan ökas genom kombination med fixpunktsnavigering.

Samhället, människan och militär verksamhet förändras i ett samspel. Säkerhetspolitisk utveckling, teknikutveckling samt förhållningssätt till regelverk och användning förändras över tid. Det har under lång tid rått ett allmänt synsätt om icke-användning av kärnvapen och biologiska och kemiska ämnen. Detta har flera gånger utmanats, såsom vid användning av kemiska ämnen i konflikter och mot individer. Mot 2050 spås bioteknik utvecklas snabbt och erbjuda en bioteknikrevolution som kan ge disruptiva, och kanske skrämmande, konsekvenser. Trots att utvecklingen huvudsakligen drivs av civila aktörer innebär de hot som möjliggörs, genom den framtida utvecklingen inom BC-området, att vissa omtag i försvarets skyddsverksamhet blir nödvändiga.

Mot 2050 kan synsättet på liv komma att utmanas genom möjligheter att i grunden förändra biologin, och därmed människan och andra levande system. En allt bättre förståelse för hjärnan, medvetandet och kognitionen kan också innebära banbrytande genombrott och kanske även leda till bättre minneschip och processorer för beräkningskapacitet. Tillämpning av ny bioteknik och bioelektronik är ett i vissa delar oreglerat område där synsätt om användning varierar globalt. Teknikutvecklingen kommer att ge många möjligheter att förstärka människan såväl fysiskt som kognitivt. Här kommer den etiska debatten att vara livlig.

Kvanttekniken ger potential för omvälvande förändringar, men det är svårt att förutspå utvecklingstakten och införandetakten. Tillämpningarna har länge sagts kunna inträffa först om cirka 10 år, men är det nu som dessa 10 år faktiskt inte skjuts ytterligare framåt i tiden? För kvantteknik finns fortfarande utmaningar både tekniskt, såsom kylning och robusthet, och vad gäller förståelse av vilka användningsområden som har störst potential. Bland de områden som brukar lyftas fram, och där kvantteknik kan ge ny eller bättre förmåga, finns sensorer, GNSS-oberoende navigering och beräkningar.

Relaterat till diskussionen om disruptiva genombrott och kvantteknikens potential, är det transparenta slagfältets spridning till undervattensmiljön av stort strategiskt intresse. Ökad transparens i världshaven skulle kunna äventyra ubåtars förmåga att verka dolt och därmed potentiellt utmana de system som utgör stormakternas andraslagsförmåga och som är en väsentlig del av kärnvapenavskräckningen. Här finns till exempel potential genom gravitationssensorer, vilka kan möjliggöras genom den kvanttekniska utvecklingen. Räckvidd och känslighet hos dessa och vilka motmedel som kan finnas för att undgå upptäckt är föremål för forskning och studier.

Energiområdet ges mycket uppmärksamhet i rapporten. Mindre och kapablare batterier och andra energikällor gör att små system och plattformar kan ges bättre uthållighet och klimatprestanda. Distribuerade system kan dra fördel av den snabba civila omställningen exempelvis i form av tillgång till elnät och batteristationer för laddning. Försvarsmakten kommer att behöva anpassa sig till den civila utvecklingen, till exempel vad gäller den väntade utfasningen av fossila bränslen, då man till stor

del kommer att vara beroende av civila försörjningskedjor vad gäller sådant som fordonsbränslen. Detta kan innebära ett antal utmaningar. Till exempel krävs, om försvarets fordon ska ställa om till eldrift, att detta kan möta kraven på räckvidd, effektuttag och laddning under fältmässiga förhållanden. Hybridlösningar kommer dock sannolikt att bli allt vanligare. För plattformar som flygplan och större fartyg kommer omställningen av drivmedel att innebära särskilda utmaningar.

Vi ser också att nya hot och tekniska framsteg idag skapar nya nischer för välkända teknologier. Redan på 1980-talet förutspåddes att vapentillämpningar av laser och HPM (*High Power Microwave*) skulle slå igenom och få stor betydelse på 1990-talets stridsfält. Så skedde inte på grund av tekniska utmaningar. Båda dessa vapentekniker är idag istället intressanta för skydd mot drönare och andra mindre vapensystem genom verkan mot elektronik, sensorer eller strukturer.

Beslutsfattande är centralt i militär verksamhet och tillgång till datamängder om det som sker, en uppdaterad lägesbild, och sensorer nära verkanssystem ger ökade möjligheter till delegerat beslutsfattande. Samtidigt kan förekomsten av allt fler gemensamma uppgifter och förmågor ge ökade behov av koordinering och eventuell kommandostyrning. Autonoma system i ledningssystemet (digitala assistenter och agenter), tidskrav och förekomsten av autonoma system i den fysiska miljön ställer människans roll i det tekniska systemet på sin spets. Beslutsstöd på alla nivåer, nyttjande av digitala och fysiska autonoma system, realtidsintegration, sensorernas stora dataflöden med metadatakrav, massiva mängder lagrade data, integration av människa och maskin, autonomi för tillräckligt snabb planering och respons gällande vissa händelseförlopp; allt detta kommer att införas mot 2050 och radikalt förändra sättet att bedriva operationer, utbildning, logistik, reparationer och underhåll. I princip all verksamhet kommer att påverkas.

Mot framtiden kan allt fler uppgifter utföras av obemannade, semiautonoma och på sikt helt autonoma system. Detta gäller både fysiska rörliga system (UxV) och agenter i de digitala systemen. Idag används i Ukraina drönarplattformar från både civila och militära producenter. Tillgängligheten möjliggörs genom låg kostnad och stor volym. Ett exklusivt system har omformats och blivit en civil mängdvara. Men drönaren är inte ett enhetligt system. En drönare kan se ut på en mängd sätt och bär allt som oftast teknik och materiel som sensorer, granater eller kommunikation, och nyttjas för logistik och transport. Även dessa typer av drönare har blivit billigare, lättare och mindre och finns till del på den civila marknaden. Materielen sammantaget ger drönarens effekt.

Utvecklingen mot en större andel obemannade och autonoma system är redan påbörjad och kommer att fortsätta i samtliga fysiska domäner. Fler roller kommer att tas över av obemannade, och på sikt autonoma, system. Exempelvis kommer kombinationer av autonoma system vara en lösning för att hantera framskjuten logistik

även under hög hotnivå. De obemannade och autonoma systemen kommer också att fungera i nära samverkan med bemannade system, soldater och beslutsfattare.

Försvarets utformning och nyttjande av teknik sker både reaktivt och väl övervägt. Beslut om och val av teknik påverkar framtida förmåga. Valmöjligheterna avseende system, kvalitet och kombinationsmöjligheter kommer i perioden mot 2050 att bli markant fler. Teknikområden flyter samman och tekniker kan kombineras på oväntade sätt. Vissa förmågor kan lösas nationellt medan andra kräver samverkan med andra stater.

Sammantaget är det omöjligt att idag veta vilka framtida tekniker som kommer att ge upphov till omslagspunkter där helt nya saker kan göras, gamla saker kan göras på nya sätt och barriärer kan passeras. Det finns dock potential för sådana tillämpningar inom flera teknikområden, men om dessa rent praktiskt kommer att kunna realiseras, eller huruvida de är kostnadseffektiva, är idag inte möjligt att bedöma. Artificiell intelligens, kvantteknik och bioteknik är tre teknikområden som är troliga kandidater för omslagspunkter. Den första kan på sikt ge en förmåga i klass med eller överlägsen den mänskliga intelligensen, den andra kan genom att använda kvantfysikens paradigm ge upphov till många tillämpningar bortom vad som är möjligt idag, medan den tredje ensam och tillsammans med andra teknikområden kan komma att förändra innebörden av liv, kognition och människan som system. Det skulle kunna innebära en värld där mänsklig kognition är sammankopplad med syntetisk beräkning, där celler används för att ge fysisk form till digitala assistenter och soldater ges bättre perception. Även om denna utveckling inte är trolig till år 2050 så kan den vara möjlig på längre sikt.

## Diskussion

I Del 1-3 finns mycket information om framtida utveckling och faktorer som påverkar tekniken. Mot denna bakgrund diskuterar vi nedan ett antal områden som vi finner centrala då de har inverkan på och påverkas av den militärtekniska utvecklingen. Det handlar om samverkan och försvarsforskningens roll i försvarssystemet, hur krig påverkar teknikutvecklingen och utmaningen att hantera konvergenser. Antologin redovisar en tekniskt otaktad utveckling och en organisation som måste vara oerhört förändringsbar, men där organisationen utgörs av strukturer som traditionellt utformats för längre livscykler. Vi diskuterar utmaningen med att förstå framtiden och namnsättning av den nya tekniken och materielen. Människans centrala roll i systemet och aspekter av fysiskt och digitalt kommer att genomsyra försvaret mot framtiden; det påverkar verksamhet, planering, ekonomi och organisationen i stort. Innan de avslutande kommentarerna lyfter vi vikten av framsyn i en tid av snabb förändring och stora osäkerheter.

## Rådighet, samverkan och integritetskritiskt

Den strategiska styrningen av försvaret, för Sverige enskilt, i koalition och i allians med andra, är av stor betydelse. Den beror av den säkerhetspolitiska kontexten, nationella prioriteringar avseende försvarsförmågor, internationella relationer och ekonomiska intressen. I detta innefattas integritets- och säkerhetskritiska kompetenser, nationella försvarsindustriella intressen, tillgång till råvaror, delning av data, infrastruktur, samt försörjningstrygghet och produktionsförmåga. Viss teknik har Sverige förfogande över, medan annan har externa beroenden.

Med utgångspunkt i dagens förutsättningar har under de senaste åren arbetsformer och samarbeten som fanns inom det kalla krigets försvar till del återinförts. Samverkan mellan myndigheter, näringsliv, akademi och andra aktörer som är centrala för försvaret utvecklas successivt. Samarbeten och försöksverksamhet gagnar samtliga aktörer. Det är även ett sätt att genomföra kunskapsöverföring från forskningsverksamheten till användare och andra intressenter.

Balansen mellan civilt inriktad verksamhet med mervärden för försvar och den rent militära produktionen kommer förmodligen att fortsätta skifta i takt med tekniska genombrott. Det är ett samspel där även militärt finansierad forskning ger avkastning in i civil produktutveckling. Längs vägen mot 2050 blir samverkan mellan aktörer förmodligen än mer nödvändig.

Den av försvaret finansierade forskningen har stor betydelse för militär förmågeutveckling. Försvarsforskningsprogram har generellt sett långa livscykler. Exempel på program med långa tidshorisonter och hög risk finns hos amerikanska aktörer som DARPA[344] och IARPA[345]. I större och militärtekniskt framstående nationer finns institut och industrier inriktade mot för försvarets kritiska kompetens- och förmågeområden. Den försvarshemliga forskningen kommer fortsatt att vara av betydelse för framtida militär förmåga. Några exempel på sådana områden är kärnvapen, hypersoniska vapen och skydd mot dessa, samt cyber, telekrig och signaturanpassning i samtliga domäner på det alltmer transparenta slagfältet. Rymddomänen bidrar till teknikutvecklingen i stort.

Den försvarshemliga, långsiktiga och kvalificerade forskningen kommer troligen att bidra till framtida disruptivitet. Sådan utveckling drivs av stater med rådighet över kritiska resurser såsom forskning, kunskap, material och produktion.

Ett tekniskt kompetent land som Sverige har nischområden med spets. Inom dessa väljs samarbeten med omsorg och nischområdena kan också öppna för samarbeten inom andra teknikområden. Globalt pågår en maktkamp om tekniskt kunnande

344 Defense Advanced Research Projects Agency. DARPA är ett oberoende forskningsinstitut inom det amerikanske försvarsdepartementet med uppdrag att bedriva och finansiera forskning i syfte att utveckla kvalificerad teknologi för militära ändamål.

345 Intelligence Advanced Research Projects Activity är en organisation som ansvarar för att leda forskning för att övervinna svåra utmaningar som den amerikanska underrättelsetjänsten står inför.

inom områden som AI, bioteknik, materialteknik och nanoteknik. Det går inte att bortse från satsningar som görs av stater för att i framtiden bli teknologiskt överlägsna. Viss teknikutveckling kommer även att gå under radarn och kunna bidra till att en nation får ett styrkemässigt övertag i morgondagens konflikter.

De omfattande försvarssatsningarna och den globala teknikkonkurrensen mellan främst USA och Kina kommer att bidra till att påskynda tekniksprång och korta ledtiderna från idé till system. Det gäller för oss att hänga med, åtminstone inom strategiska områden. Samtidigt är det en utmaning att samverka, särskilt utanför försvarssektorn, utan att i någon mån riskera att integritetskritisk kunskap hamnar i fel händer. Då samarbetena är nödvändiga är det viktigt att de kombineras med ett utvecklat säkerhetsskyddsarbete.

## Krigets betydelse för teknikutveckling

Den framtida operationsmiljön bedöms bli mer omfattande. Den fysiska miljön täcker större geografiska områden och har en högre detaljupplösning. Den virtuella verkligheten är redan idag en framträdande del av slagfältet och samhället. Datamängderna ökar och möjligheterna till kartläggning och kognitiv påverkan skulle kunna bli nästintill obegränsade givet att tillgång till data inte begränsas. Den tekniska utvecklingen möjliggör dessutom samtidiga konflikter i de fysiska, virtuella och kognitiva dimensionerna.

Varje konflikt har sin egen karaktär. Traditionell militär materiel och metod kombineras med enklare och påhittiga lösningar i Ukraina. I media uppmärksammas drönare i stor kvantitet från civil industri, konstellationer av satelliter för kommunikation i låg bana, applikationer på mobiltelefoner, allt billigare och mindre sensorer och hot mot kärnkraftverk och mycket mera. I andra konflikter finns andra medel och miljöer. Allt handlar dock inte om teknik och konflikters karaktär beror av kontext. Befintligt kombineras med nytt i en kamp där förutsättningarna för manöverkrigföringen förändrats i grunden.

Hot mot samhället finns redan idag om än på en nivå som inte innebär väpnat angrepp. Denna hybridkrigföring möjliggörs i allt högre utsträckning i framtiden med teknik och militära medel som kan ha stor effekt på sårbara system.

Delar av stridsfältet är idag otillgängliga för människan. I dessa zoner är det mycket svårt att undgå upptäckt eller bekämpning. Konsekvenser av det transparenta slagfältet, drönare, plattformar och logistikens betydelse har studerats teoretiskt. Ändå överraskas vi av verkligheten. Liksom i tidigare rapporter beskrivs i denna antologi trender såsom ökad hastighet, räckvidd, kvalitet, precision, transparens och snabbare uppdatering av lägesbilden. Dock har relevansen av kvantitet, uthållighet, utbildning och produktion stärkts i författarnas beskrivningar i förhållande till tidigare rapporter.

Antologin blickar framåt och ett väl etablerat synsätt som bekräftas av pågående händelser är att ny teknik och materiel inte innebär att allt det gamla är obsolet. Den metod och materiel som ger effekt kommer att leva kvar och utvecklas och kan användas på nya sätt tillsammans med helt nya typer av materiel och metoder. Det är en risktagning att ta bort något fungerande. Istället existerar system från olika tekniska generationer och bara det som tydligt blivit obsolet fasas ut.

Dagens utmaningar har stor koppling till transparens och risk att upptäckas och bekämpas. Omfattande användning av drönare är ett nytt tillvägagångssätt som ger möjlighet till aktioner på djupet av motståndarens territorium på nya sätt. Men även drönaren har genomgått en gradvis utveckling som startade långt tidigare. Exempelvis fanns militärt framtagna mindre drönarplattformar för spaning redan under 1990-talet och var redan då relativt kvalificerade militära system. Resonemang om allmänt tillgängliga produkter, exklusivitet, kvalitet, kvantitet, robusthet för militära miljöer, effekt och livslängd är exempel på faktorer i långsiktiga arbeten om teknik och framtida militär förmåga.

Ledningssystem är en infrastruktur som bland annat tillhandahåller dataflöden, beräkningar och lagring för den kommande autonomin, där inte nödvändigtvis människan är mottagare av informationen. AI-agenter kan fatta beslut om exempelvis skydd mot snabbt inkommande hot. I det uppkopplade samhället finns militära och civila system som kan fungera som sensorer och länkar. En frågeställning, som är aktuell redan idag, är att avgöra vilka data som kan och får samlas in, hur dessa får sammanställas och användas, vem eller vad som får och bör agera på informationen, under vilka premisser och med vilken typ av lägesbild som stöd.

## Försvarskoncept påverkar utvecklingen mot framtiden

Krig driver militär förmågeutveckling, där bland annat doktrin, metod, organisation och materiel förändras. De uppgifter som försvaret har att lösa enskilt, som del av koalition och i allians, både inom en nära framtid och på längre sikt, innebär nya typer av ansvarstaganden och inriktningar. Dessa uppgifter, och de försvarsförmågor de kräver, utgör utgångspunkter för val om militär teknik och materiel och påverkar därför forskning och utveckling, nationella kompetensområden, produktion och exportkontroll. Försvarsmaktens arbeten med försvarskoncept och utveckling bidrar till utformningen av det framtida försvaret och hur uppgifter blir lösta.

Totalförsvaret är ett nygammalt koncept som åter utvecklas för dagens och morgondagens behov. Kanske innebär det tekniktäta samhället, behovet av nationellt försvar mot störningar och de uppgifter som Sverige nu har i Nato, att försvarsförmågan kan stärkas genom en mer omfattande samverkan mellan centrala civila aktörer och delar av det militära även inom Sverige.

Nato och västlig syn påverkar svenskt försvar mot framtiden. Nato strävar mot att alliansen ska ha en teknisk fördel gentemot potentiella motståndare. Utvecklingen

drivs mot multidomänoperationer (MDO) där verksamheten ska genomföras samordnat i alla domäner (mark, sjö, luft, rymd, cyber). Därutöver ingår synkronisering med andra (civila) aktörer i konfliktområdet. Vår strävan är att i denna antologi beskriva en tid och utveckling som tidsmässigt ligger efter det att MDO införts.

En stor del av teknikområdena i denna antologi drivs av såväl konceptuell strävan mot MDO som av att de är kritiska förutsättningar för att nå den tekniska funktionalitet som krävs för ett väl fungerande MDO. Till 2050 kommer sannolikt MDO tas vidare mot nya koncept och begrepp. Det finns utmaningar gällande samsyn om teknik, regelverk och nationella intressen. Helt oavsett kommer behovet av samverkan både inom och mellan militära domäner, mellan nationer, i allianser och med övriga delar av samhället att kvarstå.

Sveriges försvar utvecklas mot både kortsiktiga och långsiktiga behov. Den säkerhetspolitiska situationen innebär att försvarsverksamheten måste prioritera arbete med ett kortare tidsfokus på grund av ett akut tillväxtbehov.

Det är och kommer fortsatt att vara en balansakt att fatta beslut för långsiktiga förändringar utan att tappa befintlig förmåga på vägen. Vi behöver bibehålla blicken mot de långsiktiga utmaningarna även när de kortsiktiga är åtskilliga, komplexa och kräver snabba beslut. Teknikutvecklingen innebär att uppgifter kan lösas på nya sätt, att ny materiel driftsätts och att krigföringen utvecklas.

## Människan i systemet

Försvarsmakten består av en mängd förband med olika specialiseringar, kompetenser och materiel. Personal är en värdefull resurs. Utifrån texterna i antologin framträder en teknikberoende verksamhet där tekniken även till del ersatt personal. Personalen är dock fortsatt i centrum av systemet. Individerna ska kunna verka i en miljö som sträcker sig från full tillgång till mycket avancerad materiel och kvalificerad information, till situationer där tekniken är kraftigt begränsad eller helt otillgänglig. Detta ställer höga krav på personalen.

Försvarsmaktens personal utbildas, tränas och övas för att kunna lösa uppgifter anpassat efter kontexten i stressade och farliga situationer. Oavsett införande av autonoma system, bättre beslutsstöd och lägesbilder kommer människan fortsatt att ha en väsentlig och gränssättande betydelse inom försvaret. Däremot kan människans roll stå inför en genomgripande förändring i takt med att artificiell intelligens får allt större genomslag i samhället.

I antologin, liksom i den offentliga debatten, lyfts legalitet och etik fram som viktiga faktorer vid utveckling av framtidens försvar. Ofta diskuteras enskilda verkansmedel utifrån hur beslut fattas, vilket gör människans roll i framtida krig central. Framtidens system och processer kommer att skilja sig från dagens. Interaktionsytor och interaktionssätt med digitala system kommer att förändras. Mot 2050 kan även

människan som biologiskt system vara föremål för förändring. Vad det innebär att vara människa kan komma att förändras i takt med att tekniker för att läka, förbättra och interagera med våra biologiska system utvecklas, vilket innebär ännu fler etiska utmaningar.

Tekniska framsteg inom bioteknik, materialteknik och mänsklig (kroppslig och kognitiv) förstärkning kan både förstärka de mänskliga sinnesintrycken och förändra människans prestationsförmåga. Även om juridiska och etiska ramar begränsar möjliga användningsområden, kan olika aktörer ha väsentligt skilda uppfattningar om vad som är acceptabelt. Detta gäller såväl i vardagliga sammanhang som för militär användning. Detta är en stor utmaning i alla typer av konflikter och något att beakta i planeringen för att möta framtidens hot. Liknande resonemang gäller autonoma system, men där också med en stark koppling till var och hur beslut om vapeninsatser tas.

Uppgifter som idag utförs av människor kommer i ökande grad att automatiseras. Förvaltning och stabers uppgifter kommer att effektiviseras, och både organisation och arbetssätt förändras. I såväl fysisk som digital miljö kommer helt eller delvis autonoma system (robotar) att lösa uppgifter som idag utförs av människor. Personalen är dock central för att utforma och driftsätta en autonom verksamhet.

Frågan om vad som kan och bör automatiseras är central mot framtiden. Kraven på människans förmåga att interagera med maskiner och digitala assistenter kommer att öka, liksom kraven på att det digitala ska fungera som ett effektivt stöd för människan. Detta gäller särskilt bland annat i tidspressade situationer och vid hantering av omfattande datamängder. Militär verksamhet kommer fortsatt att kräva mycket kompetent och anpassningsbar personal.

Automatiseringen är nära kopplad till ledning. Människans roll i det militära systemet förändras kontinuerligt. Teknikutvecklingen skapar mervärden men det är människan som väljer var och hur intelligenta system kan och får användas. Människans centrala roll för ledning och lösande av uppgifter i krig, även i situationer med hög belastning och betydande risker för individen, kommer att bestå. Dock kommer allt fler uppgifter att delegeras till AI-agenter och autonoma system.

Digitaliseringen innebär att ledningssystemen och dess datamängder kan användas av fler aktörer och kan stödja fler verksamheter, både inom och utom Försvarsmakten. Digitalisering ger tillgänglighet och minskar fysiska beroenden, vilket skapar nya sätt att interagera med den del av Försvarsmaktens personal som inte är kontinuerligt tjänstgörande i organisationen. Med digitalisering kan kvalificerat lärande genomföras på nya sätt i en verklighetstrogen simulerad miljö, även på distans.

## Konvergens och begreppsbildning för det nya

Antologins texter visar på konvergens mellan olika teknikområden. Med konvergens brukar förstås att utvecklingen inom områden samverkar, möjliggör och förstärker varandra. Konvergens gäller inte bara teknikområden utan återspeglas också i beroenden mellan försvarsaktiviteter, aktörer, teknik- och systemutformningar och organisationer. Det är konvergens av flera olika typer, i flera olika lager. En utmaning är att än mer och på nya sätt koppla samman olika teknikområden, utövare och förmågeområden utan att för den delen skapa något ohanterligt och alltför komplext.

En aspekt av teknisk konvergens som vi brottats med är namnsättning och en gemensam förståelse av funktionaliteten hos det nya. Det kan vara behäftat med risk för missförstånd att diskutera något som ännu inte finns, eller som är under utformning.

Vi lyfter här några exempel. Drönare är ett exempel på namnförvirring. De har funnits en längre tid och deras utveckling kan jämföras med de klassiska plattformarnas. Drönare är plattformar som kommer i många olika skepnader. De har fundamentalt olika kvaliteter och sårbarheter, kan bära olika system och leverera olika effekt. Därutöver kan drönare vara obemannade, semiautonoma och autonoma. Ibland används begreppet plattform synonymt med drönare. Begreppet plattform har dock traditionellt använts för exempelvis stridsflyg, stridsvagnar och fartyg. Beroende på utgångspunkt omfattar begreppet drönare allt från mycket små plattformar till plattformar av betydande storlek.

Drönare används i alla domäner, för en rad funktioner och deras utformning varierar. De kan till exempel vara flygande system med vingar eller rotorblad, eller markgående system där rörligheten möjliggörs av hjul, band eller annat. Drönaren är en plattform för de system som monteras på den och som bidrar till dess funktionalitet. Det gäller spaning, kommunikation, logistik, bekämpning och så vidare. Variationen är enorm och funktionaliteten i militärt utmanande miljöer kan skilja sig markant åt.

Samma system kan användas av flera olika vapenslag och försvarsgrenar. En mindre flygande drönare som tillhör armén finns i luften, en mindre sjögående enhet kan tillhöra hemvärn eller markförband och en markgående plattform kan användas för bevakning av flygbas. Graden av autonomitet i vissa funktioner eller för styrning av drönaren (uppgiftsautonomitet) påverkar behovet av organisation, personal och stödsystem.

Drönare har så fundamentalt olika egenskaper att det snarare handlar om mängder av olika typer av plattformar men som ibland ges samma arbetsnamn. Så vad är en drönare egentligen? I tider av snabb utveckling krävs sätt att namnge, eller specifikt beskriva, framtidens system funktionsmässigt. Prestanda och kvaliteter för ”drönaren” avseende plattform, autonomitet, störskydd, räckvidd, miljötålighet och så vidare behöver beskrivas tydligare. De måste sättas i relation till de miljöer och

uppgifter de är avsedda för. Här behövs en utvecklad begreppsanvändning och klargöranden avseende funktionalitet, kvalitet och kapacitet. Resonemanget har bäring på civila system som modifieras för militärt bruk och för system specifikt utformade för militär verksamhet.

Verkansmedel är ett annat exempel på otydlig namnsättning och som också knyter an till drönare. Räckvidd, precision och skydd har förändrats i och med drönare och nyare kvalificerade verkanssystem. Idag och mot framtiden överlappar effekter av vissa verkanssystem. Det kan gälla artilleri, fjärrstyrda flygfarkostsystem, hypersoniska robotar, kryssningsrobotar, granater och minor. Däremot skiljer sig kvalitet och exklusivitet, systemkomplexitet, tillförlitlighet, kostnad och beroenden av förutsättande system åt mellan de olika verkansmedlen. Även de organisatoriska och logistiska faktorerna varierar.

Samma resonemang kan föras för andra områden där system förbättras, tillförs helt ny prestanda eller kombineras till multifunktionella system. En förstärkt människa är kvalitetsmässigt långtifrån ett enhetligt begrepp. Vi ser en konvergens med delvis oförutsägbara resultat och där namnsättning och gemensam förståelse är en utmaning.

## En tidsmässigt otaktad teknikutveckling

Teknikutvecklingen är inte linjär. Den kan både ta enorma steg, och då möjliggöra disruptiva tillämpningar, eller stanna av under kortare eller längre perioder när problem uppstår inom forskning eller tillämpning. Ett exempel på detta är så kallade AI-vintrar, ett annat den stora tilltron till att HPM- och laservapen skulle få stora genombrott redan under 1990-talet. I det senare fallet blev det inte så, men dessa vapensystem är på väg tillbaka bland annat på grund av den explosionsartade ökningen av antalet mindre drönare på stridsfältet.

Ett område som för några år sedan betraktades som intressant var kvantradar, men den bedöms inte längre vara intressant utifrån det militära förmågeperspektivet. Sådana inbromsningar eller teknikvintrar kommer att inträffa även framöver.

Teknik och materiel utvecklas i varierande och ojämförbara hastigheter och har olika livslängd. Realisering av det tekniskt omogna behöver inte ligga långt bort i tid, samtidigt som det tekniskt mogna kan ligga långt bort från produktifiering.

Komplexa system finns på och mellan samtliga nivåer och organisatoriska enheter i hela Försvarsmakten. De är intrikata system av system där soldatsystemet, ubåtar, ytfartyg, stridsflyg, spaningsflyg, stridsvagnar och verkanssystem klassiskt räknats som de effektgivande medlen i krig. Dessa system innebär stora och långsiktiga investeringar i vilka även ingår integrerade digitala funktioner och ledningsstöd. Dessa kan sägas gå både på bredden och höjden i organisationen och är numer, och än mer mot framtiden, integrerade delar av plattformar med lång livslängd. Vissa

produkter såsom specifika mjukvaror kan vara utdaterade ett år eller mindre efter inköp, medan ett fartygsskrov troligen har en livslängd om minst 20 år.

## Teknik i organisation och förband

I antologins texter beskrivs både fysiska och digitala plattformar. Det visas på betydelsen av enskilda komponenter såsom en processors kvalitet. Samtidigt är i princip all materiel system av system med interna och externa teknikberoenden.

Mognads- och tidsbedömningar gäller inte enbart teknik. Försvarsmakten agerar genom förband och önskan om snabbhet gäller hela produktionskedjan. Dagens diskussion fokuseras på att tiden måste kortas från forskningsresultat till färdig produkt. En färdig produkt ger inte effekt i sig själv, det gäller även att implementera och uppnå förmåga i övade förband.

Vissa produkter går snabbt att anskaffa och implementera i Försvarsmakten, andra är föremål för långsiktighet och större systemförändringar i organisationen. Kopplingen mellan teknik, materielutveckling, anskaffning, förmåga och effekt är långtifrån linjär. Processer och produktionsprinciper har länge varit anpassade för lägre konfliktnivåer. Tid kan vinnas genom förändrade arbetssätt. Samtidigt måste regelverk efterlevas eller förändras.

Implementering av teknik innebär behov av såväl utvecklade metoder som förändrad organisation. Teknik måste också testas och valideras i rätt miljö. Mängden verksamhet där omogen teknik och kommersiellt tillgängliga produkter testas i labb och i fält har ökat. Det bedrivs verksamhet i gränslandet mellan forskning, utveckling och tillverkning med en bredd av aktörer som samverkar för att korta tid från idé till förbandsimplementerad produkt.

Det svenska försvaret ska kunna möta kvalificerade aktörer i svåra miljöer som förmodligen blir än mer utmanande mot framtiden. Dagens krig visar hur relativt enkel och i vissa fall billig teknik kan ha stor påverkan på klassiska och kostsamma militära system. De enklare produkterna kan dock snabbt bli obsoleta och behöva vidareutvecklas och kompletteras för att klara den militära miljön. Vi kan således behöva arbeta med olika utvecklingsparadigm parallellt och integrerat.

## En alltmer digital organisation

En utmaning med koppling till AI är den snabba civila förändringstakten inom informations- och kommunikationsteknikområdet (IKT). Jämfört med andra områden, såsom klassiska plattformssystem, rusar utvecklingstakt, omsättningstakt, behov av systemförändringar och modifierbarhet inom IKT-området. Såväl hård- som mjukvara utvecklas snabbt, men mjukvara har en helt annan karaktär än fysisk materiel och kräver en organisation som kontinuerligt vidareutvecklar och

uppdaterar systemen. Under senare tid har en diskussion om rådighet över digital infrastruktur tagit fart, vilket även diskuteras i antologins IKT-kapitel.

Arbetet med att införa obemannade, semiautonoma och autonoma system kommer att fortsätta. I och med detta kan kostnaden för den digitala infrastrukturen komma att öka markant. Autonomi, AI-agenter och digitala system existerar och används i en kontext. Digitalisering kräver anpassning av personalens kompetens, samt personal för att tillhandahålla digitala tjänster och system. Aspekter såsom sekretess, organisationens utformning och kultur samt teknikens mognad innebär en resursmässig balansering med förbandens övriga materiel, personal och utbildningssätt.

IKT-områdena utgör en förutsättning för ledning och genomförande av operationer, men också för förvaltning samt för förmågeskapande aktiviteter såsom övning, träning, utbildning och utveckling. Funktioner och flöden skär tvärs igenom organisationen och kan mot en nära framtid liknas vid sammanfogade lager av nätverk.

Digitalisering är en genomgripande verksamhet och inom flera områden är Försvarsmakten sedan länge en digitaliserad verksamhet. Detta gäller bland annat plattformar som JAS Gripen, informationskedjor för bekämpning, träningsanläggningar och simulatorer samt förvaltningssystem. Försvaret har en rad IKT-system som integreras och har olika sätt att dela information. Digitaliseringen som nu pågår sammankopplar olika strukturer. Det pågår omfattande arbeten för att nå tillräcklig och effektiv interoperabilitet för MDO.

Digitaliseringen drivs idag av behov såsom bättre förvaltning, träningssystem och operativ förmåga. En digital transformation innebär att strukturer och materiel som tidigare varit oberoende vävs samman. Data tillgängliggörs, kan hämtas och delges mer obundet av organisationen och kan nyttjas mellan verksamhetsområden på olika nivåer. Samma data kan komma att användas inför, under och efter genomförande av operationer (förmågenyttjande), för utveckling och anskaffning (förmågeskapande) samt i kombinationer av förvaltnings- och insatssystem (logistik och underhåll). IKT innebär, frånsett säkerhet och regelverk, minst tre större utmaningar:

- Omhändertagande av de möjligheter digitaliseringen kan ge, utan att vara låst vid gamla tankemönster och verksamhetsområden.
- Förändring av såväl förvaltnings- som utvecklingsprocesser i relation till materielsystemen, då åtminstone delar av IKT-systemen har andra utvecklings- och livscykler än traditionella materielsystem.
- Tillhandahållande av tillräckliga IKT-tjänster i operationsområden, för att leda operationer och merutnyttja data för exempelvis planering och förbättring av materiel och metod.

Det finns många frågeställningar i och med digitalisering. En som återkommer är risker för verksamheten i balanseringen mellan tillgänglighet och sekretess, en annan hur IKT, AI och tillhörande organisation ska hanteras i de traditionellt sett förbands- och plattformsbaserade underlagen avseende ekonomi och livscykelkostnader. En tredje frågeställning är synsättet på informationsbehov och vad som är avgörande för den tekniska och organisatoriska strukturen.

## Hur planeras och resurssätts den framtida Försvarsmakten?

Beroenden mellan teknikområden, olikheter i utvecklingsparadigm samt fundamentalt ojämförbara livscykler hos komponenter i materielsystem har fått oss att reflektera över hur detta kan påverka planeringen inför försvarsbeslut. Idag ser vi en del förenklade resonemang där det skulle behöva tas större hänsyn till framtida materiels karaktär och beroenden. Viss materiel kommer fortsatt ha långa livscykler där utveckling och produktion tar tid. Andra tekniker och komponenter har en mycket snabb omsättning men kan genom kvantiteter och mängder av objekt ses som större system. Detta innebär att materielsystem i ökande omfattning innehåller flera delsystem med sinsemellan olika uppdaterings- och omsättningstakt.

Utbildnings- och träningssystem kommer att ha en starkare koppling till operationer och insatsverksamhet. Viss materiel är specifik för Försvarsmaktens krigsförband, annan kan vara del av såväl utbildnings- som krigsförband samt förvaltande verksamhet. Detta kan innebära utmaningar avseende beräkningar av kostnad för det framtida försvaret. I tider där teknik och metod snabbt förändras kan planering och allokering därutöver behöva kontinuerliga omtag. Viss materiel och förmåga kan planeras långsiktigt, medan annan bättre införs inkrementellt och med flexibilitet.

## Varför blicka framåt när säkerhetsläget är kritiskt idag?

Den inneboende utmaningen med att blicka framåt är att inte låsa sig vid befintliga koncept, förutsättningar och utformning. Det befintliga är utgångspunkter som kan kombineras med nytt innehåll, eller förändras för att anpassas bättre mot framtiden. Till följd av den säkerhetspolitiska situationen vi ser idag har försvarsverksamheten i mångt och mycket inriktats mot en relativt kort tidshorisont. Det pågår omfattande arbeten såväl med att nyttja civil teknologi och produkter, som med att påskynda införande av ny materiel till försvaret. Förändringen grundas i ett akut tillväxtbehov.

Det är en utmaning att samtidigt växa snabbt och omhänderta behov som säkrar investeringar mot framtida hot och utmaningar. Framsynsarbeten genomförs bland annat för att minska risken att bli överraskad, att vara proaktiv, att skapa hållbarhet och undvika felinvesteringar. Det kan innebära att avvakta eller att fatta successiva beslut för att bibehålla flexibilitet och anpassning. Arbeten om framtiden kan ge oss bättre förutsättningar att förbereda oss, både mentalt och rent praktiskt,

mot det som kan komma. Att skapa och värdera utfallsrum samt att ge underlag för agerande tillräckligt tidigt är en central roll för framsynsarbeten. Snarare än att enbart skapa långsiktiga visioner tas underlag fram i syfte att vara bättre förberedd för nästa eventuella krig och tekniksprång.

Den mänskliga och organisatoriska insikten om vad kommande materiel och teknik kan innebära är avgörande. Vissa av de överraskningar som erfarits i pågående krig är kanske till del konsekvenser av ett konservativt tänkande. Idéerna om det nya ges troligen för lite utrymme i formandet av uppfattningen om hur krig kan bedrivas och vad som är avgörande för effekt. Som exempel förändras såväl materielsystem som metoderna snabbt i Ukraina.

Kunskap från forskning används för att förbättra befintlig materiel och förmåga samt för att stödja strategi och beslut mot framtiden. Insikterna om framtiden omsätts i verksamhet men har en tendens att kopplas samman med de formella och i tid utdragna processerna för forskning, materielutveckling och anskaffning. Den forskande och långsiktiga verksamheten bygger kunskap och skapar insikter om möjliga, mer eller mindre sannolika, utvecklingar. Framsynsunderlag kan både visa prov på framtida verksamhet och tillämpning som är lätt att acceptera och sådan som omstörtar synsätt på uppträdande, organisation och förmåga. Det handlar om att skapa nytt och att erhålla en mental förberedelse. Förmodligen kommer den ordinarie verksamheten alltmer samverka med forskning och utveckling för att omhänderta de möjligheter och utmaningar som en snabb teknikutveckling kan föra med sig.

## Avslutande kommentarer

I denna antologi har författarna haft som ambition att belysa merparten av den teknikutveckling vi ser som försvarsrelevant mot framtiden. Därutöver vill vi belysa tekniken i en kontext. Vi tar upp såväl omvärldsutvecklingen som betydelsen av korskopplingar mellan teknikområden och aktörer och den påverkan tekniken kan få på processer och organisation.

Det förutspås att dagens varierade och komplexa konfliktspektrum är här för att stanna, där händelser som är svåra att attribuera, under nivån för väpnad konflikt, utmanar samhället och suveräniteten. Den fysiska miljön täcker större geografiska områden och har genom sensorer en högre detaljupplösning som är tidsmässigt uppdaterad. Den virtuella verkligheten är redan en framträdande del av slagfältet och samhället. Datamängderna ökar och möjligheterna till kartläggning och kognitiv påverkan skulle kunna bli nästintill obegränsade givet att tillgång till data inte begränsas. Framtiden kommer att bjuda på en samtidig konflikt i den fysiska, den virtuella och den kognitiva dimensionen.

Vi ser det klassiska och till del nya krigets karaktär och brutalitet i Europa, där effekter av kombinationer av fysisk och digital materiel, modern informationsdelning och användning av drönare och kvalificerade långräckviddiga vapen kombineras med plattformar som i möjligaste mån anpassats för nya hot. Detta i en miljö där människor söker skydd under jord och i befästningar. Det är ett krig där rörlighet, uthållighet och utnötning möts och konsekvenser av den tekniska utvecklingen, som till del påvisats i tidigare rapporter, nu blivit verklighet. Flöden, platser, geografi, infrastruktur, resurser och råvaror, statsskick, tro och åsikter är exempel på föremål för krigföring. Det är teman som är tidsmässigt obundna.

Vi upplever oss idag stå inför en framtid fylld av både möjligheter och hot. Det gäller inte enbart teknikutvecklingen utan även hur den kan användas i fredstid och i konfliktnivåer upp mot ett fullskaligt krig. Samtidigt som det väpnade angreppet fortsätter att vara det dimensionerande hotet, kan vissa av teknikområdena även nyttjas vid andra konfliktnivåer och för andra typer av hot. Att samtidigt hantera den allt större utfallskonen av möjliga utvecklingar och utveckla försvarets operativa förmåga med ett ekonomiskt ansvarstagande kommer fortsatt att innebära avsevärda utmaningar. Teknikernas olika karaktär och utvecklingshastighet kan komma att ställa nya krav på samverkan, förvaltning och ekonomi.

Framtiden bjuder på en omfattande palett av teknik som kan nyttjas för försvarsförmåga. Frågan är vad vi väljer att utveckla och införa. Ett sätt att hantera spännvidden kan vara att behålla fokus på det som ska skyddas, de uppgifter som ska genomföras samt förmågor och processer som stödjer detta.

Tekniken är central för militär förmåga och ska användas såväl i fredstida verksamhet som i krig. Nu, liksom i framtiden, står människan – förstärkt eller inte – i centrum i en digital, fysisk och kognitiv verklighet som alltmer integreras med nya system.

Det kan inte antas att det västliga sättet att se på förmågeskapande och förmågenyttjande är detsamma som hos en framtida motståndare. De hot som kan riktas mot Sverige, och flera av de tekniker som lyfts fram i denna antologi, påverkar såväl samhället som landets försvar. Teknikutvecklingen rymmer legala och etiska frågor där samsyn mellan länder saknas. Det är en oviss framtid vi går till mötes; hur teknik kan komma att nyttjas, om regleringar kommer att införas och huruvida efterlevnad av och respekt för regelverk kommer finnas i samsyn mellan parter såväl i fred som under konflikt.

Hur dagens trender fortsätter mot 2050 är omöjligt att förutspå, än mindre hur de utvecklas sammantaget. Idag finns få tecken som tyder på att den globala maktkampen och de olika synsätt som finns när det kommer till nyttjande av teknik och krigets lagar, inte skulle fortsätta in i framtiden.

Dimensioneringen av försvarets förmåga antas fortsatt behöva inriktas mot att kunna möta en kvalificerad motståndare i krig. Andra fortsatt relevanta uppgifter är bidrag till hantering av hybrida hot och att stödja händelser där civila aktörer

bär ansvar för hanteringen, såsom naturkatastrofer. En frågeställning i sammanhanget är vad Försvarsmaktens mandat och uppgifter kan vara i lägre konfliktnivåer, i en värld av hybridkrig med hot mot territoriell integritet och suveränitet. Därutöver torde hantering av kvalificerade statsbundna aktörer, i närheten av eller inom Sveriges territorium, i en konfliktnivå under krig fortsatt behöva omhändertas i samtliga domäner.

I en tid av osäkerhet är det inte längre en fråga om antingen eller, utan om både och; nu och framtiden, olika tekniker och vapenslag, civilt och militärt. Detta kräver helhetssyn, tankearbete, experiment och strategi. Skyddet av central verksamhet och förmågan att hantera olika typer av händelser är avgörande. Omvärldsutvecklingen kan komma att innebära att synen på vad som ska skyddas, varför och när kan ändras. I detta sammanhang kan tekniken innebära både utmaningar och möjliga lösningar.

Det finns en tilltro till att tekniken kommer att lösa utmaningar, både för försvaret och för samhället i sin helhet. Inom försvaret ses användning av produkter och teknik från den civila marknaden som ett sätt att snabbare öka försvarets förmåga. Stater och aktörer är fortsatt enskilda entiteter men vävs samman i gemensamma intressen och samarbeten. Framtiden kan bjuda på många olika typer av tillämpningar av befintlig och ny teknik, där det är människan som bestämmer spelplanen för hur dessa bäst kan nyttjas för att försvara Sverige enskilt, i koalition och i allians.

Hybrida hot och väpnat angrepp kan i framtiden komma att genomföras med alltmer varierade medel. I antologin visas på teknik som kan användas i enlighet med regelverk, mot regelverk och där regelverk ännu saknas. Försvaret måste förhålla sig till och utvecklas i framkant av teknikutvecklingen, såväl för egen förmåga som för skydd mot befintliga och nya hot. Den kommande 25-årsperioden kan innebära stora förändringar och i denna utveckling måste vi också omhänderta och motivera hur valda tillvägagångssätt förhåller sig till regelverk och riktlinjer. Centralt i resonemanget är de värden som ska skyddas. Därför hoppas vi på en diskussion om vad som ska skyddas samt hur, enskilt eller tillsammans, i ljuset av den tekniska utvecklingen.

FOI

ISSN 1650-1942

www.foi.se