



# VITEN

FORSKNINGSFAGLIG RAPPORT 2. 2016 FORSVARETS FORSKNINGSinSTITUTT



## TEKNOLOGIEN FORSVARET TRENGER

### TEKNOLOGIKAPPLØP

Hva betyr teknologikappløpet for Europa og Nato?

side 16

### KOSTNADSVÆKST

Kan teknologien redusere Forsvarets kostnader?

side 28

### CYBERFORSVAR

Tre store utfordringer med cyberforsvar

side 38



## OM VITEN

VITEN er en ny type rapport fra Forsvarets forskningsinstitutt (FFI).

Den er rettet mot et bredere publikum og er laget i et oversiktlig tidsskriftformat. VITEN kommer i første omgang ut fire ganger i året, og er et ledd i FFIs satsing på god forskningsformidling og -kommunikasjon.

Med VITEN ønsker vi å bidra til en mer opplyst offentlig debatt, med mer forskningsbasert kompetanse, kunnskap og nettopp viten. Temaer for disse rapportene kommer fra hele bredden av FFIs forskning – fra militærtekniske forhold til forsvarsplanlegging, sikkerhetspolitikk og samfunnsikkerhet. I særlig grad vil vi belyse temaer som har betydning for de utfordringene Forsvaret og sivilsamfunnet står overfor. Vi håper at VITEN vil bidra til å vekke interesse for FFIs mange forskningsområder, og vise at forskningen vår bidrar til et bedre forsvar og et tryggere samfunn.

En elektronisk utgave av VITEN ligger på [ffi.no](http://ffi.no), ofte sammen med utfyllende rapporter og annet materiale.

Har du spørsmål om VITEN? Ta kontakt med oss: [VITEN@ffi.no](mailto:VITEN@ffi.no)

## Hva teknologi betyr for Forsvaret

Da FFI ble etablert i 1946, var det i erkjennelse av at den teknologiske utviklingen var og ville være svært viktig for Forsvaret. FFI skulle bidra til moderniseringen av Forsvaret, industrien og det vitenskapelige miljøet i Norge. Det er fortsatt avgjørende å henge med i den teknologiske utviklingen. Bare slik kan vi utvikle et relevant forsvar. Det vil si et forsvar som kan møte endrede forsvars- og sikkerhetsutfordringer, herunder å danne en krigsforebyggende terskel og trygge eget personell. Ved å ta i bruk teknologi på en smart måte vil vi kunne løse oppgavene mer effektivt og med større kraft, alene og sammen med allierte og partnere.

Forspranget som USA og Vesten har hatt siden den første Golfkrigen, er nå i ferd med å utlignes. Det russiske forsvarsforskningsbudsjettet ble doblet mellom 2012 og 2015. Kinas investering i forsvarsforskning er sterkt økende og er nå vurdert til å være mer enn dobbelt så stor som den tilsvarende samlede investeringen i Europa. Fortsetter trenden, anslås det at Kina vil gå forbi USA før 2025. USA har ambisjoner om å beholde den militære overlegenheten så lenge som mulig og lanserte flere strategiske tiltak i 2014 for å klare dette. Europas samlede investering i forsvarsforskning har på den annen side blitt redusert med 29 prosent de siste årene og utgjør omtrent en sjettedel av USAs forskning- og utviklingsbudsjett på omtrent 600 milliarder kroner – eller et halvt norsk statsbudsjett. Dersom denne utviklingen ikke endres raskt, vil Europa ha valget mellom å bli en kunde av amerikansk forsvarsindustri eller være uaktuell som samarbeidspartner.

Mye av den grunnleggende teknologiutviklingen er fortsatt finansiert av militære midler, spesielt i USA, Russland og Kina, men anvendelsene er på mange områder drevet av sivile behov og av investeringer i forskning og utvikling i sivile selskaper. En konsekvens er at mye avansert teknologi er rimelig og lett tilgjengelig for alle. Dette bidrar også til å redusere Vestens forsprang.

Denne utgaven av VITEN tar for seg spesifikke teknologiområder og teknologier som vil gi Forsvaret store muligheter i dag og i årene framover. Den teknologiske utviklingen vil fortsatt utfordre forsvarssektoren, og vil på sikt kunne medføre store endringer i struktur, organisasjon og operasjonskonsepter for å opprettholde et bærekraftig forsvar. Vi må utnytte de mulighetene teknologien gir oss for å være relevante for våre nære allierte, og vi må forberede oss på at motstanderne våre, symmetriske så vel som asymmetriske, vil ta den samme teknologien i bruk.



**John-Mikal Størdal**

Administrerende direktør  
Forsvarets forskningsinstitutt

UTGIVER:  
Forsvarets forskningsinstitutt

FORSIDE/ILLUSTRASJON:  
Terje Tønnesen/byHands

REDAKTØR:  
Wenche Gerhardsen

DESIGN:  
Isabel A. Nordang

viten@ffi.no

BIDRAGSYTERE:  
Lørns Bakstad  
Trude H. Bloebaum  
Marianne R. Brannsten  
Torgeir Brøen  
Karsten Bråthen  
Sverre Diesen  
Wenche Gerhardsen  
Martin Gilljam  
Steinar Gulichsen  
Morten Hansbø  
Roy Hansen  
Frank T. Johnsen  
Bjørn Olav Knutsen  
Torbjørn Kveberg  
Ketil Lund  
Karl Erik Olsen  
Richard Olsen  
André Pettersen  
Bård K. Reitan  
Torbjørn Skauli  
Trygve Sparr  
John-Mikal Størdal  
Tom Thorvaldsen  
Einar Østevold

FOTO/ILLUSTRASJON:  
nyhetsgrafikk.no, Forsvaret,  
FFI, Terje Tønnesen/byHands,  
UTIAS/SFL, Shutterstock

Trykk: Fladby as

Opplag: 1500

P ISBN: 978-82-464-2738-6  
E ISBN: 978-82-464-2739-3

ABONNER PÅ  
VÅRT NYHETSBRV:  
ffi.no/nyhetsbrev

FØLG OSS PÅ:  
Facebook  
Instagram  
ffi.no

Forsvarets forskningsinstitutt  
Besøksadresse:  
Instituttveien 20  
2027 Kjeller

Postadresse:  
Postboks 25  
2027 Kjeller

Telefon:  
63807130



# TEKNOLOGIEN FORSVARET TRENGER

- 4 Introduksjon
- 6 Teknologiutviklingen påvirker forsvaret vårt
- 8 Skyter fart med informasjonsteknologien
- 12 Kunstig intelligens og autonomi
- 18 Sensorer for bedre situasjonsforståelse
- 20 Militær luftromsovervåking med radar
- 24 Romteknologi for Forsvaret
- 30 Augmented Reality på bakken
- 34 Tid for en blandet virkelighet
- 40 Bedre beskyttelse med nye materialer
- 42 Strøm uten en tråd
- 44 Referanser

- 16 **TEKNOLOGIKAPPLØP**  
Hva betyr teknologikappløpet for Europa og NATO?
- 28 **KOSTNADSVEKST**  
Kan teknologien redusere Forsvarets kostnader?
- 38 **CYBERFORSVAR**  
Tre store utfordringer med cyberforsvar

# Teknologiutviklingen påvirker forsvaret vårt

Teknologiutviklingen påvirker krigføringen. Dermed påvirker den både vårt og alle andre lands forsvar. Påvirkningen skjer på flere måter, ikke bare ved at våpen, kjøretøyer og annet materiell stadig forbedres. Grovt sett kan vi si at teknologiutviklingen påvirker krig og krigføring på fire forskjellige måter.

## 1

---

### **Ny teknologi gir høyere ytelse**

Den første måten er åpenbar og direkte: innsats av mer og bedre teknologi fører til at nytt militært materiell stadig får høyere ytelse enn det materiellet det avløser. I de fleste tilfeller er forbedringen fra en utstyrsgenerasjon til den neste ikke dramatisk, men den kan likevel gi store utslag på slagmarken. For eksempel demonstrerte den første Golfkrigen i 1991 at termiske stridsvognsikter – sikter som ser varmestrålingen fra målene – ga fullstendig overtak om natten mot stridsvogner med sikter som kun forsterker lyset fra måne og stjerner.

## 2

---

### **Forsvarsspesifikk kostnadsvekst**

Medaljen har en økonomisk bakside. Både anskaffelse og drift av moderne utstyr er knyttet til en spesiell type kostnadsvekst. Denne kostnadsveksten er annerledes enn den vi kjenner fra annen industriproduksjon, der ny teknologi ofte bidrar til å gjøre ting rimeligere. Produksjon av militært materiell kjenne- tegnes av en spesiell type kostnadsvekst som gjør at alle vestlige lands forsvar i perioden etter den kalde krigen har krympet, fordi myndighetene ikke har vært villige til å erstatte eldre utstyr med like mange nye og forbedrede våpensystemer. Småstater som Norge, med et lite forsvar i utgangspunktet, er nå kommet ned på et nivå som gjør at vi ikke lenger vil greie å opprettholde hele bredden av kapasiteter i et moderne, nasjonalt forsvar, med et flatt videreført budsjettnivå. Teknologiutviklingen påvirker med andre ord militære organisasjoner på en helt grunnleggende måte gjennom den forsvarsspesifikke kostnadsveksten. (Les mer om denne kostnadsveksten på side 28.)

### Teknologien gir gjennombrudd og motmidler

Fra tid til annen skjer det teknologiske gjennombrudd som endrer både kostnader og ytelser på militært materiell og skaper såkalte paradigmeskifter – omveltninger som fullstendig endrer måten militære organisasjoner utrustes og opererer på. Oppfinnelsen av forbrenningsmotoren er et eksempel på en slik omveltning: Ikke bare ble det mulig å motorisere og mekanisere militære styrker, det ble også mulig å bygge flymaskiner som førte til at krigføringen kunne utvides til luftdomenet. Et annet eksempel er informasjonsteknologien, som har gjort det mulig å føre krig i cyberdomenet. (Les om utfordringer med cyberforsvar på side 38.) Noen slike teknologiske paradigmeskifter er med på å øke kostnadene for å kunne opprettholde et moderne forsvar, for eksempel flymaskinen. Andre ganger har det fungert motsatt – det er funnet opp billige og enkle våpen som har snudd opp-ned på forholdet mellom pris og ytelse. Da armbrøsten kom mot slutten av middelalderen, ble det plutselig mulig for en bondeknekt å beseire datidens høyteknologiske og meget kostbare våpensystem: ridderen til hest i panser og plate.

I enkelte tilfeller har slike teknologiske gjennombrudd vært så omfattende at det i seg selv har utløst ny forskning og nye gjennombrudd. Det opprinnelige gjennombruddet ga en krigførende part et så stort forsprang at det ble helt avgjørende for motstanderen å komme opp med et motmiddel. Da tyske jagerfly i første del av andre verdenskrig hindret britiske bombefly i å angripe mål i Tyskland på dagtid, gikk de over til å bombe om natten. Det var mulig med datidens bombesikter, mens det var svært vanskelig for jagerfly å finne og skyte ned bombeflyene i mørket. De britiske bombetoktene utviklet seg imidlertid til å bli en så stor trussel at dette i seg selv forserte den tyske utviklingen av nattjagere utstyrt med radar, som raskt begynte å gjøre innhugg i bombeflyformasjonene. De britiske nattbombesiktene var med andre ord blitt ofre for sin egen suksess – en sammenheng mellom middel og motmiddel som går igjen i hele den militære teknologihistorien.

### Teknologiutviklingen har en sosial kontekst

Den fjerde og siste siden av teknologiutviklingen er den vi kanskje tenker minst på: Teknologiutviklingens sosiale kontekst. Det vil si at måten det blir teknologisk mulig å føre krig på endrer måten vi som samfunn tenker når det gjelder krig og krigens legitimitet. Et eksempel er den moderne droneteknologien, som reiser en rekke etiske og rettslige spørsmål knyttet til den formen for fjernstyrt krig som dronene representerer. Et teknologisk framskritt som i utgangspunktet fører til at krigføringen effektiviseres, kan ha andre konsekvenser som i neste omgang påvirker synet på og aksepten for bruk av militærmakt som et politisk virkemiddel.

Den kombinerte teknologi- og kostnadsutviklingen som pågår akkurat nå er uten tvil den største utfordringen vi i Norge står overfor når det gjelder å bevare et eget nasjonalt forsvar. Men fordi dette gjelder alle små og mellomstore stater i den industrialiserte verden – hvor forsvar etter hvert utkonkurreres av andre offentlige oppgaver – ligger det også et insentiv til forsterket flernasjonalt forsvarssamarbeid i årene framover.

# Skyter fart med informasjonsteknologien

Siden internettets opprinnelse har det vært viktig å koble ting sammen i nettverk for bedre samhandling og effektivitet både sivilt og militært. Forsvaret var tidlig med på denne utviklingen, men etter hvert som teknologiutviklingen har gått raskere, har Forsvaret og forsvarsindustriens evne til å utnytte den nye teknologien blitt dårligere. Teknologiutviklingen gir mange muligheter for bedre samhandling og effektivisering, men også utfordringer med å utnytte dette i Forsvarets prosedyrer, organisasjon og kultur.

## Rollene snur med internett

Utviklingen av internett går tilbake til 1960-tallet og ARPANET, utviklet av USAs Advanced Research Projects Agency (ARPA). Datidens datamaskiner var svært dyre, og amerikanerne ønsket at forskningsinstitusjoner skulle ha mulighet til å benytte regneressurser hos hverandre.

Norge ble som første land utenfor USA knyttet til [ARPA-NET](#), først med Norwegian Seismic Array (NORSAR) i 1973, og deretter med FFI i 1974. FFI var også med på utviklingsarbeidet som endte med den grunnleggende teknikken for dagens internett. Arbeidet pågikk mellom 1973 og 1982 og ble ledet av ARPA. I tillegg til FFI deltok universiteter fra USA og England og en håndfull amerikanske firmaer og forskningsinstitusjoner. FFI bidro med målinger av trafikk på nettet, inkludert satellittkanaler. Universitetsmiljøer holdt seg borte fra dette samarbeidet, noe som antakelig hadde sammenheng med ideologiske reserverasjoner mot forsvar generelt. Utover 1980-tallet fikk imidlertid et økende antall amerikanske, europeiske og andre universiteter tilknytning til nettet.

Det var først i starten av 1990-årene at internett virkelig skjøt fart. Medvirkende faktorer var oppfinnelsen av World

Wide Web i 1989, opphevelsen av forbudet mot kommersiell trafikk i 1991 og utviklingen av den første nettleseren, Mosaic, i 1993. Dette var også det året internett ble åpnet for alle. Fra 1991 begynte tilknytninger og trafikk på internett å øke tilsvarende en dobling hver syvende måned. Fram til begynnelsen av 1990-tallet kan vi derfor si at Forsvaret, gjennom FFI, var helt i forkant av internett-teknologien. Etter dette ble imidlertid rollene snudd, og den sivile verden har i stor grad drevet utviklingen siden. Et eksempel på dette er prinsippet med å splitte opp dataprogrammer i mindre, uavhengige tjenester som gjenspeiler forretningsprosessene og samhandler over nettverket, såkalt tjenesteorientering (SOA). Dette prinsippet oppsto på 1990-tallet, og er i dag en svært moden teknologi som brukes mye både i privat og offentlig sektor. Til tross for at både Forsvaret og Nato har innsett nytten av denne teknologien, og ønsker å ta den i bruk, er militær bruk av tjenesteorientering fortsatt på forsøksstadiet.

## Militære løsninger

Etter hvert som flere brukere ble tilkoblet internett, økte også etterspørselen. Det oppsto et behov for tettere samarbeid mellom bedrifter som tilbød ulike tjenester, for eksempel mellom nettbutikker. Samtidig kom også de første tjenestene som la til rette for at det var brukerne selv som skulle generere informasjonen som ble delt, noe som etterhvert utviklet seg til å bli dagens sosiale medier.

Også i det militære domenet økte behovet for informasjonsdeling. Både nasjonalt og internasjonalt var det et ønske om å utnytte den teknologiske utviklingen slik at Forsvaret kunne oppnå bedre samhandling. Alle militære beslutningstakere, uansett hvor i organisasjonen de befant seg, skulle ha tilgang til



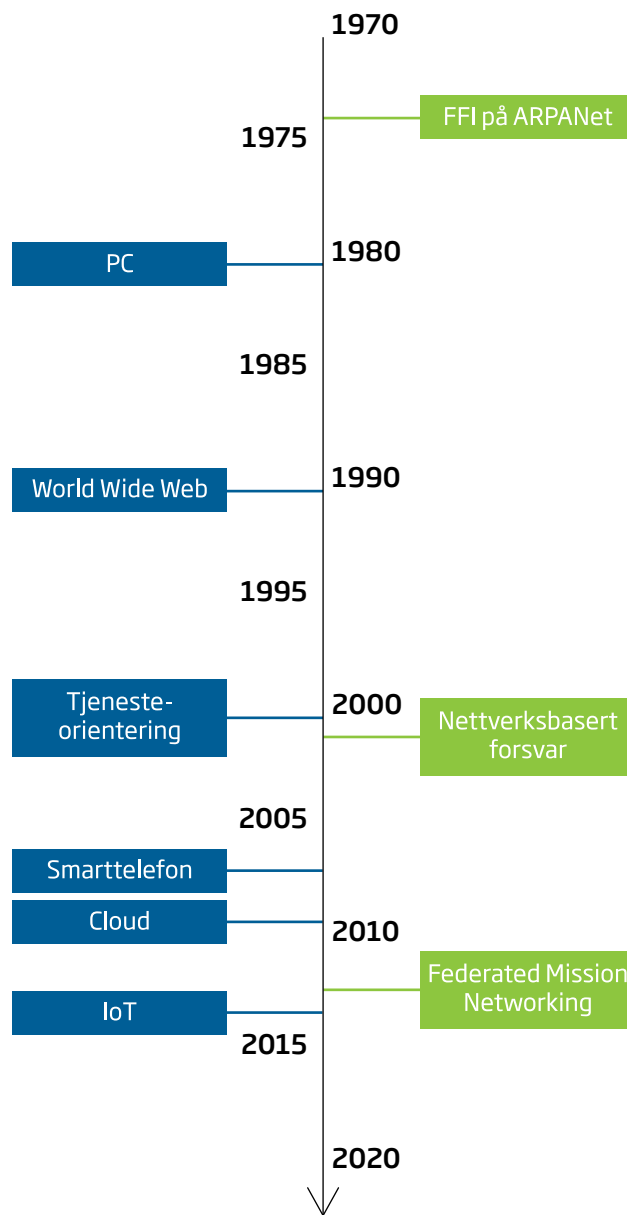
all nødvendig og relevant informasjon til enhver tid, for økt operativ evne og mer effektiv utnyttelse av ressurser. Denne tankegangen, kalt nettverksbasert forsvar, oppsto tidlig på 2000-tallet. Nato, og forsvaret i de ulike nasjonene, var tidlig ute med å identifisere tjenesteorientering som en brekkstang for nettverksbasert forsvar.

Dagens internasjonale militære satsing på det som kalles *Federated Mission Networking* (FMN) har som mål å få på plass både prosessene og de teknologiske rammene som skal til for at vi raskt og effektivt kan sette sammen nye nettverk til bruk i internasjonale operasjoner. Teknologisk ser forskere mest på standardene og de tekniske løsningene som ble utviklet tidlig på 2000-tallet, og jobber med å sikre at ulike nasjoners systemer kan virke sammen. I FMN er det per i dag lite interesse for nyere teknologier, for eksempel skytjenester, som i det sivile brukes for å videreutvikle tjenesteorienteringen. Motsatt går den sivile utviklingen fra komplekse standarder til enklere, men mindre standardiserte løsninger.

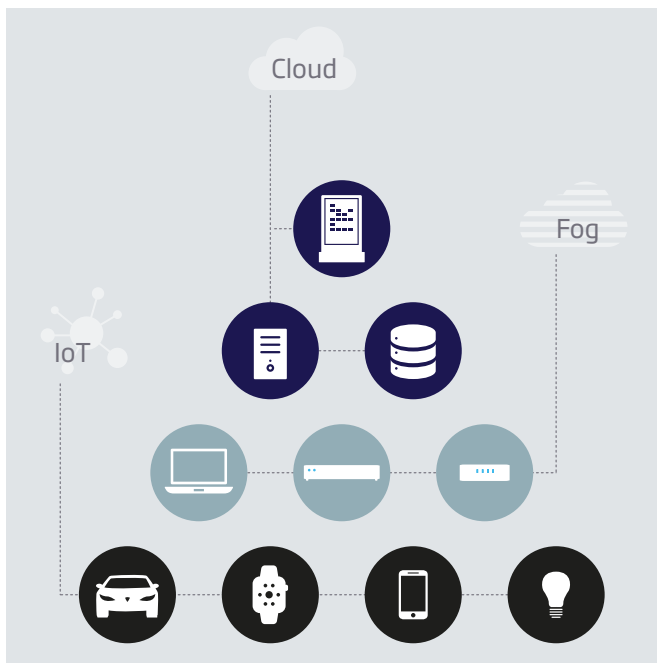
### Beregninger i skyen

Historien har en tendens til å gjenta seg selv, og for det relativt nye begrepet cloud computing, gjelder dette også for historien til datamaskiner. De siste tretti årene har store, sentraliserte maskinsystemer har vært avleggs og normen har vært personlige datamaskiner (PC). Før PCer tok av i 1980, var det vanlig å kjøpe databehandlingstjenester fra selskaper som kunne tilby regnekraft på dyre og spesialiserte datasystemer. Datasystemene var så store at de gjerne fylte et helt rom eller en hel bygning. Dagens datamaskiner er så kraftige at du kan gjøre samme jobben med en billig, liten PC. Eller kan du det? Med inntoget av informasjonssamfunnet har databrukere også et behov for å behandle store datamengder, større enn det som er overkommelig å behandle eller lagre på en enkelt datamaskin. Vi snakker om *big data* eller stordata.

Som på 70-tallet er det igjen et økende antall selskaper som tilbyr datatjenester. Slik *cloud computing* er tett knyttet til økt bruk av internett som en kommersiell plattform. Nå er vi på vei tilbake



Tidslinje over utviklingen av informasjonsteknologien. Til venstre sivil utvikling og til høyre militær utvikling.



IoT er det laveste nivået i en pyramide der vi har *cloud computing* på toppen med stor lagrings- og prosesseringskapasitet og *fog computing* som et mellomstjikt. På IoT-nivå har vi typisk lite prosesseringskraft slik at vi må sende data til behandling høyere opp i pyramiden. Om vi da ser for oss tusener eller millioner av «ting» på nedre felt, vil dette utgjøre store datamengder, *big data*. Over disse dataene vil vi måtte resonnerer maskinelt for å finne mønstre vi kan reagere på, noe som medfører en økt satsing på andre temaer, for eksempel dyp læring/maskinlæring/kunstig intelligens, som alle kan sies å være sider av samme sak.

mot 1970-tallets prinsipper med store datamaskinhaller. Å ta skyen i bruk er ofte kostnadseffektivt for bedrifter, fordi de kan velge å skalere dynamisk opp og ned etter behov til enhver tid og bare betale for ressursene de faktisk trenger. Til forskjell fra 1970-tallet er dagens løsninger mer dynamiske og skalerbare. Det er også mye konkurranse på markedet. Det kommer forbrukeren til gode. Datakraft har aldri vært så billig som nå.

Det finnes ulike tilnærminger til å ta skyen i bruk. En tilnærming kalles offentlig sky mens det andre ytterpunktet kalles privat sky. Den offentlige skyen er tjenester som tilbys av store private aktører som Amazon, Google og Microsoft. Felles for dem er at de tar seg av alt av drift og sikkerhet i forbindelse med de tjenestene vi kjøper av dem. Ulempen er at vi har liten kontroll over hvor data ender opp – mest sannsynlig havner de i et datasenter i utlandet. Microsoft har for eksempel et datasenter i Irland, men ikke noe i Norge. For Forsvaret vil det neppe være aktuelt å tillate at data forsvinner utenfor landets grenser. Med tanke på Sikkerhetsloven og graderte data er det mange andre aspekter å ta hensyn til, slik som for eksempel fysisk sikring av serverhaller. En privat sky kan tilby det samme som en offentlig sky, vesensforskjellen ligger i at brukeren selv anskaffer og drifter skyløsningen. Det er dyrere enn å bruke en offentlig sky, men da har brukeren samtidig full kontroll over hvor data lagres og den fysiske sikringen av infrastrukturen. På lik linje med smarttelefoner vil en sky representere en forstyrrende teknologi ettersom den bryter med tradisjonell tankegang i Forsvaret.

### Smarttelefoner i Forsvaret

Siden 2007 har smarttelefoner og nettbrett blitt allemannseie i store deler av verden. For Forsvaret representerer smarttelefoner og nettbrett en tankegang og et sett med teknologi som har vært svært vanskelig å ta i bruk. Teknologiens nytte er åpenbar. Aktiviteter ved FFI og i Forsvaret peker i retning av at dette er veien å gå. I fremtiden vil Forsvaret også benytte smarttelefoner, moderne mobile nettverk og mange av de samme tjenestene som vi benytter sivilt. Likevel er det som om Forsvaret

som organisasjon holder igjen. Hvorfor er det slik?

FFI har undersøkt bruk av smarttelefon og nettbrett i Forsvaret: Hvilke forventninger har Forsvaret til nytte og kompatibilitet? Hvordan kan vi benytte denne teknologien effektivt, og hvor godt passer den inn? Så godt som alle deltakere i undersøkelsene mener at slik teknologi er en god idé for Forsvaret, og at nyttepotensialet er stort. Forventningene hos potensielle brukere, som kjenner teknologien godt fra det sivile, er skyhøye. Likevel sier samtidig flertallet at teknologien ikke passer inn. Den passer ikke til måten de jobber på eller måten de er organisert på. Den passer også dårlig til den teknologien Forsvaret allerede har. Sikkerhet og tillit til teknologien trekkes fram som de største utfordringene.

Alt tyder på at smarttelefonene representerer en forstyrrende, eller disruptiv, teknologi for Forsvaret. Det er en teknologi som har et sett med egenskaper som er forskjellig fra den teknologien vi tradisjonelt benytter og

som beslutningstakerne verdsetter. De tradisjonelle teknologiene representerer noe kjent, og vi har kontroll på verdikjeden. Det oppfattes som sikkert og robust. Smarttelefonene utfordrer – de er rimelige, funksjonelle og tilgjengelige, men samtidig har de en ukjent, kaotisk og uoversiktlig teknologi. Ennå vet vi lite om hvordan denne utfordrende teknologien best skal utnyttes for å løse Forsvarets oppgaver, men det er «nykommeren», i dette tilfellet representert ved smarttelefonene, som har det største utviklings- og forbedringspotensialet.

### Kobler sammen det vi trenger

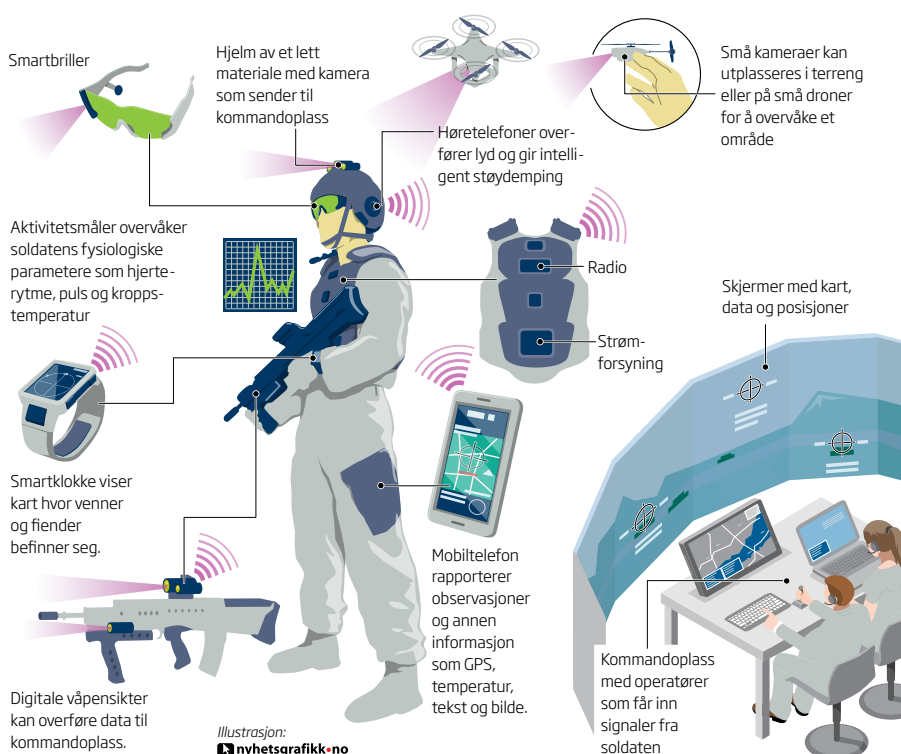
Ideen om tingenes internett, *Internet of Things (IoT)*, begynte med konseptet allestedsnærværende databehandling (*pervasive computing*) i 1995, da visjonen om å kople sammen alle mulige enheter på internett oppsto. For eksempel begynte vi å leke med tanken om smarte hjem. Hva om et kjøleskap selv kunne bestille mer mat rett fra butikken når det begynte å bli tomt? Eller om du kunne fjernstyre huset ditt mens du var på ferie,

og for eksempel slå lyset av og på? I dag er IoT et hett tema innen sivil forskning, og utviklere ser for seg millioner av ting som gjøres tilgjengelig på nett, på en slik måte at hverdagen blir enklere. De ser for eksempel for seg at kritiske komponenter selv varsler når de er i ferd med å feile, slik at de kan skiftes før systemet svikter. Dette kan bli praktisk for eksempel til utskifting av deler i fly eller deler på oljeplattformer. Andre viktige bruksområder kan være innen helsevesenet, der IoT vil kunne automatisere en del funksjoner som må gjøres manuelt i dag, som glukosemåling av diabetikere eller GPS-sporing av demente. Sivilt er det en del etiske utfordringer med teknologien ettersom den på enkelte områder kan sies å gripe dypt inn i privatlivet. Dette er aspekter som må tas tak i etter hvert som løsninger og teknologi modnes enda mer. Utviklingen går fort. Noen mener at maskiner med disse teknologiene i løpet av femten år kommer til å være smartere enn mennesker, med de etiske problemene det medfører. ■

Scenario for

## Internet of Military Things

For Forsvaret kan IoT potensielt fungere som en enkel og billig sensorplattform. Spesielt i USA snakker forskningsmiljøene om konseptet *Internet of Military Things (IoMT)*. Her er det viktig at det norske Forsvaret følger med og kommer på banen. Vi må utforske mulighetene og vurdere operative konsepter som den sivile IoT-satsningen baner vei for. Det vil være nødvendig med endringer i Forsvarets doktriner og kultur for å få det til. Utstrakt deling av informasjon på tvers av ulike nettverk og organisatoriske nivåer er nøkkelementer.



# Kunstig intelligens og autonomi

Mobiltelefonen vi har i lommen i dag, er flere ganger kraftigere enn de store superdatamaskinene som slo Gary Kasparov i sjakk for tjue år siden. Datamaskiner kan gjøre mange oppgaver på en mye bedre og billigere måte enn vi mennesker er i stand til. Roboter har bidratt til å avlaste mennesker fra rutinemessig, repeterende, tungt og farlig fysisk arbeid i mange år. Utviklingen det siste tiåret gjør at maskiner nå kommer for fullt i arbeid der informasjonsprosessering er viktig. Datamaskiner kan samle, håndtere og trekke ut informasjon fra store mengder data svært raskt, og det har vist seg at de er gode til å finne løsninger på komplekse problemstillinger. Men noen oppgaver er rett og slett for krevende å regne på, selv for en datamaskin. Hvis vi for eksempel skal besøke ti byer og ønsker å finne den korteste veien, er det over 3,6 millioner mulige løsninger. For tjue byer øker tallet over 2,4 trillioner (atten nuller). Hvis vi legger til nye dimensjoner og ønsker å finne den kombinert raskeste og billigste ruten, øker kompleksiteten. Det er mye forskning på hvordan datamaskiner kan finne gode løsninger på problemstillinger der det er vanskelig å regne seg fram til optimale løsninger. Kunstig intelligens er en del av denne forskningen. Dyp læring har fått spesiell oppmerksomhet de siste årene. Dette er en metode som etterlikner hjernens oppbygging og måte å lære på. Ved å bruke denne metoden kan datamaskiner trenes og lære seg de gode løsningene. Det er demonstrert at datamaskiner på kort tid kan lære seg dataspill fra 1980-tallet bedre enn ekspertspillere, bare ved å få tilgang til skjermen, joystick og poengene.

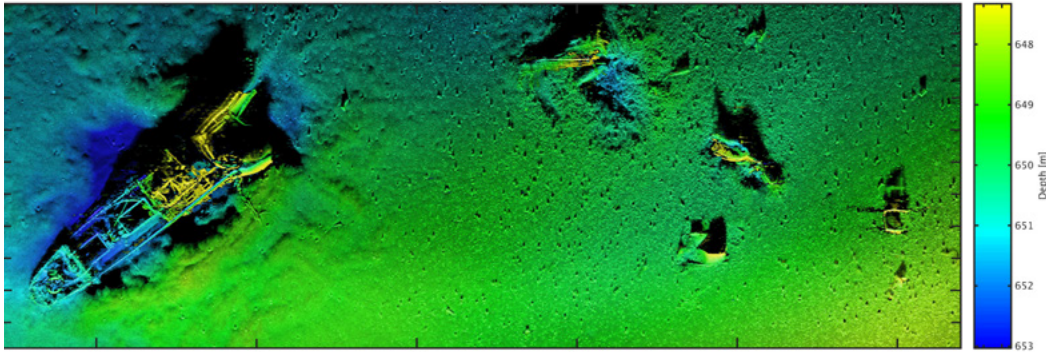
## Ubemannet er ikke noe nytt

Etter første verdenskrig ble både radiostyrte fly og stridsvogner benyttet i militær sammenheng. For eksempel brukte Sovjetunionen radiostyrte stridsvogner i vinterkrigen mot Finland i 1939. Hvis vi ser bort fra utviklingen av missiler og ra-

ketter etter andre verdenskrig, har utviklingen av ubemannede systemer gått relativt sakte. Teknologien var ikke moden for å ta de neste stegene. Det har utviklingen innen informasjons- og kommunikasjonsteknologi endret på. De siste tjue årene har utviklingen av fjernstyrte ubemannede systemer skutt fart, og de siste årene har automatiske og autonome ubemannede systemer tatt store steg.

Med autonome systemer mener vi systemer som ikke bare handler automatisk, men som også håndterer uforutsette hendelser på en intelligent måte. Fjernstyrte systemer er ressurskrevende og ikke spesielt billige. Det store potensialet for slike systemer er til stede når maskinene blir mer selvstendige, enkle å operere og bare må overvåkes. Denne modenheten gjør slike systemer mye mer kommersielt interessante. Når slike systemer samtidig er blitt mye billigere og tilgjengelige, har samfunnets interesse for dem økt kraftig. Nye kommersielle krefter involveres og teknologien utvikles raskere og blir billigere. Aktører som Google, Facebook, Amazon og bilindustrien har store ambisjoner og investerer tungt. Tidligere var ubemannede systemer forbeholdt militær forskning, nå er det de sivile som sitter i førersetet og driver teknologien framover. Eksempelvis brukes smarttelefoner som "hjerne" i små ubemannede systemer i luften. En smarttelefon er som en liten datamaskin med kameraer, navigasjon og kommunikasjon. Miniaturisering og masseproduksjon av komponenter gir lavere vekt og bedre ytelse på små systemer med lavere pris. FFI kjøpte et lite ubemannet helikopter i 2006 for 260 000 kroner. I dag kan en bedre modell med videokamera og videolink til bakken kjøpes på lekebutikken for 8 000 kroner.

Datamaskiner og autonome systemer endrer samfunnet økonomisk, sosialt og teknologisk. Roboter støvsuger huset vårt og klipper plenen. Snart kjører bilene selv og datamaskiner støtter oss i et større spekter av arbeidslivet. Denne



Dette syntetisk aperture sonar-bildet er tatt med FFIs AUV HUGIN, med FFIs forskningsskip HU Sverdrup II på tokt i Skagerrak i januar 2016. Bildet er av et drøyt 100 meter stort skipsvrak som har betydelige skader. Fremre del av skipsvraket mangler eller er brutt opp i biter. Deler av lasten, mulige kjemiske stridsmidler og annet potensielt farlig avfall, er spredt utover bunnen rundt vraket. Vraket ligger i dumpfeltet på cirka 600 meters dyp. De sorte områdene er skyggeområder der sonaren ikke kan observere. Farge angir dybde og lysstyrke angir ekkostyrke.

teknologien kommer også til å endre Forsvaret. Teknologien som trengs i det sivile og i det militære har mange likhetstrekk, og det er stort potensial for flerbruk. FFIs oppgave er å forstå teknologien og bidra til at Forsvaret ser mulighetene og kan utnytte dem. Samtidig må Forsvaret forstå truslene og utfordringene som denne teknologien gir.

### Maskiner som forstår, sanser og samarbeider

Hva kreves av teknologi for å utvikle et autonomt ubemannet system? Autonome systemer må selv kunne tolke en oppgave, planlegge og gjennomføre den, og tilpasse seg situasjonen og omgivelsene underveis. Systemene må legge om planene når situasjonen endrer seg eller når det kommer ny informasjon. Det kan for eksempel oppstå feil som må håndteres. Maskinen må derfor forstå, prioritere og ta beslutninger. Et eksempel på planlegging er at systemene må beregne optimale posisjoner og ruter, både før og under gjennomføring av oppgaven. Grunnlaget er data som er kjent på forhånd, men mye er observasjoner underveis. I likhet med mennesker må maskinene være i stand til å sanse sine omgivelser for å kunne utrette noe. De må kontinuerlig registrere og oppfatte det som er vesentlig for å løse oppgavene. En viktig del av dette er å gjenkjenne objekter og hindringer, og å orientere seg og finne veien. Sansene kan være et sett av sensorer som innhenter data og sammenstiller informasjon. Det kan være lyd, bilder, varmestråling, reflekterte laserstråler eller radarbølger. Ofte er det bredere og bedre informasjon enn det vi mennesker får fra våre sanser. Selv om maskiner kan håndtere store mengder data er utfordringen for maskinene å forstå denne informasjonen. Der er mennesket fremdeles overlegent.

Også for maskiner er det som oftest en fordel at flere samarbeider om å løse en oppgave. Hvert av de autonome systemene kan være brikker i et større nettverk, en gruppe med like en-

heter eller ulike enheter med komplementerende egenskaper. Hvert system har da en rolle i den større helheten og må samspille. De kan opprette et nettverk mellom seg og utveksle informasjon som gir en bedre forståelse av situasjonen og en raskere og bedre oppgaveløsning.

### Overalt i Forsvaret

FFI arbeider med autonome ubemannede systemer i luften (*unmanned aerial vehicle*: UAV), på vannet (*unmanned surface vehicle*: USV), under vann (*autonomous underwater vehicle*: AUV) og på bakken (*unmanned ground vehicle*: UGV). Disse systemene kan støtte alle grenene i Forsvaret. Med slike systemer kan vi unngå at personell utsettes for de farligste oppdragene, hindre skader og spare liv. Personell kan få hjelp til å unngå eksponering for beskyting, skjulte bomber, eller radiologisk eller kjemisk forurensing. Andre formål er de samme som i det sivile, for eksempel å gi maskinene oppgaver som de kan gjøre bedre og billigere enn mennesker – kjedelig rutinearbeid, oppgaver som krever lang utholdenhet med høy nøyaktighet, og innhenting og sammenstilling av mye informasjon. Autonome ubemannede systemer kan lettere skaleres i antall og ytelse, og er mindre sårbare enn bemannede løsninger. Ved å ha mange billige og selvstendige systemer som ikke krever for mye ressurser kan vi lettere øke antallet eller håndtere tap av enheter.

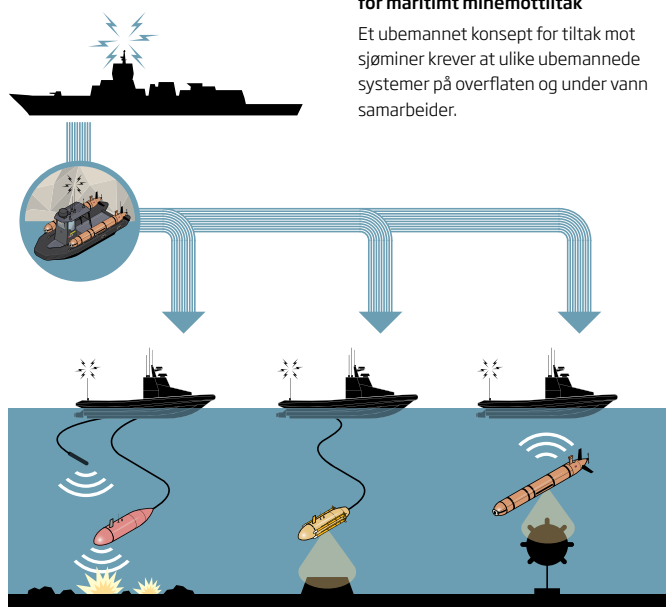
FFI er verdensledende på autonome undervannsfarkoster, og har sammen med Kongsberg Maritime utviklet en farkost, HUGIN, som er solgt både til forsvaret i flere land og til oljebransjen. Under vann er det dårlig kommunikasjon, og farkostene må klare seg selv. HUGIN har derfor et automatisk beslutningssystem. Den finner veien selv og klarer å lete opp og gjenkjenne gjenstander, som miner, uten menneskelig inn- gripen.

## Noen konkrete planer for framtidige operasjonsmodi er bruk av:

- AUV til minejakt, potensielt framskutt og skjult. AUV-en vil kjøre autonomt i et mønster for å lage sonarbilder over større områder av havbunnen, tolke bildene, og selv legge planer for identifikasjon av mistenkelige objekter ved bruk av andre sensorer.
- USV til minesveip, autonomt eller fjernstyrt.
- USV som taxi for å bringe AUV-er inn i et operasjonsområde med stor avstand fra det bemannede moderskipet.
- USV for å bringe engangsvåpen inn i et operasjonsområde for å nøytralisere miner.
- USV som vertsplattform og relestasjon til AUV. Dette vil kunne gi bedre navigasjon og kommunikasjon for AUV-en under minejaktoperasjonen.

### Et mulig framtidig konsept for maritimt minemottiltak

Et ubemannet konsept for tiltak mot sjøminer krever at ulike ubemannede systemer på overflaten og under vann samarbeider.



## Autonome løsninger for minejakt

Forsvaret ønsker et ubemannet konsept for søk og uskadeliggjøring av miner. Dette er farlige oppdrag som krever store ressurser og mye tid. Derfor har Forsvaret nylig besluttet at i framtiden skal slike oppdrag løses ved hjelp av ubemannede farkoster.

FFI samarbeider med Sjøforsvaret og industrien om å utvikle framtidens konsept for maritimt minemottiltak, bygget på bruk av ubemannede systemer på overflaten og under vann (se figur side 14). Ubemannede systemer kan operere trygt i potensielt farlige minelagte områder. Dersom AUV-en også kan operere skjult i langt framskutte posisjoner, vil det åpne for operasjoner i områder med sjønektelse, og samtidig skjule planlegging av operasjoner og egne intensjoner. En AUV kan operere framskutt og skjult ved å fraktes med ubåt eller ved å øke AUV-ens rekkevidde markant gjennom ny teknologi for strømforsyning. FFI har utviklet en prototype på et luftuavhengig strømforsyningssystem for AUV, basert på brenselceller. (Les mer om strømforsyningssystem på side 42.)

HUGIN har et avansert GPS-uavhengig navigasjonssystem som også bruker terrenget for å navigere. I krise og krig er vi ikke sikret GPS-signaler. Det er derfor et behov for å ha robuste navigasjonsløsninger som utnytter tilgjengelig informasjon i alle domener – i luften, på sjøen, på bakken og under vann. Det er mulig å navigere etter terrenget, eller å gjenkjenne objekter eller kjennemerker og navigere i forhold til disse. Vet vi posisjonen til dette landemerket, vet vi også hvor vi er. FFI arbeider med flere teknikker for GPS-uavhengig navigasjon. Sonarene på HUGIN har høy kvalitet og er viktige for både kartlegging og navigasjon. Sensorekspertisen på FFI bidrar til utvikling av sansene til autonome ubemannede systemer.

## Førerløse kjøretøy

Det er en viss sammenheng mellom pris og størrelse på ubemannede systemer, der «liten» ofte betyr «billig». Små og billige farkoster gjør det mulig å øke bruken av systemer som UAV og UGV i Forsvaret. Forsvaret har allerede lenge operert ubemannede bakkekjøretøy i form av *Explosive Ordnance Disposal*-roboter (EOD) som ødelegger bomber. De er relativt små og enkle systemer.

Den raske utviklingen innen selvkjørende biler drives hovedsakelig av et kappløp i sivil bilindustri, som vil komme Forsvaret til nytte. Vi forventer en gradvis innføring av ubemannede bakkekjøretøy som jobber sammen med bemannede plattformer. Arbeidsfordelingen mellom de bemannede og ubemannede plattformene vil utvikle seg over tid. Et ubemannet bakkekjøretøy trenger mange sensorer og prosesseringskraft. Bilindustrien etterspør nye sensortyper med bra ytelse, høy pålitelighet og lav pris. Det kan være daglyskamera, termisk kamera, radar og andre sensorer som måler fart og avstand. Alle disse sensorene bidrar til at datamaskiner som benyttes i kjøretøy får økt ytelse og lavere pris. FFIs oppgave vil etter hvert være å sikre at løsninger fra det sivile markedet blir robuste nok til militært bruk mot en avansert motstander.

I tillegg til EOD-roboter er det mange bruksområder for UGV-er i Forsvaret. UGV-er kan bære store nyttelaster og være til stede i områder over lengre tid. Dette er egenskaper som

er viktige for å drive rekognosering, oppklaring, overvåking og målfatning. Avfyring av våpen gir ofte stor signatur som en motstander vil oppdage. Derfor vil bruk av UGV-er som våpenbærere og avfyringsplattformer være ønskelig i framtidens stridsfelt. Bruk av UGV-er til logistikk vil være et område der teknologi som utvikles sivilt kan overføres til militær bruk. Det kan være selvkjørende lastebiler, som sammen med bemannede lastebiler frakter forsyninger over lange avstander. Et annet eksempel er mindre kjøretøy som frakter utstyr og forsyninger for et soldatlag i felt. Slike systemer finnes i dag på demonstratornivå.

### **Framtidens bruk av robotikk i Forsvaret**

Nyskaping i måten mennesker og roboter samvirker på, er viktig for å utnytte potensialet som ligger i bruk av ubemannede systemer. Samvirket vil spenne over land, luft, på og under vann og i cyberdomenet. Menneskers rolle vil variere fra direkte kontroll av farkoster til en mer overordnet eller sideordnet rolle. Et stort antall enheter og høyt operasjonstempo krever at personellet støtter seg på systemenes autonome evner, mens de selv bidrar med det som mennesker er best på – å forstå og delta i komplekse sosiale kontekster og kreativ problemløsning. Operatører vil først og fremst gi ordre til roboter, konfigurere og overvåke systemer og allokere ressurser. De vil i mindre grad selv delta direkte i strid eller direkte kontrollere ubemannede farkoster.

Ubemannede luftfarkoster utgjør allerede i dag kostnadseffektive og viktige tillegg til den eksisterende forsvarsstrukturen. Små farkoster er kjent som *Miniature Unmanned Aircraft System* (MUAS) og enda mindre farkoster går under navnet *Nano Unmanned Aircraft System* (NUAS). De er i bruk for taktisk informasjonsinnhenting til enkeltsoldat og avdeling i Hæren. I likhet med det norske Forsvaret har det amerikanske, britiske og australske Forsvaret kjøpt inn en norskutviklet NUAS, kalt Black Hornet. Dette systemet har FFI vært med på å utvikle sammen med det norske selskapet Prox Dynamics. Små MUAS og NUAS vil bli tallrike i Forsvaret som naturlige og viktige ressurser for Hæren og Forsvarets spesialstyrker.

Større ubemannede luftfarkoster er aktuelle som erstatning for nåværende P-3 Orion, til bruk i maritim overvåking. I denne anvendelsen vil ubemannede plattformer kunne gi en meget stor kapasitet. De vil kunne gi mye bedre tilstedeværelse og sensordekning enn det vi har råd til å opprettholde med dagens bemannede systemer. Dette skyldes i stor grad den lange utholdenheten til de autonome farkostene og utviklingen innen sensorer. Andre potensielle anvendelser av mellomstore til store UAV-er inkluderer etterretning og målfatning langt fra egne styrker, med særlig vekt på å gjøre Forsvaret i stand til å utnytte de nye kampflyene og langtrekkende våpen på en mest mulig effektiv måte. Bruk av både store og små UAV-er som bærer av kommunikasjonsutstyr blir også viktig framover, og kan bidra til å opprette nettverk lokalt eller tilby langdistansekommunikasjon. ■

## HVA BETYR TEKNOLOGIKAPPLØPET FOR EUROPA OG NATO?

Teknologiutviklingen i verden er del av amerikansk og europeisk sikkerhetspolitikk, der forsvarsrelatert forskning er et geopolitisk virkemiddel.

Begge sider av Atlanterhavet erkjenner at satsing på forsvarsrelatert forskning er høyst nødvendig for å sikre egne forsvarsbehov, men også for å sikre landenes økonomiske utvikling og evne til å møte den globale konkurransen i forsvarssektoren. Derfor er amerikanerne bekymret for økt konkurranse fra stormakter som India, Russland og i særlig grad Kina, selv om amerikansk forsvarsforskning er langt mer omfattende og teknologisk utviklet enn hos noen annen aktør. Budsjettet for forsvarsrelatert forskning i USA var på cirka 70 milliarder dollar i 2013. Det tilsvarer ti prosent av det amerikanske forsvarsbudsjettet.

I Europa er bildet et annet. Europeisk sikkerhets- og forsvarspolitisk samarbeid befinner seg i en krisesituasjon. En oversikt fra det europeiske forsvarsbyrået (EDA) viser at de totale forsvarsutgiftene i de 27 EDA-landene i 2012 var 189,6 milliarder euro, eller om lag 1,5 prosent av landenes bruttonasjonalprodukt. Nivået er det laveste siden 2006. I tidsrommet 2006–2013 falt bevilgningene til forsvarsrelatert teknologiforskning i EU fra 2,66 milliarder euro i 2006 til 2,09 milliarder i 2013. Dette tilsvarer et fall i reelle termer på 27,6 prosent i løpet av tidsrommet. Konsekvensen er at forsvarsindustrien nå overlever på grunnlag av tidligere forsvarsforskning. I tillegg svarer de på reduksjonen i europeisk etterspørsel etter forsvarsmateriell med eksport. Målet for EU i årene som kommer er likevel å videreutvikle evnen til å ta et større ansvar for europeisk sikkerhet

gjennom en felles sikkerhets- og forsvarspolitikk (CSDP) etter Lisboa-traktatens bestemmelser.

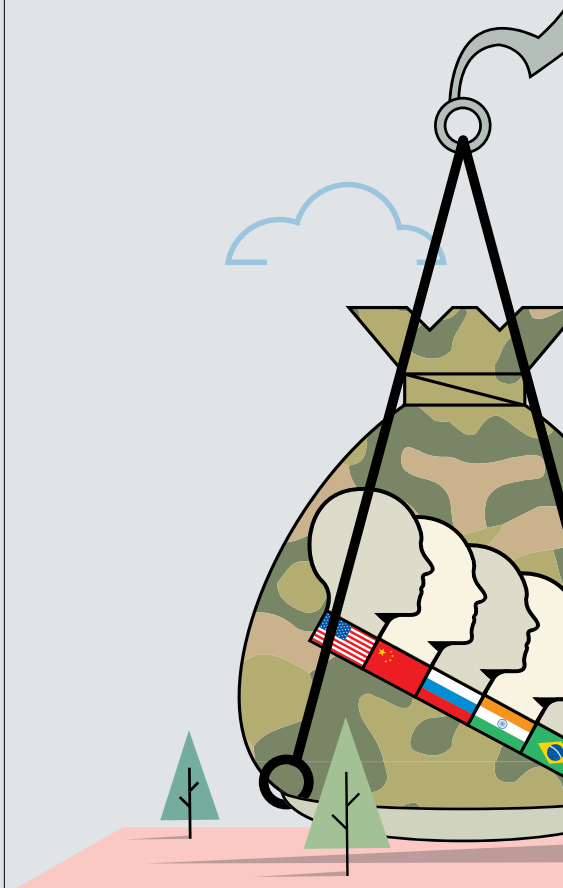
En av bakgrunnene for CSDP er USAs sikkerhetspolitiske forskyvning mot Asia og Stillehavsområdet. EU må bli i stand til å handle alene uten amerikanerne i Europas nærområder. Det innebærer å utforme diplomatiske, økonomiske og militære tilnærminger til kriser i egne nærområder, fremme maritim sikkerhet på global basis og støtte FN og andre arenaer for globalt samarbeid.

### Det amerikanske initiativet

Den økte amerikanske bekymringen for konkurranse fra andre stormakter på det forsvarsteknologiske området, som tidlig varsling-systemer og presisjonsstyrte våpen, fikk tidligere forsvarsminister Chuck Hagel i august 2014 til å lansere et eget initiativ for forsvarsinnovasjon. Amerikanerne omtaler initiativet som *the third offset strategy*. De vil utvikle innovative teknologier som vil opprettholde og fremme USAs militære dominans i det 21. århundre. Vil dermed det teknologiske gapet mellom USA og Europa øke ytterligere? I så fall, på hvilken måte? Vil europeiske forsvarsforskningsmiljøer kunne knyttes til USAs offsetstrategi? Hvordan vil strategien påvirke Nato? Disse spørsmålene indikerer at det er like viktig å undersøke hvordan offsetstrategien vil fremme forsvarsteknologisk innovasjon som det er å undersøke strategiens sikkerhetspolitiske virkninger for det transatlantiske sikkerhetsfellesskapet.

### European Defence Technological and Industrial Base (EDTIB)

Det europeiske råd understreker betydningen av å utvikle en integrert, innovativ og konkurransedyktig EDTIB, slik at EU kan utvikle en forsvarspolitikk som kan handle selvstendig. Målet er at EDTIB vil bidra til økonomisk vekst, høyteknologiske arbeidsplasser og innovasjon for europeisk industri. Utviklingen i EDTIB er et vesentlig utgangspunkt for å forstå teknologiutvikling i en sikkerhetspolitisk sammenheng.





### Forsvarsforskning som geopolittikk

Forsvarsforskning kan dermed ikke bare ses fra et teknologisk og økonomisk perspektiv, men må også få en geopolitisk side. Dette er årsaken til at vi må være opptatt av forsvarsforskningens betydning for innovasjon og skaperkraft i Europa sammenlignet med utviklingen på dette området hos andre maktsentra som Kina, Russland og USA. De to førstnevnte vil være vesentlige utfordrere til sikkerhet og samarbeid i det nordatlantiske området. Bakgrunnen er at Vesten ikke lenger har unik kontroll over de mest ledende teknologiområdene.

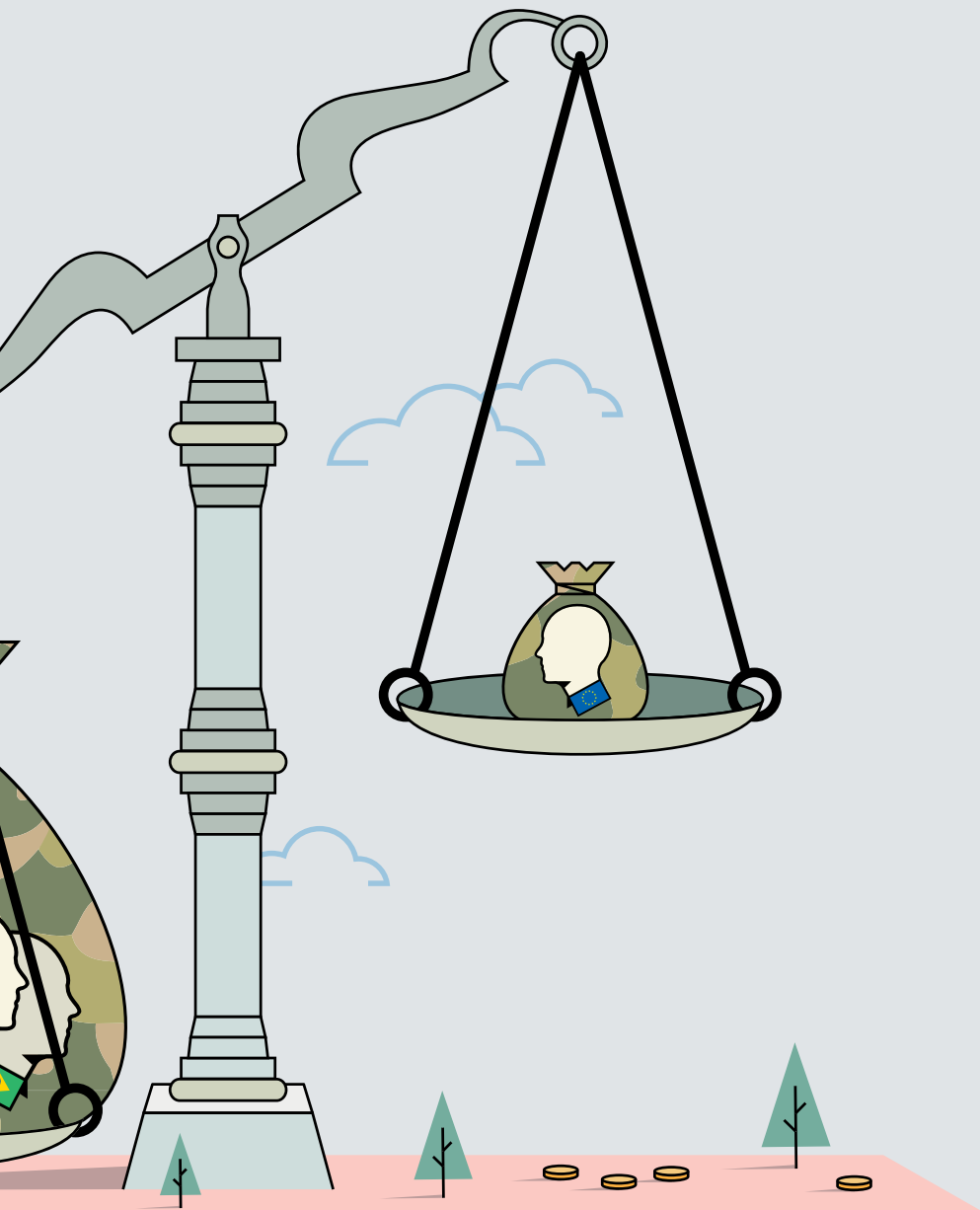
Sivil sektor har dessuten blitt betydelige innovatører innenfor forskning og utvikling på forsvarsområdet og noen av de mest lovende innovatørene blir rammet av mangel på fleksibilitet i anskaffelsesprosessene. Natos ambisjon om å være enhver potensiell motstander teknologisk overlegen, har i løpet av 2000-tallet blitt vanskeligere å oppfylle.

Teknologiutvikling og sikkerhetspolitikk henger tett sammen når vi sammenlikner utviklingen i Europa med utviklingen i en verden med flere maktsentra enn bare USA. Utviklingen i Europa sakker i denne sammenliknin-

gen. For eksempel har forsvarsutgiftene i Asia i løpet av 2010-tallet gått forbi de europeiske lands forsvarsutgifter for første gang i moderne tid. Den samlede innsatsen på forsvarsforskning i land som Brasil, Russland, India og Kina er dobbelt så stor som i Frankrike, Tyskland og Storbritannia samlet. I tillegg har forsvar mot andre statsaktører som kan true egen stats overlevelse, såkalte symmetriske trusler, igjen blitt reelt i EU. Bakgrunnen for dette er Ukraina-krisen og at Russland i dag framstår som en potensiell trussel mot Nato og EU. De europeiske landene erkjenner at de nå må ta et større sikkerhetspolitisk ansvar i sine nærområder. Dette inkluderer utfordringer som å håndtere krisen i Ukraina, terrorutfordringene og migrasjonsstrømmer fra deler av Afrika og Asia. Alternativet til europeisk ledelse i sikkerhetspolitikken blir dermed ikke amerikansk ledelse, men ingen ledelse i det hele tatt.

### USA er fortsatt størst

Bakgrunnen for at USA i flere årtier har vært den ledende teknologinasjonen i verden skyldes at de amerikanske føderale myndighetene har satset på høyteknologisk forskning og innovasjon. Dette har bidratt til amerikansk velstand og til at USA uten tvil har blitt den ledende militærmakten i verden. Selv om verden ellers går i multipolar retning der USA i årene framover må satse mer av sine forsvarsressurser i Asia, er verden likevel unipolar når det kommer til militærmakt. USA er i dag den eneste militærmakten i verden som har evne til global militær maktprojeksjon. En vesentlig årsak til dette er USAs satsing på forskning og utvikling i forsvarssektoren. I følge Europakommisjonen bruker USA i dag mer enn sju ganger så mye på forsvarsforskning som alle de 28 medlemslandene i EU til sammen. Dette bidrar selvsagt til å opprettholde og forsterke de allerede store militære asymmetriene mellom USA og Europa. Paradoxet blir stort når USA i årene framover vil kreve større europeisk lederskap i sikkerhetspolitikken, enten det kommer til uttrykk i EU eller i Nato.



# Sensorer for bedre situasjonsforståelse

Informasjon fra sensorer og informasjonskilder brukes til overordnet bildebygging og situasjonsforståelse og gir grunnlag for beslutninger. I skarpe operasjoner gir sensorer tidskritiske måldata og støtteinformasjon. En effektiv og hurtig prosess for å samle inn, analysere og fordele informasjon er en forutsetning for operativ effekt.

Utviklingen innen våpensystemer gjør det mulig å treffe mål nøyaktigere og på lengre avstand enn før. En god utnyttelse av slike våpen stiller høye krav til sensorer og informasjonssystemer. Koordinert bruk av land-, sjø- og luftstridskrefter gir mest effektiv utnyttelse av langtrekkende presisjonsvåpen, men krever tettere samarbeid mellom avdelinger enn det de tradisjonelt har hatt.

## Mer fleksible sensorer

Sensorer blir raskere og nøyaktigere. For eksempel får kameraer stadig større bildesensorer som gir bilder med høyere oppløsning. Radarsystemer blir mer fleksible og får høyere ytelse ettersom aktive fasestyrte antenner tas i bruk. Passive systemer får økt båndbredde og følsomhet, noe som øker evnen til å fange opp signaler. Mer av funksjonaliteten til sensorene ligger i programvare. Det gir bedre fleksibilitet og mulighet for oppgraderinger.

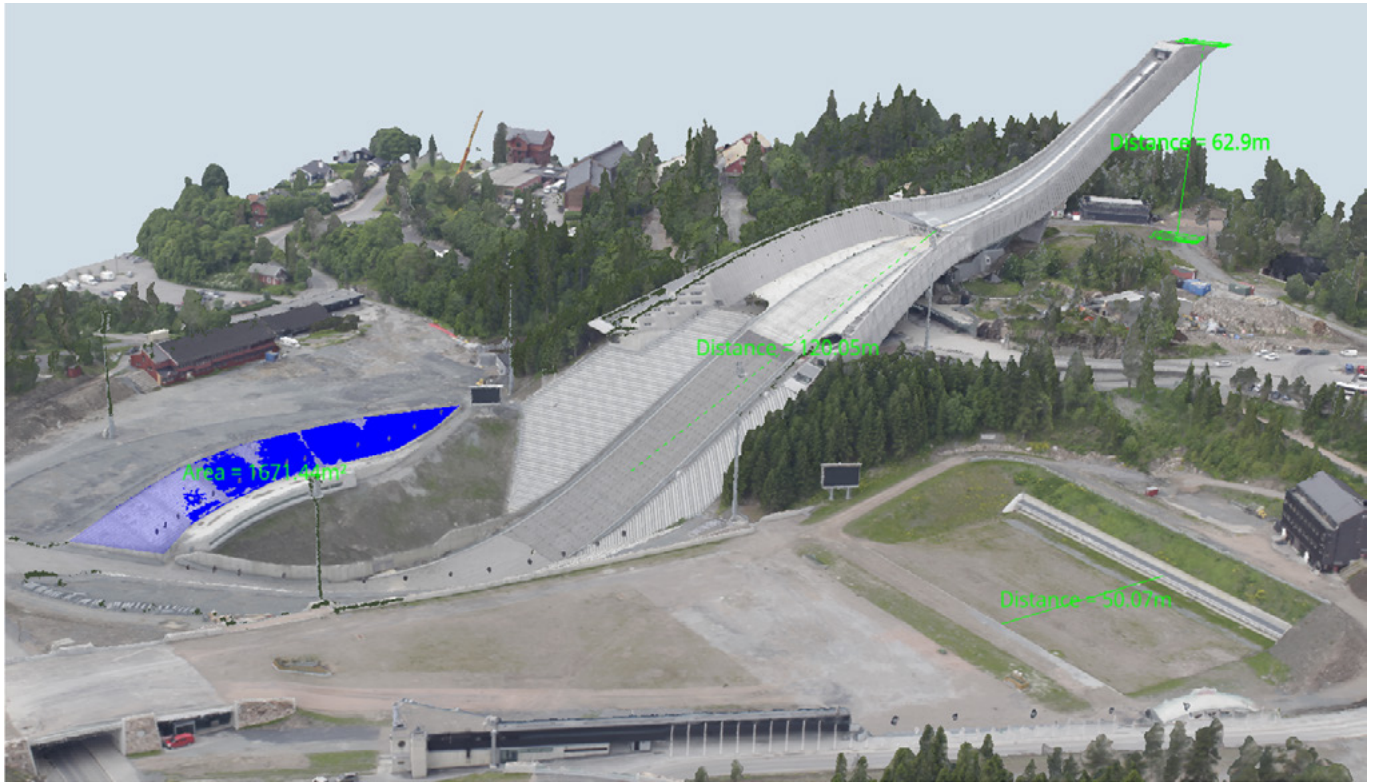
Større datamengder fra sensorer utfordrer både faste og mobile kommunikasjonsnettverk. Bruk av fiber i faste nettverk tilbyr imidlertid god kapasitet, og sivile teknologier som mobiltelefoni og trådløst nett har potensial også for militær bruk. Satellittkommunikasjon brukes i økende grad i vanskelig tilgjengelige områder og over lange avstander.

## Mer informasjon i bilder

Bilder fra ulike typer kameraer kan i større grad gi Forsvaret viktig informasjon. Forsvaret har tradisjonelt utnyttet video og overvåkingsbilder via manuell tolking, innenfor de begrensningene som sensorteknologien og tilgangen på sensorplattformer setter. Nå kan automatisk deteksjon og analyse støtte manuell vurdering av den økende informasjonsmengden. Metoder for automatisk gjennom søking og analyse av store datamengder er i rask utvikling. Teknologi for bildeanalyse har for eksempel kommet til et punkt hvor maskiner ofte kan tolke bilder like godt som mennesker, og vesentlig raskere. Dessuten kan maskiner hente ut helt nye informasjonsprodukter fra bilder, for eksempel tredimensjonale strukturer eller navigasjon for autonome systemer. Støtteverktøy gjør det dessuten mulig å visualisere informasjon på nye måter. Det gjør at analytikere kan lete etter mønstre i sammenstilte data ved hjelp av avanserte, men intuitive grensesnitt.

Nye typer bildesensorer kan også samle informasjon som tidligere ikke var tilgjengelig. Nye deler av det optiske spekteret er i ferd med å bli tatt i bruk, blant annet med hyperspektral avbildning. Det tilbyr radikalt bedre fargesyn enn øyet, og kan avsløre detaljer som ingen andre sensorer ser.

Data kan dessuten forbedres, for eksempel ved nøyaktig georeferering av bilder, som er en metode for å navigere og beregne kart og måldata. FFI har utviklet et instrument kalt Georeffinator. Det er et lite navigasjonsinstrument som georefererer bilder – det vil si at det bruker tregghetsnavigasjon til å måle hvilke områder i et gitt kart som dekkes av fotografier tatt i området kartet viser. Resultatet av denne metoden er de-



taljerte 3D-modeller som gir nøyaktige avstander, størrelser og plasseringer. Da kan vi for eksempel se hvor høy en bygning er, eller om et skipsdekk er stort nok til å romme et helikopter. Modellene får til og med fram enkeltelementer som trær og stolper, slik at vi på forhånd kan få en detaljert forståelse av hva som er innenfor synsvidde når vi står på en bestemt plass i modellen. Med en slik metode vil Forsvaret bedre kunne utnytte navigasjon i bildene, ta ut terrengmodeller og raskt lage kart over steder der det ikke finnes gode kart fra før.

Disse utviklingstrekkene er ikke unike for militære systemer. Sivil sektor driver fram mange av de underliggende teknologiene. Det er likevel krevende å finne ut hvordan teknologiene kan tilpasses militære formål, og hvordan Forsvaret skal møte en utvikling som går raskt sammenliknet med gjeldende anskaffelsessyklus. En balansert utnyttelse av teknologiene har til gjengjeld stort potensial for økt operativ effekt, fordi den kan bidra til bedre beslutningsgrunnlag og raskere tempo. Militære sjefer kan med nye sensorer bestemme seg raskere og med mindre risiko. ■

Dette bildet er hentet fra en 3D-modell av Holmenkollen, som er satt sammen av over hundre enkeltbilder. Bildene ble tatt fra et helikopter som fløy rundt hoppbakken. Modellen har fått riktig form og skala fra FFIs Georeffinator. Med en slik modell er det blant annet mulig å gjøre detaljert siktanalyse, der vi kan ta hensyn til små strukturerer som enkelte trær eller gjerder.

FFI tester ut en prototyp av Radar Imager for Mars' Subsurface Experiment (Rimfax) på Svalbard. Radaren skal være på Nasa-fartøyet som skal sendes til planeten Mars om få år.  
Foto: FFI



# Militær luftromsovervåking med radar



Norge er et langstrakt og smalt land med høye fjell og dype daler, noe som gjør militær luftromsovervåking komplisert og fordyrer løsningene våre. Norge er også et Nato-land som ligger alene i nord, og skal dermed overvåke et mye større volum enn for eksempel Tyskland, som har omtrent samme areal landmasse. Tyskland er omgitt av Nato-allierte, mens Norge må gjøre dette alene, med unntak av den hjelpen vi får fra Danmark.

Militær luftromsovervåking har kontinuitet og høy oppdateringsrate. Militært er det viktig å ha luftherredømme, samtidig som det er krevende og kostbart å ha fly kontinuerlig i luften. Kravet til kontinuitet og kvalitet i tid og rom, med en varslings tid på minutter, gjør bakkebasert militær luftromsovervåking til en kostnadseffektiv løsning sammenliknet med alternativene. Norge har ikke egen luftbåren overvåkingskapasitet for luftrommet. Det betyr at vi må være gode til å overvåke luftrommet fra bakken.

## Radar overvåker effektivt

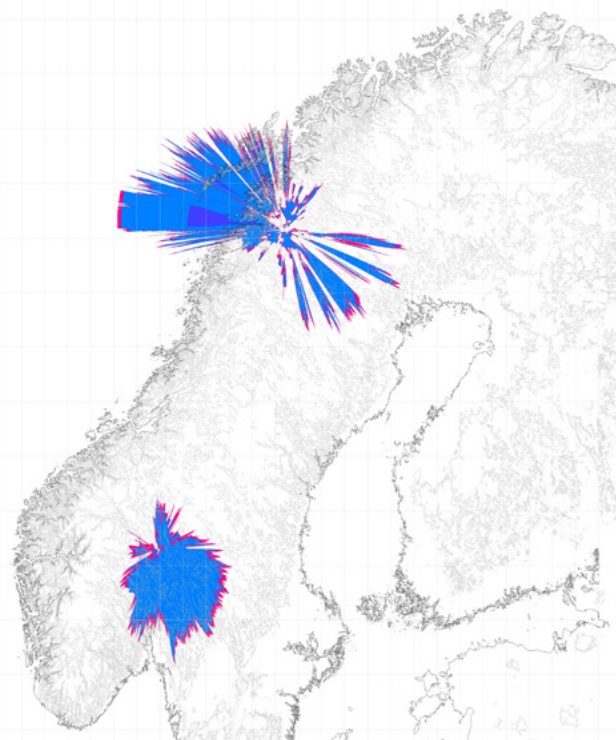
Radar er en viktig sensor i militære operasjoner. Sensoren utmerker seg med sin allværskapasitet og store rekkevidde, som til sammen gir høy militær relevans. Allværskapasitet betyr at radaren ser gjennom skyer, tåke og regn. Den store rekkevidden gjør effektiv overvåking av store volumer fra ett punkt mulig.

Militært er det stor interesse for radar med avbildende egenskaper. Denne kan understøtte situasjonsoversikten før, under og etter en militær operasjon. Tradisjonelt kan det være bakkekartlegging fra satellitt, eller nyere teknologi som ubemannede fly og kampfly med avanserte radarer. De avbilder store områder fra lang avstand og finner objekter under alle vær- og lysforhold.

## Radarer som enkelt kan flyttes

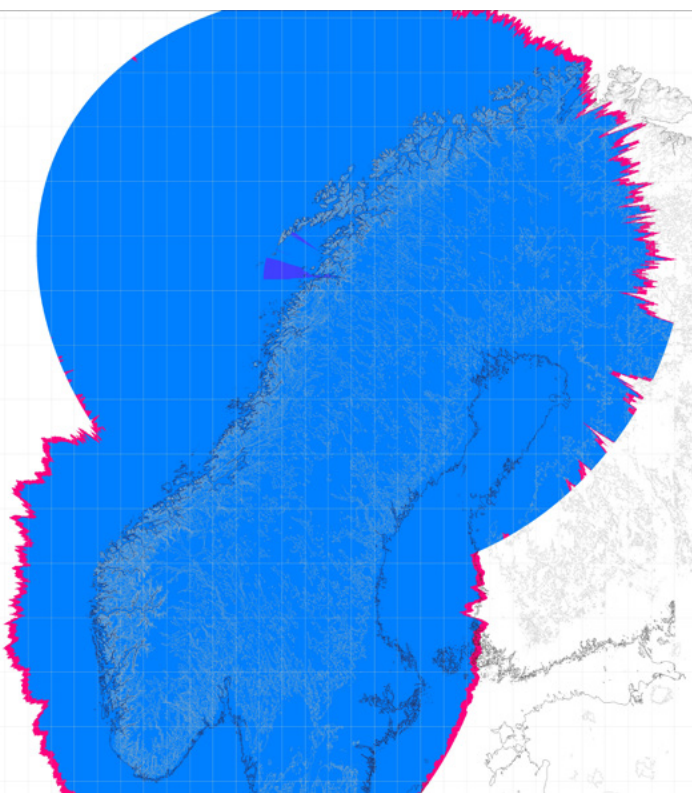
Militær luftromsovervåking har tradisjonelt hatt store, tunge systemer som det ikke har vært mulig å flytte, men utviklingen av radartechnologien har endret på dette. Flyttbare radarsystemer gjør det nå mulig å gå fra stasjonære systemer til systemer som er transportable på timer eller dager. Det gir mindre sårbarhet og høyere relevans for trusler.

Flyttbare radarer åpner for gjenbruk et annet sted. De nyere luftromsradarene til Forsvaret er i prinsippet allerede flyttbare. Disse radarene er silo-radarer på norske fjelltopper, det vil si at de kan senkes ned i fjellet i løpet av svært kort tid. Dette er en statisk installasjon rundt et i utgangspunktet transportabelt, men meget stort og tungt system. Dette systemet var



Radar kan ha stor rekkevidde, og det er ikke uvanlig med radarsystemer som ser mål på flere tusen kilometers avstand. Dette er store systemer som produseres i lite antall og helst for militære formål.

Over: Eksempel på radardekning i 1000 fot for to 600 kilometer-rekkevidde radarer.  
Under: Eksempel på radardekning i 50 000 fot for to 600 kilometer-rekkevidde radarer.



tradisjonelt ment for overlevelse, men med presisjonsstyrte våpen har vi mindre tro på denne løsningen nå enn for tretti år siden.

Flyttbare radarer gir Forsvaret nye muligheter til å løse flere oppgaver. Det kan være oppgaver som å understøtte bakkebasert luftvern eller å forsterke hav- eller luftromsovervåkingen. Systemene blir mindre (utstyret kan nå monteres på tilhengere som kan trekkes etter en kraftig bil og ikke i tunge containere) og samtidig går radarytelsen opp.

### Radarer som lagrer erfaringer

På grunn av den teknologiske utviklingen innen radar snakker vi heller om oppgavefokuseret radar enn spesialisert radar. Industrien som produserer luftromsovervåkingsradarer tilbyr nå produkter med et høyere teknologisk nivå. Produktene spenner fra familier av spesialiserte systemer til systemer som skal dekke flere oppgaver. Den funksjonaliteten som tidligere lå i hardware, legges nå i programvare. Dette gir en fleksibilitet som tidligere ikke var tilgjengelig, og sammen med økt regnekraft vil en radar selv kunne bestemme hvordan egne ressurser skal benyttes. Det er ikke kunstig intelligens, men et system som har evnen til å ta beslutninger på bakgrunn av tidligere erfaringer. Vi kan tenke oss at en operatør vil overvåke alle fly og skip langs kysten, men det regner og er storm og grov sjø. Dette vil påvirke radarytelsen. Operatøren kan da selv velge hvordan han skal bruke radaren og løse oppgaven. I framtiden vil radarsystemet selv kunne velge hvordan det skal bruke sin fleksibilitet for å løse oppgaven, basert på et sett kriterier og tidligere erfaringer. Tidligere erfaringer kan her være fra sekund til sekund, eller med lengre tidshorison, som fra måneder til måneder.

I militær luftromsovervåking betyr dette at sensorene også vil kunne gjøre andre oppgaver med god nøyaktighet. Dermed kan deteksjon, målfølgning, klassifikasjon, levering av måldata og samarbeid med andre militære systemer skje på en helt annen måte enn tidligere. Skal vi flytte på radarene, vil dette være viktig. I dag er de optimalisert for å stå på en fjelltopp, men i framtiden vil vi måtte optimalisere dem effektivt på nye steder. FFI jobber mye med nye teknologiske muligheter og måter å løse oppgavene på. Ved en militær prioritering kan Norges luftromsradarer benyttes mye tettere sammen med bakkebasert luftvern eller kampfly for å forsvare et område. Ytelser og størrelser og topografiske forhold spiller inn, sammen med dekning og risiko for å nås av et missil.

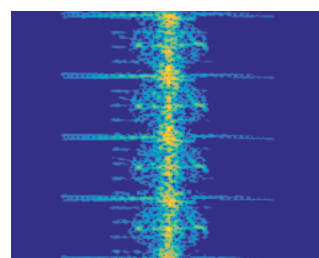
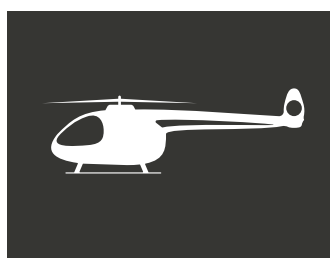
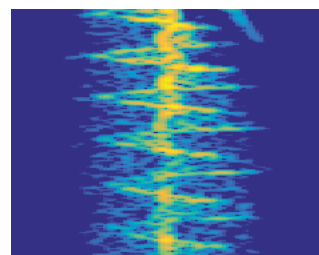
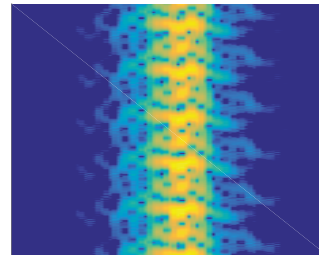
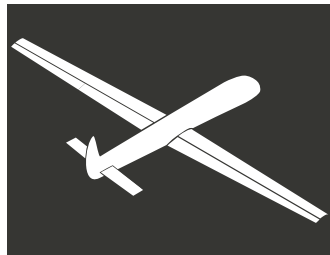
Noen radartyper spesialiserer seg på å se gjennom materie. FFI leverer radarteknologi til Nasa-fartøyet som skal sendes til planeten Mars om få år. Denne radaren kalles *Radar Imager for Mars' Subsurface Experiment* (Rimfax), og den kan se ned i bakken. På jorda ser slike radarer ofte etter begravde objekter som miner, eller etter undergrunnstrukturer i isbreer og formasjoner. På Mars skal den utforske jordlaget og lete etter vann. I samme radarfamilie er en radar som ser gjennom veggen. Målet med slike radarer er å avbilde bygningsstrukturer og mennesker inne i rom. Både militær og sivil bruk av slike radarer er vanlig. En tredje type radar er medisinsk radar, som kan måle fysiske egenskaper hos en person, for eksempel puls, hjerteslag og blodgjennomstrømming. En slik radar kan hjelpe legene med å diagnostisere en pasient.

## Teknologi som lurar radar

Små autonome systemer vil bli mye brukt i militære operasjoner i framtiden. De vil da også kunne bli et militært problem. Større UAV-er i stor høyde er som regel ikke vanskelige å oppdage og følge. Men mange små og sakte droner vil kunne utgjøre en trussel i mange sammenhenger. Disse UAV-ene vil av og til kunne likne fugler og insekter. Slike UAV-er må bekjempes. Noen nylig publiserte forskningsresultater viser at radar er i stand til å oppdage, følge og skille UAV-er fra fugler og insekter.

Bruk av radar er ikke ufarlig i en militær operasjon. Den største prinsipielle forskjellen på et militært og et sivilt radar-system er – foruten evnen til å se små mål – evnen til å motstå narring eller blanding (jamming). Dette er elektronisk krigføring. Det ene ytterpunktet i elektronisk krigføring er at det blir sendt et så sterkt signal inn i radaren at den ikke ser noe. Det andre ytterpunktet er at radarens signal etterliknes slik at den tror at den har sendt det selv. Da vil radaren tro den ser et ekte mål og rapportere dette, noe som igjen vil kunne utløse meningsløs og ressurskrevende militær respons. Militær forskning og utvikling legger ned mye tid og krefter på å motvirke dette.

Elektroniske støttetiltak betyr at vi tar opp signalet fra radaren for å lære hva radaren gjør og hvordan den opererer. Da vil vi i ettertid kunne gjenkjenne radaren og dermed kanskje også plattformen den befinner seg på, om forholdene ligger til rette for det. I framtiden vil nok de fleste militære radarer kunne gjennomføre både vanlige radaroppgaver, elektronisk krigføring og elektroniske støttetiltak. FFI forsker på alle disse framtidige radaroppgavene. ■

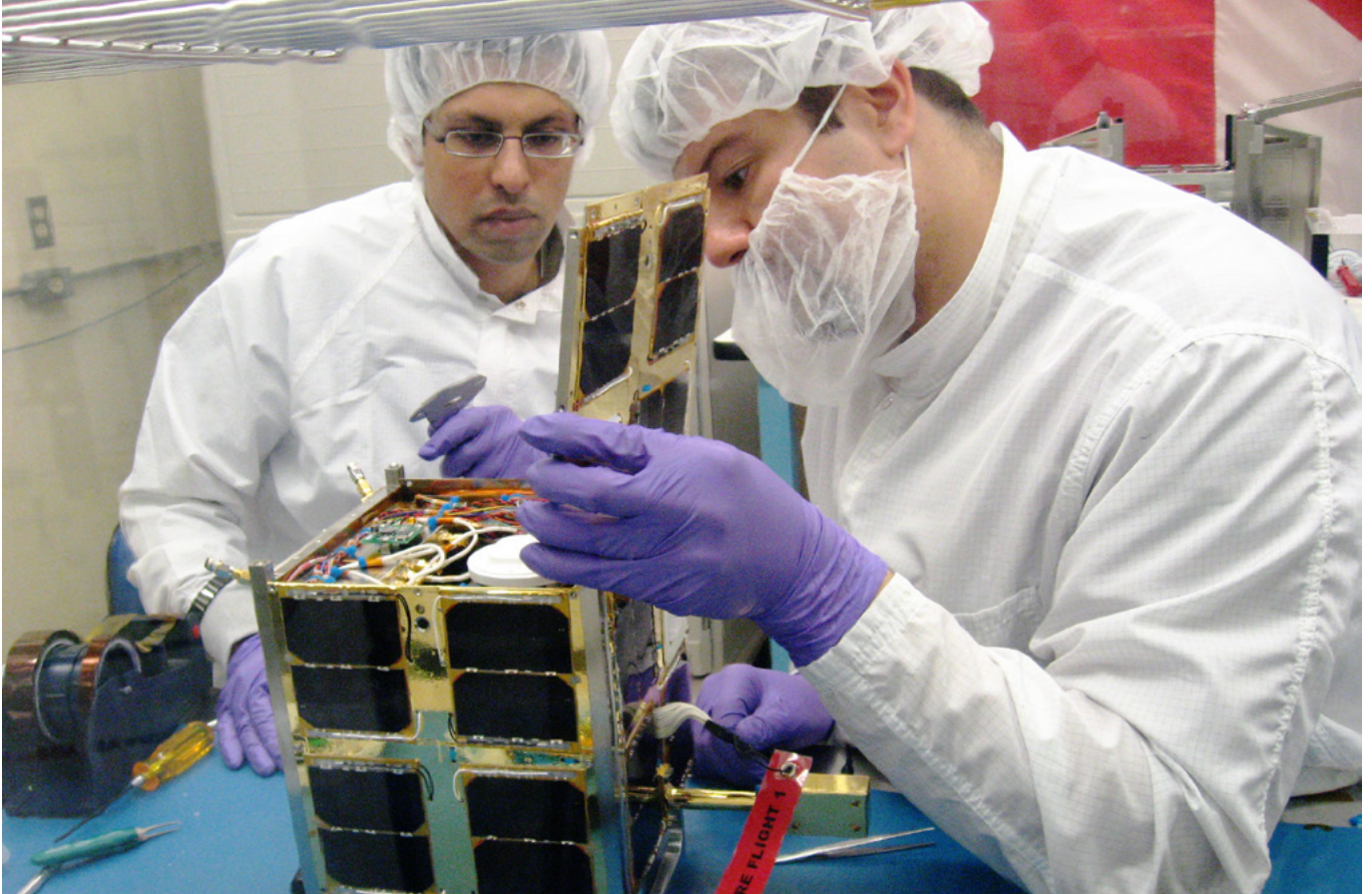


Forskjeller på UAV, fugl og mikrohelikopter i et radarbilde.

## RADAR

*Radio detection and ranging* (Radar) er en sensor som ved hjelp av radiobølger oppdager (*detection*) og måler avstand (*ranging*) til et objekt. Radiobølgene spenner i frekvens fra megahertz (MHz) til et fåtalls hundre gigahertz (GHz). Radar benyttes både militært og sivilt, og den etter hvert mest kjente sivile bruken er nå i biler for å måle avstand til andre biler og slik unngå kollisjoner.

Radar understøtter sanntidsovervåking, og siden radiobølgene går i lysfart undersøkes en sektor fra null til 300 kilometer på 0,002 sekund. Det er heller ikke uvanlig at en radar kan kartlegge et område på 80 000 kvadratkilometer på femten sekunder.



# Romteknologi for Forsvaret



Space Flight Laboratory ved Universitetet i Toronto leverte satellittbussen til AISSat-1, og monterte den for FFI. Her jobber ingeniørene Karan Sarda (til venstre) og Stephen Mauthe med satellitten.  
Foto: UTIAS/SFL

Romalderen regnes for å ha startet i 1957 da satellitten Sputnik ble skutt opp av Sovjetunionen. Romalderen på FFI startet faktisk ikke så lenge etter: 18. august 1962 ble Ferdinand-1 raketten skutt opp av FFI fra Andøya. Den gang ønsket FFI å utforske den øvre atmosfæren (ionosfæren) og innvirkningen på langtrekkende kommunikasjon. Siden da har det vært en kontinuerlig romvirksomhet ved FFI. I 2010 skjøt vi opp Norges første satellitt, AISSat-1, for å samle inn data om skipstrafikk i norske farvann og på verdenshavene.

Hvorfor tok det nesten 50 år å få opp en norsk satellitt? Her er det mange faktorer som spiller inn. Drivkraften i den internasjonale romutviklingen var fra begynnelsen av et militærteknologisk og ideologisk kappløp mellom USA og Sovjetunionen. For alle andre var romprogrammer for krevende og kostbare. Satellitter, og ikke minst oppskyting av dem, var dyre. I Europa begynte det sivile romsamarbeidet på 1960-tallet og resulterte i etableringen av European Space Agency (ESA) i 1975. De første europeiske vær satellittene, Meteosat-1 og -2, ble skutt opp til geostasjonær bane over ekvator i 1977 og 1981. De første jordobservasjonssatellittene til ESA var ERS-1 og -2, skutt opp i 1991 og 1995. Disse var utstyrt med flere radarer for jordob-

servasjon, vind- og bølgemålinger, og et infrarødt kamera for måling av havtemperatur. ENVISAT var en mye større satellitt med ti instrumenter for jordobservasjon. Disse eksemplene viser at den tidlige utviklingen gikk i retning av stadig større og mer avanserte satellitter til høye kostnader. Elektronikk og materialer som skulle tåle belastning av oppskyting og flere års eksponering mot stråling i rommet, var spesiallagde.

På 1960- og 70-tallet var Norge avventende til det europeiske romsamarbeidet, men da planleggingen av ERS-satellittene kom i gang, så de muligheten til å utnytte disse til effektiv overvåking av de store havområdene i nord. Norge gikk inn i ESA i 1987 og var godt forberedt da ERS-1 ble skutt opp i 1991, blant annet som et resultat av utviklingen av digital prosesseringsteknologi ved FFI. Dette la det tekniske grunnlaget for operativ utnyttelse av radarsatellitter i Forsvaret og sivilt.

1990-tallet la grunnlaget for viktige endringer i internasjonal romvirksomhet. Datateknologi ble forbrukervare, vi fikk internett, mobiltelefoner og stor vekst i kommersiell satellittkommunikasjon. I bilindustrien begynte elektronikk å få stor betydning for sikkerhet, komfort og effektivitet. Elektroniske komponenter fikk økt ytelse, mindre fysisk størrelse, lavere pris og de ble mer pålitelige. 1990-tallet var også det første tiåret etter den kalde krigen. Dette fikk konsekvenser for romindustrien. Myndigheter i flere land søkte offentlig-privat partnerskap for bygging og oppskyting av satellitter, og satellittbasert jordobservasjon ble kommersialisert. Vi fikk sivile satellitter som kunne ta bilder med oppløsning på en meter og sivil tilgang til satellittnavigasjon gjennom GPS-systemet. Resultatet ble utviklingen av en «geoindustri» som i dag står for den raskeste veksten globalt innen anvendelser av romteknologi.

Den etter hvert etablerte romindustrien var motivert av behovet for å få ned kostnader, og begynte å dra nytte av teknologit utviklingen slik at mindre satellitter kunne sendes opp i rommet til lavere kostnad. På ledende universiteter var de imidlertid opptatt av å kunne lage svært små satellitter for forsknings- og undervisningsformål. Begrepene «mikrosatellitter» og «micro-space» dukket opp.

### FFI lagde Norges første satellitt

FFI fulgte mikrosatellittutviklingen og utredet bruk av små satellitter til både romforskning (NISSE satellitten) og maritim overvåking (NSAT-1). Ingen av disse ble realisert, men i 2006 var Norsk Romsenter på jakt etter idéer for en ny romsatsing. FFI foreslo da bygging av en nanosatellitt utstyrt med en radiomottaker for å fange opp meldinger fra større skip i det såkalte *Automatic Identification System* (AIS). Dette automatiske identifikasjonssystemet var da etablert av International Maritime Organization (IMO) for å bedre sjøsikkerheten – alle fartøy over 300 tonn skulle kringkaste egen identitet, posisjon, kurs og hastighet på to frekvenser i det maritime VHF-båndet.

FFI hadde gjort beregninger som viste at det burde være mulig å fange opp AIS-meldingene fra lav jordbane. Forslaget fikk støtte, og vi gikk i gang med utvikling av AISSat-1, en satellitt på 20×20×20 centimeter som veier 6,5 kilo. For å holde kostnadene nede brukte vi «micro-space»-tilnærmingen. Det vil si at vi brukte standard industriell elektronikk som siden ble kvalifisert for bruk i rommet etter at delsystemer og hele satellitten var satt sammen. Dette sparte både tid og penger i forhold til etablert praksis i romindustrien. Kongsberg Seatex var etablert som leverandør av AIS-mottakere og leverte nyttelasten. Space Flight Laboratory ved Universitetet i Toronto leverte satellittbussen. Vi ønsket også å få bakkestasjonen så langt nord som mulig, og inngikk avtale med Kongsberg Satellite Services om drift av antenner på Svalbard.

AISSat-1 ble skutt opp sommeren 2010, og skulle være en demonstrasjon på en til tre år. Både den og AISSat-2 fra 2014 leverer fremdeles gode data. Satellittene samler inn data fra omtrent 35 000 skip i døgnet, og bistår både norske og utenlandske myndigheter med å følge skipstrafikk over hele kloden. Satellittene har vist at selv svært små satellitter kan levere nyttige data og tjenester for operativt bruk.

### Hva med skipene som jukser?

FFI er nå opptatt av hvordan vi kan ta erfaringen videre. AIS er svært nyttig for maritim overvåking, men er avhengig av at skipene faktisk følger internasjonale regler. AISSat-erfaringen viser at noen rapporterer feil posisjon, og slår av AIS-senderen i perioder. Andre bytter identitet rett som det er. Det er derfor interessant å utvikle og demonstrere såkalt ikke-kooperativ overvåking ved bruk av andre sensorer. Vi har erfaring med bruk av radarbilder fra store satellitter som Radarsat og den nye europeiske Sentinel-1. Radarbilder gir oversikten både i mørke og gjennom skydekket.

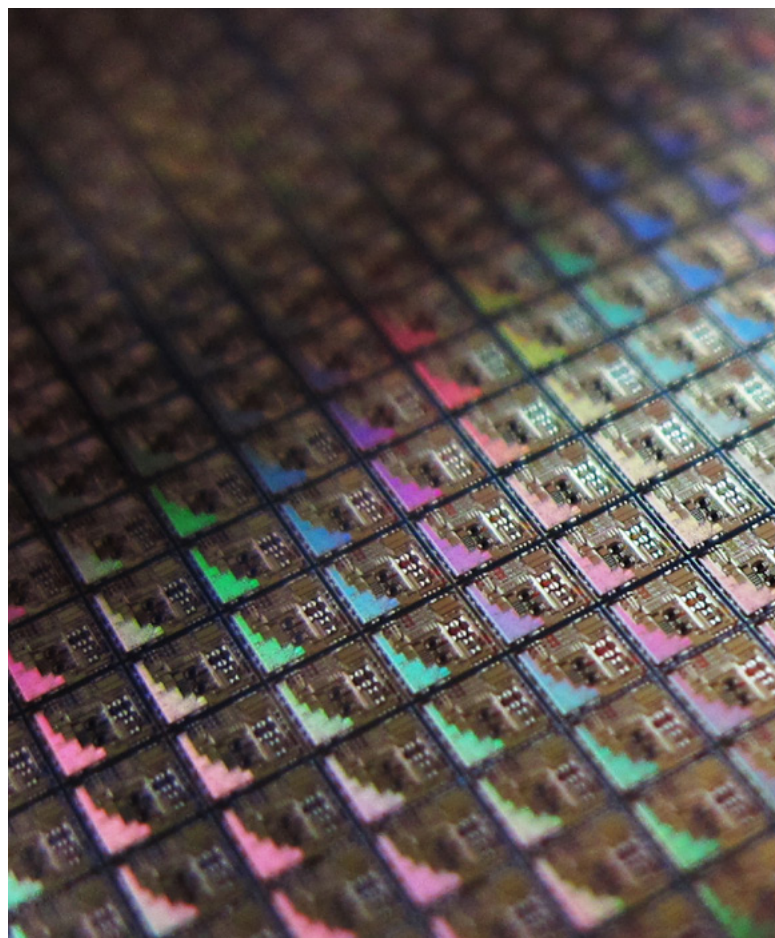
Det er imidlertid vanskelig å identifisere skip kun med radar. Andre teknikker er derfor også interessante og lar seg kanskje realisere fortere, for eksempel lavlyskamera, som er svært lysfølsomme kameraer, og radardetektorer. FFI forsker på begge teknikkene og bruken av dem på små satellitter. Spesialiserte radardetektorer er eksempelvis testet i et pilotprosjekt kalt [LINE](#), der detektorer blir festet til små ubemannede fly (UAV-er) som skal kartlegge radarsignaler de plukker opp fra skip og bestemme posisjonen deres. UAV-er kan fly langt og derfor dekke store havområder bedre enn for eksempel fastmonterte sensorer på land. Radardetektorer er nyttige sensorer når vi vet at skipsfarten langs norskekysten er stor og økende, med mange utenlandske båter som ofte fører farlig last. Radardetektorene kan verifisere at fartøyene faktisk er der deres AIS-sender sier at de er, ved å finne den egentlige posisjonen til navigasjonsradarene på hvert av fartøyene. Avvik mellom signalene fra båtenes AIS-sender og de signalene radardetektorene plukker opp,

kan selvsagt skyldes feil på utstyret i båtene. Det kan også være avvik fordi båtene manipulerer signalene, for eksempel fordi de vil skjule tjuvfiske, smugling eller andre lovbrudd.

### En helhetlig norsk utvikling

De mer avanserte systemene har større behov for strøm, temperaturregulering og styring/stabilisering av satellitten. Avanserte sensorer krever mer strøm enn en AIS-mottaker. Dette kan løses med mer effektive solpanel og noe øking i satellittstørrelse for å få plass til flere solceller. Strømbruken i en radar eller i en avansert signalprosessor produserer imidlertid varme, som må ledes bort og sendes ut i rommet. Gode bilder krever tilstrekkelig eksponeringstid, noe som krever kompensasjon for satellittens og jordens bevegelser. Alt dette betyr at vi må ha en helhetlig tilnærming til satellittens design og produksjon.

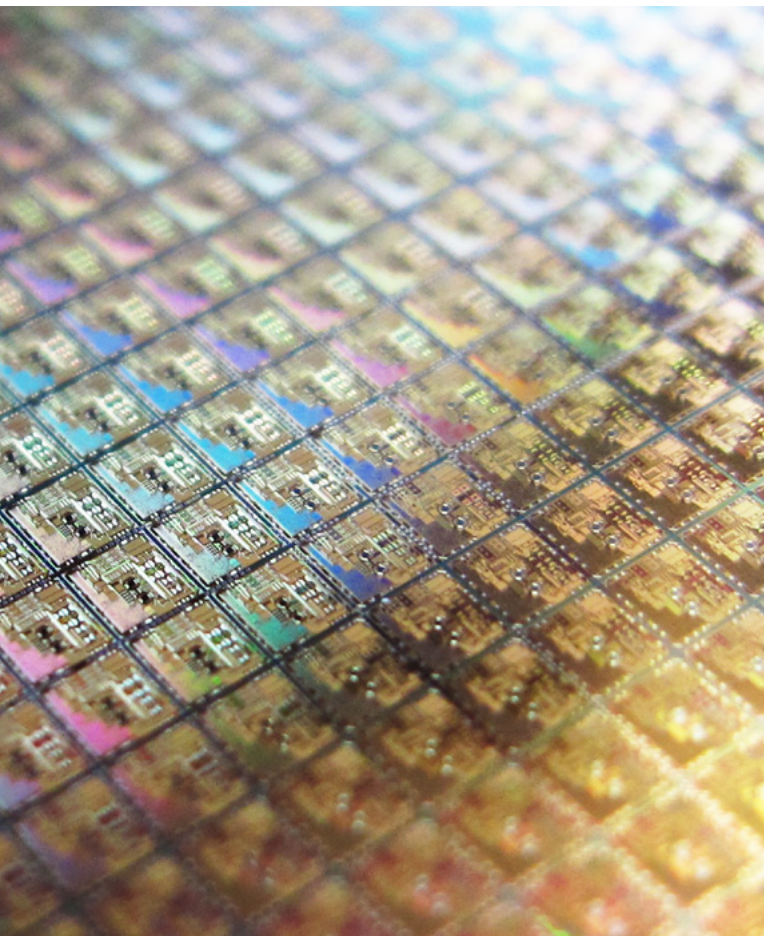
En helhetlig mikrosatellittutvikling er mulig i Norge dersom viljen er til stede. Vi har erfaring med avanserte ingeniørløsninger i maritim sektor der miljøforholdene er krevende,



om enn annerledes enn 500-600 kilometer oppe i rommet. Vi har miljøer som satser og er langt framme innen autonome systemer. Vi har dessuten tradisjon for å se på nytteverdi også innen romvirksomhet, og får oppmerksomhet for dette internasjonalt.

En helhetlig mikrosatellittutvikling er vanskelig å få til i én enkelt sektor. En tverrsektoriell satsing mellom samferdsel, nærings- og fiskeri-, kunnskaps- og forsvarssektorene vil kunne føre fram, men krever en omforent visjon og satsing. Per i dag er det en betydelig organisatorisk utfordring. ■

Fra produksjon av mikroelektronikk:  
En skive av silisium med tusenvis av elektroniske kretser. Hver enhet her inneholder både prosessor og radio-kommunikasjon. Foto: FFI



## MIKROELEKTRONIKK

### - grunnlaget for informasjonsrevolusjonen

Mikroelektronikk er små, veldig komplekse komponenter. Det kan være minnebrikker og prosessorer, som behandler informasjon i form av elektriske signaler, eller det kan være en sensor, for eksempel en bildesensor i kameraer. Mikroelektronikk gir også helt nye muligheter for å lage små satellitter med avansert funksjonalitet.

Mikroelektroniske funksjoner er "stemplet inn" i overflaten av en krystall av silisium. Nøkkelen til den teknologiske utviklingen er at disse elementene tar stadig mindre plass, slik at komplekse funksjoner passer i en komponent på størrelse med en lillefingernegl. På denne måten har mikroelektronikk muliggjort utviklingen av moderne informasjonsteknologi, drevet av sivile massemarkeder.

I militær bruk av mikroelektronikk møter vi noen spesielle utfordringer. Det er for eksempel at komponentenes produktivsyklus er svært kort i forhold til levetiden på militære systemer, og det kan være vanskelig eller dyrt å skaffe reservedeler. I tillegg tilfredsstillers ikke alltid siviltilgjengelige komponenter Forsvarets krav til pålitelighet og bestandighet mot miljøpåvirkning. Det er også dyrt å utvikle mikroelektronikk for spesialiserte militære formål, det er begrenset kontroll på tilgjengelighet av mikroelektroniske komponenter, og vi kan ikke uten videre ha tiltro til at disse komponentene er fri for skadelige funksjoner.

## KAN TEKNOLOGIEN REDUSERE FORSVARETS KOSTNADER?

En videreføring av dagens forsvarsstruktur med bedre teknologi vil ikke nødvendigvis gi en bedre økonomisk situasjon for Forsvaret. Hvorfor er det slik? Og hva kan Forsvaret gjøre med det?

1. oktober 2015 overleverte forsvarssjefen sitt fagmilitære råd til forsvarsministeren. I rådet tegner forsvarssjefen et dystert bilde av framtidens forsvar dersom ikke bevilgningene øker. Forsvarssjefen identifiserer et merbehov i forsvarsbudsjettene fram til 2034 på 175 milliarder kroner sammenliknet med et videreført 2015-budsjett. For perioden 2017-2020 anbefaler han en total øking på 30 milliarder kroner.

FFI har blant annet stått for utarbeidelsen av kostnadsberegningene som ligger til grunn for det fagmilitære rådet. Figuren oppsummerer kostnadsberegningen av den anbefalte strukturen i det fagmilitære rådet. Figuren viser tydelig at kostnadene forbundet med den anbefalte strukturen, langt overgår det estimerte budsjettet. Avviket gir et merbehov i tjuenårsperioden på størrelsesorden 175 milliarder kroner. Hva er årsaken til dette avviket?

### En spesiell kostnadsvekst for Forsvaret

På mange områder har Forsvaret i dag en moderne materiellpark. Samtidig er

det behov for en betydelig modernisering og fornying på andre områder. Dette gjør at Forsvaret står overfor store investeringer i moderne og høyteknologisk materiell i årene som kommer. Historisk ser vi at prisene på forsvarsmateriell øker mer enn prisene i samfunnet for øvrig. Denne enhetskostnadsveksten finnes både på drift og investering, og er en viktig årsak til de økonomiske utfordringene vi ser i figuren, samtidig som en generell ubalanse mellom struktur og budsjett bidrar til et merbehov.

Hvorfor eksisterer denne kostnadsveksten? Forsvaret representerer det som i økonomisk litteratur kalles et turneringsgode. Det vil si at Forsvaret har liten verdi i seg selv, og får først verdi i sammenlikning med andre lands forsvar - da gjerne en motstanders forsvar. På mange måter kan forsvar sammenliknes med en ulykesforsikring. Det finnes mange eksempler på turneringsgoder, kanskje spesielt hentet fra idrettens verden. Formel 1-biler og fotballspillere har for eksempel en tilsvarende sektorspesifikk kostnadsvekst. Forskjellen ligger imidlertid i muligheten til å gjøre noe

med den. I Formel 1-konkurranser har de innført restriksjoner på hva som er lov, og i fotball har de forsøkt å begrense overgangssummene. Det er ikke mange muligheter til å begrense et lands sannsynlighet for å komme seirende ut av en krig.

### Må levere mer for å være like relevant

At forsvar kan sees på som et turneringsgode, gir også opphav til et annet sentralt begrep innenfor kostnadsvekstfeltet, nemlig relativ effekt. For Forsvarets del har dette betydning på flere områder. For det første betyr det at effekten vi får ut av det forsvar vi tar oss råd til å holde oss med, best forstås hvis vi sammenlikner det med en potensiell motstander. Dersom vi antar at denne motstanderen driver en kontinuerlig utvikling av sine egne væpnede styrker, vil en opprettholdelse av den operative nytten av Forsvaret på dagens nivå føre til en redusert relativ effekt, og dermed redusert nytte, av de midlene vi bruker på forsvar. Et godt eksempel på dette er overgangen fra de gamle F-16-kampflyene til moderne F-35-kampfly. For å ha et relevant forsvar for framtiden må med andre ord Forsvaret opprettholde en konstant relativ effekt, og ikke en konstant absolutt effekt over tid.

Det betyr at Forsvaret i realiteten må levere mer i framtiden for å være like relevant som det er i dag. Dette er et kjernepoeng ved den forsvarsspesifikke kostnadsveksten, og gjør at Forsvaret skiller seg fra andre offentlige sektorer. Forsvaret må opprettholde en konstant relativ effekt - i mange andre offentlige sektorer holder det med en konstant absolutt effekt. Dette er den andre årsaken til at relativ effekt-begrepet er så sentralt i omtalen av den forsvarsspesifikke kostnadsveksten.

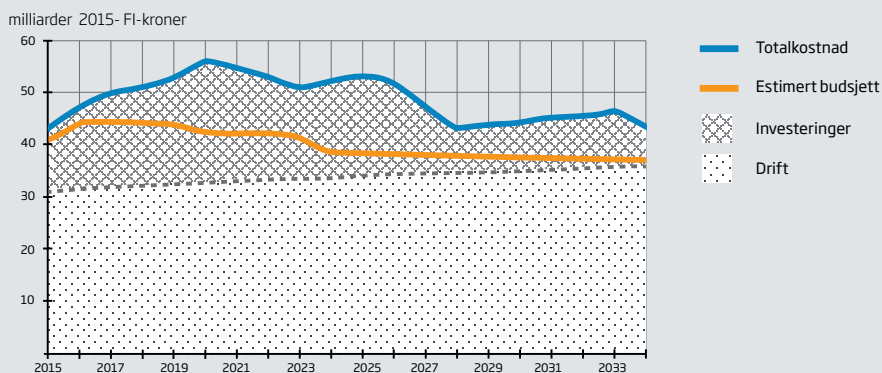
### Utnytte teknologien annerledes enn i dag

Forsvaret kan vurdere å utnytte ny teknologi for å videreføre dagens operative leveranse. Skal den nye teknologien utnyttes på en måte som gjør at den ikke skaper større økonomiske utfordringer, er det imidlertid nødvendig at Forsvaret tenker annerledes enn i dag om hvordan denne teknologien kan utnyttes. En videreføring av dagens struktur med bedre teknologi vil nemlig ikke nødvendigvis gi en bedre økonomisk situasjon for Forsvaret.

For å ta i bruk en ny teknologi med økt operativ nytte kan det bli nødvendig å ta strukturelle grep, som å bytte ut innsatsfaktorer. For eksempel kan Forsvaret bytte personell mot materi-

ell. Gitt et konstant nivå på budsjettet vil vi i så fall måtte akseptere reduserte leveranser. Nedgangen i den operative nytten ved bruk av ny teknologi vil likevel kunne bli mindre enn ved en videreføring av dagens struktur. Det er avhengig av den operative effekten på teknologiene som byttes ut.

Skal vi etablere en langsiktig bærekraftig forsvarsøkonomi, må vi imidlertid skape inndeckning for den forsvarsspesifikke kostnadsveksten. Det betyr at Forsvaret må få dekket denne kostnadsveksten i framtidige budsjetter. Uten en slik inndeckning vil det ikke være mulig å opprettholde en konstant relativ effekt over tid. Vi vil da ikke kunne videreføre et teknologisk nivå på høyde med våre potensielle motstandere.



### Langsiktig økonomisk kostnadsbilde for forsvarssektoren i perioden 2015–2034, anbefalt struktur i Forsvarssjefens fagmilitære råd

FI-kroner er Forsvarsindeks kroner, som er en reell kroneverdi hvor pris- og lønnskompensasjonen som forsvarssektoren mottar fra Finansdepartementet er tatt ut. Dette gjør tallene sammenlignbare med de flerårige budsjettene til Forsvarsdepartementet. Den nederste delen av figuren viser driftskostnaden for den anbefalte strukturen i Forsvarssjefens fagmilitære råd. De estimerte investeringskostnadene ligger øverst i figuren, og utgjør sammen med driftskostnadene totalkostnadene for strukturen. Den oransje linjen i figuren representerer et videreført 2015-budsjett, inkludert tilleggsfinansieringen for de nye kampflyene som ble besluttet i den gjeldende langtidspanen for forsvarssektoren (Prop. 73 S (2011–2012)).

# Augmented Reality på bakken



Foto: Forsvaret

Utvidet virkelighet, bedre kjent som *Augmented Reality* (AR), er en teknologi som kombinerer data fra den fysiske verden med syntetiske data. Militær bruk av AR kjenner vi fra kampflypiloter som får informasjon om andre fly og truende missiler inn på sin skjerm eller rett på visiret. På bakken gjør åser og fordypninger det mer komplisert. En operatør trenger ekstra informasjon fra kart. Skogen skjuler i tillegg fiender på en effektiv måte, og informasjon om vegetasjon stemmer ikke alltid overens med kartet.

Likevel nærmer vi oss en løsning som kan gi bakkestyrkene bedre situasjonsforståelse i strid. Et AR-beslutningsstøtteverktøy for Hæren kan sørge for det. Utviklingsprosjektet blir kalt *Awareness through Augmented Reality* (AWARE) og er et samarbeid mellom FFI, Hæren og det norske selskapet Augmenti Defence. Prosjektet integrerer AR i en fjernstyrt våpenstasjon fra Kongsberg Protech Systems for å presentere taktisk informasjon rett inn i operatørens sikte. Operatøren er typisk en vognkommandør eller en skytter.

Ekstra informasjon fra AR gir bedre samarbeid mellom mannskaper på ulike vogner og mellom dem som er om bord i en vogn og dem som er til fots ute. Dette skaper bedre kjennskap til egne styrkers posisjon, slik at de for eksempel unngår å skyte på hverandre. Samtidig kan de få med seg annen informasjon, som navigasjonsmerker og områder som er forbudte å kjøre i. Slik kan de koordinere kjøreruter og unngå minefelt. AR i sikte-ene fører til mer effektiv utnyttelse av in-

formasjonen og dermed bedre evne til å løse kompliserte oppgaver under stress.

### **AR som passer i Hæren**

FFI har verifisert den operative nytten av å få informasjonen fra det norske informasjonssystemet *Battlefield Management System* (BMS) presentert på denne måten i et AR-system. Operatøren får raskere og enklere oversikt over den taktiske situasjonen, og det fører til raskere og riktigere beslutninger og reaksjoner. AR-symboler (se side 32) som referansepunkt for dirigering av kjøretøy eller tropp har vist seg svært nyttig. I tester gikk innretting av sikte eller våpen mot angitt mål tre ganger raskere med AR enn uten. Andre ting som kan vises ved hjelp av AR er mulige minefelt og anbefalte kjøreruter.

På kort sikt er det mulig å implementere AR i Hærens CV90 kampvogner og Leopard 2 stridsvogner. Disse kjøretøyene har innebygd navigasjonsenhet, og dermed er en viktig komponent i AR-løsningen for disse vognene allerede på plass. En av de tekniske utfordringene som gjenstår, er å få AR vist i det optiske dagsiktet til skytter i stridsvognene.

### **Trender innen AR**

Fra oppstarten av AR-forskningen ved FFI i 2006 og til den siste demonstrasjonen i oktober 2015, har utviklingen kommet langt, også sett i internasjonal sammenheng. Vi forventer rask utvikling innen AR-forskning, både sivilt og militært. Den videre AR-forskningen ved FFI vil følge to spor. Det ene er å



Foto: Forsvaret

### Eksempler på AR-symboler

Øverst vises tilhørighet/klasse og nederst type avdeling/objekt.



Ukjent



Nøytral



Venn



Fiendtlig

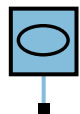


Mål



Veipunkt

FFI har testet ut hvordan symbolene bør se ut på operativt personell og fått mange svar. Noen svar er: Samme symboler som i BMS (Nato-standard), forholdsvis små symboler med moderat eller ingen skalering med avstand, halvgjennomsiktige symboler, stolpe ned som markerer posisjonen.



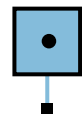
Stridsvogn-avdeling



Infanteri-avdeling



Mekanisert infanteri



Artilleri



Sanitet



Stridsvogn



CV90



### Slik kan AR se ut

Utsnitt av BMS-kart (til venstre), siktebilde uten AR (midten) og siktebilde med AR (til høyre).

Bilder fra kamera leses inn i prosessoren sammen med BMS-informasjonen som skal vises. Nødvendige navigasjonsdata og de grafiske symbolene beregnes og legges oppå bildet.





## Noen AR-utfordringer

Informasjonen må være plassert på riktig sted i bildet av scenen. Vi må da vite hvor vi er og i hvilken retning kameraet ser. Det krever stor nøyaktighet og hurtig oppdatering i sann tid – i praksis trenger vi en meget god navigasjonsenhet. Oppdatering av GPS-signaler i et travelt BMS-nettverk er i dag typisk en gang per 30. sekund. Vi ser altså våre kjøretøy der de var for inntil 30 sekunder siden.

AR-bilde i et optisk sikte krever blokkering av bakgrunnsbelysning i delene av bildet som har AR-informasjon. Visning av AR for fotsoldat, for eksempel på head-up-display eller briller, krever egne løsninger.

God informasjonshåndtering er en forutsetning for at AR skal bli nyttig. Løsninger må være tilpasset ulike operatørroller, og operatørene må ha en viss valgfrihet. FFI har sammen med operativt personell lagt ned mye arbeid for å finne gode løsninger på denne utfordringen.

tilpasse AR i CV90 kampvogner, i samarbeid med BAE Hägglunds, som leverer disse kampvognene. Det andre sporet er å integrere navigasjonshardware og -programvare med AR-programvaren i én og samme boks, for anvendelse på plattformer og systemer uten eget navigasjonssystem.

Navigasjon er et sentralt element i utvikling av AR for både kjøretøy og fotsoldater. For en del anvendelser er fullgode og økonomisk overkommelige løsninger ikke tilgjengelige ennå, men FFI er nær ved å bryte målnøret med noe som kan virke på dagtid og ved rimelig god sikt. For operasjoner i mørke, i tåke eller andre dårlige siktforhold, eller på snødekte vidder hvor det er få holdpunkter i terrenget å navigere etter, er situasjonen en annen. Her er trenden å utvikle mest mulig GPS-uavhengig navigasjon, også fordi vi ikke kan forvente sikre GPS-signaler i en krigssituasjon.

En annen viktig trend er utvikling av løsninger for visning på andre enheter når en vanlig skjerm ikke fungerer så godt. Ulike brilleløsninger eksisterer, men har betydelige svakheter. FFI er

med på å starte et prosjekt i regi av det norske firmaet Kverve, som har et nytt konsept for en AR-brille til bruk for personell. På soldatsiden utvikles dessuten ulike hjelm-monterte displayløsninger med brille eller monokkel med gjennomsiktig skjerm, slik at soldatene ser scenen bak AR-informasjonen på skjermen. FFI har i sitt arbeid med soldat-systemer (NORMANS) vært engasjert i denne utviklingen.

En litt annen AR-anvendelse er å legge inn virtuelle kjøretøy i scenen i forbindelse med feltøvelser. Ved å koble sammen en simulator og reelle feltøvelser kan øvelsen utvides vesentlig uten store kostnader. Dermed kan Forsvaret øve med større styrker enn det som ellers er mulig. ■

# Tid for en blandet virkelighet

Modellering og simulering er en svært anvendbar teknologi for Forsvaret. I dag utnyttes den spesielt i simulatorer for opplæring, trening og øving. Teknologiutviklingen vil i årene som kommer gi helt nye muligheter og åpne for andre bruksområder. Vi vil kunne lage modeller av virkeligheten raskt, og modellene vil ha stor detaljrikdom og omfatte menneskelig adferd. Simuleringer vil kunne bli utført av programvare som består av mange deler i nettverk som sammen kan simulere store og komplekse systemer.

## Fra enkel simulering til blandet virkelighet

Militær simulering deles gjerne inn i tre typer avhengig av i hvilken grad mennesker og utstyr simuleres eller ikke. På den ene siden har vi militære styrker i felt hvor typisk bare våpen og våpenvirkning simuleres (*Live simulation*). Det andre ytterpunktet er at både utstyr og mennesker simuleres i en virtuell verden (*Constructive simulation*). Mellom disse ytterpunktene finner vi simulatorer, hvor mennesker bruker simulert utstyr (*Virtual simulation*). Dette er den mest kjente kategorien, med fly- og kjøretøysimulatorer som eksempler.

Økt tilgang på data om den virkelige verden og muligheten til å skape en virtuell verden som speiler den i stor detalj, gjør det mulig å kombinere de tre typene (*LVC simulation*). Dermed skapes en blandet virkelighet hvor skillet mellom det reelle og det virtuelle viskes bort. Trening i en slik blandet virkelighet kan bli mer realistisk og billigere enn å benytte en av simuleringstypene alene. Stadig mer av informasjonen om stridsfeltet kommer gjennom digitale kanaler, noe som også gjør denne trenden enklere å få til. I de situasjonene hvor stridsfeltet observeres direkte, vil bruk av teknologi for utvidet virkelighet (AR) gjøre det mulig å plassere virtuelle aktører i den reelle verden.

I 2013 gjennomførte FFI for første gang i Norge et forsøk med bruk av blandet virkelighet i en øvelse. Det var en stridsvognøvelse i felt i Hærens Kamptreningssenter. Virtuelle

vennlige og fiendtlige stridsvogner, en simulator for en ubemannet luftfarkost og en artillerisimulator var med, og ga et blandet miljø med flere hundre enheter.

I tillegg til en detaljert digital representasjon av verden, krever en blandet virkelighet også at virkelige fly, fartøy og kjøretøy kan samvirke med tilsvarende virtuelle militære avdelinger som bare er representert i den virtuelle delen. Det har vært en stor utfordring å lage modeller som gjør at virtuelle styrker kan operere realistisk og selvstendig, og som gjør at det er mulig å samvirke med dem på samme måte som vi ville gjort med reelle styrker. På grunn av utviklingen i kunstig intelligens, vil vi få virtuelle styrker som kan opptre relativt selvstendig, forflytte seg og ta beslutninger på en måte som gjør at det er vanskelig å skille dem fra reelle styrker. Nye metoder innen maskinlæring gjør det også mer effektivt å utvikle slike modeller. I tillegg til

## Modellering og simulering

En teknologi som omfatter utvikling og bruk av modeller av systemer og prosesser. Modellene danner i sin tur basis for simuleringer som etterligner systemets eller prosessens oppførsel som er relevant for en bestemt problemstilling. Modeller uttrykkes matematisk og formelt slik at de kan omsettes i programvare som utfører selve simuleringene.

at en blandet virkelighet kan gjøre trening og øvelser mer realistiske med mindre ressursbruk, vil den også kunne teste og evaluere komplekse forsvarssystemer mer effektivt.

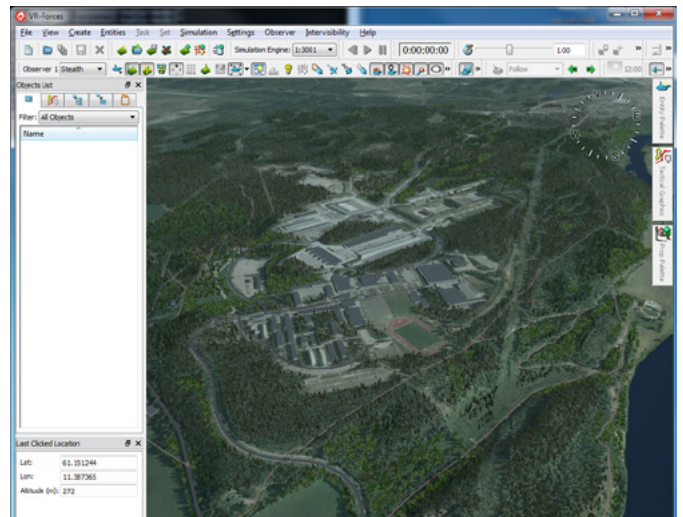
### Felles språk og simuleringer i sky

I flere år har FFI sammen med internasjonale samarbeidspartnere utviklet et digitalt språk for militære planer, ordre og rapporter. Et slikt språk er nødvendig for at virtuelle avdelinger skal kunne ledes og gis oppdrag på samme måte som virkelige avdelinger. Intelligente agenter tar i mot oppdrag, tolker dem og fordeler dem til de underliggende virtuelle styrkene, og koordinerer oppdragene. De intelligente agentene simulerer det militære ledelsesapparatet, og modellene er basert på metoder innen kunstig intelligens og delvis generert automatisk ved hjelp av maskinlæring.

En forutsetning for en slik blandet virkelighet er at det finnes teknologi for distribuert simulering, slik at simuleringer som dekker ulike deler kan virke sammen over et nettverk. Teknologi med protokoller og arkitekturer for distribuert simulering utviklet for militære formål har eksistert i mer enn femten år, og internasjonale standarder gjør nå at militære simulatorer opererer på tvers av landegrenser i Nato-land. Men simulatorene i dag er også selvstendige systemer med for eksempel modeller av virkeligheten som kan være så ulike at de kan føre til "urettferdig strid" når de samvirker i nettverk. Trenden framover blir å trekke ut felles beregninger, modeller og simuleringer og gjøre dem tilgjengelige som militære skytjenester. Modeller og simuleringer av komplekse systemer kan på den måten raskt opprettes ved å sette sammen de riktige tjenestene. Det fører også til at simuleringer kan gjøres tilgjengelige i for eksempel apper og nettlesere, slik at trening kan gjennomføres på hjemmebase, og simuleringer blir tilgjengelige i felt. Å omgjøre simuleringer til skytjenester har også andre fordeler, for eksempel at drift og forvaltning kan skilles fra dem som bruker tjenestene.



FFI har i ti år hatt et stridslaboratorium for å teste og eksperimentere med framtidige systemer og operasjonsmåter. Forskere og militære kommer sammen og gjennomfører operasjoner i aktuelle scenarier i en virtuell eller blandet virkelighet for å vurdere hvordan teknologi og operasjoner påvirker hverandre. Gjennomføring av slike tester kommer til å bli viktigere framover. Foto: FFI



FFI utvikler en slik tjeneste til bruk i simuleringer – en ruteplanlegger som virtuelle kjøretøy benytter for å finne fram i den virtuelle verden. I tillegg til det som vi finner i vanlig bilnavigasjon, dekker denne navigasjonstjenesten både kjøring på vei og i terreng. Den finner ikke bare korteste eller raskeste rute, men tar også hensyn til framkommelighet, fiender, at en ønsker å forflytte seg i skjul, og annet som er viktig for forflytninger i en operasjon. Denne tjenesten er gjort tilgjengelig for andre og benyttes i simuleringer i andre Nato-land.

### **Datafarming og sivil spillteknologi**

Modellering og simulering anvendes av Forsvaret på en rekke andre områder enn trening og øving. Det kan være til utvikling av nye systemer og operative konsepter, og til å støtte planlegging, gjennomføring og analyse av operasjoner. Militære operasjoner er svært komplekse. Det er mange usikkerhetsmomenter og uforutsette hendelser som kan oppstå under gjennomføringen. Modellering og simulering gjør det mulig å planlegge operasjoner raskere, vurdere mange flere faktorer og skape en bedre felles forståelse av det vi skal gjøre. Under framtidige operasjoner vil simuleringer som speiler operasjonen i den virtuelle verden kunne kjøres i parallell, og fores med store mengder data fra stridsfeltet med en militær variant av tingenes internett (se scenario side 11 om IoMT). På denne måten får simuleringer en sentral plass i det resulterende cyber-fysiske systemet. Slik vil vi hele tiden være best mulig forberedt på neste trekk og kan tilpasse oss situasjonen etter hvert som den utvikler seg. At vi hele tiden ligger i forkant og ikke i etterkant av hendelsene gjør at vi får et stort fortrinn over motstanderens beslutningsløkke.

FFI utvikler og vurderer nye metoder innen modellering og simulering sammen med internasjonale forskningspartnere. Datafarming er en ny metode som kan finne fram til kreative og uortodokse handlemåter. I tillegg kan den gi et overblikk over mulighetene som finnes og konsekvensene av dem. Slike metoder sammen med simuleringsbaserte krigspill, som FFI også er i ferd med å utvikle, gir raskt en mye bedre innsikt i avgjørende forhold i en operasjon. Det vil gi en helt annen mulighet for å håndtere økende kompleksitet i kriser og konflikter. Modellering og simulering er uunnværlig for utvikling av framtidige systemer og operasjonsmåter i mer komplekse miljøer. Etter hvert, med innføring av mer autonome systemer, vil tester i et simulert miljø være den eneste muligheten for å skape tillit til

systemene og til å finne ut hvordan ubemannede og bemannede systemer skal virke sammen i team for å løse oppdrag.

Utviklingen innen modellering og simulering drar stor nytte av den raske utviklingen i sivil informasjons- og kommunikasjonsteknologi, inkludert sivil spillteknologi. Tidligere var militære simulatorer spesialbygde systemer for å oppnå tilstrekkelig ytelse, men i dag og framover vil de i mye større grad bli satt sammen av kommersielt tilgjengelige komponenter. Denne trenden, sammen med andre forhold, vil føre til mye større spredning av modeller og simuleringer som innebygde funksjoner i mange forskjellige systemer. Vi vil ikke i samme grad tenke på modellering og simulering som noe eget, men mer som naturlige integrerte funksjoner som vi omgir oss med overalt. ■

## TRE STORE UTFORDRINGER MED CYBERFORSVAR

Det er først når teknologiske tiltak og militær virksomhet sees sammen at vi driver cyberforsvar.

Om du ikke er teknolog, eller ansatt i Cyberforsvaret, lurer du kanskje på om du behøver å vite noe særlig om cyberforsvar? Behøver du i det hele tatt å vite noe om de militære og teknologiske utfordringene vi står overfor? Vi mener at svaret er ja. Verden rundt jobber ulike lands forsvar iherdig med å gjøre cyberforsvar til en integrert del av militære operasjoner slik at trusler mot teknologien vi er avhengige av, ikke rammer vår operative evne. Forsvaret må ha to evner for å drive cyberforsvar: cybersituasjonsforståelse og en forsvarbar infrastruktur. Men for å teste, trene og implementere disse to evnene i realistiske øvelser, må mange som ikke jobber direkte med cyberforsvar forstå hva cyberforsvar er. Beslutningstakere i og utenfor Forsvaret har ikke alltid [den generelle forståelsen av cyberforsvar](#). Det er den første store utfordringen med cyberforsvar.

En sentral del av denne første utfordringen er rolleinndelingen og kravet til sivil-militært samspill. De vanligste cyberangrepene er enkle manipuleringer av nettsider eller overbelastninger med trafikk mot sivile mål, som offentlige nettsider og nyhetsmedier. Slike angrep kan ha både statlig og ikke-statlig opphav og skjer i tusentall over hele verden hver

dag, som oftest i regi av aktivister og kriminelle. I en konflikt kan summen av slike enkeltangrep være med på å påvirke både Norges og omverdenens virkelighetsoppfatning og dermed vårt handlingsrom. Både Forsvaret og politiske beslutningstakere må forholde seg til disse angrepene som en del av motpartens større kampanje for å oppnå informasjonsdominans. Forsvarets rolle er imidlertid å forsvare sitt eget cyberdomene mot en langt mer sofistikert motparts angrep, og å gjøre det på en måte som bevarer evnen til å levere militære operasjoner til politisk nivå. Disse aktørene kan selvfølgelig også angripe sivile mål. Norges samlede beskyttelse mot cyberangrep i en konflikt er summen av de tiltakene hver enkelt systemeier iverksetter selv, hvor Forsvaret er én slik eier. Det kan være i både offentlige eller private virksomheter, og noen av dem eier sivil infrastruktur som Forsvaret er avhengig av. Det er derfor viktig for Forsvaret at aktører satser på cybersikkerhet utenfor forsvarssektoren, og viktig å få inkludert dem i realistiske øvelser. For at Forsvaret skal kunne øve realistisk på militære ledere forstå nok om cyberforsvar, og konsekvensene ved dårlig cyberforsvar, til å prioritere det i øvelser og egne stabsprosesser.

### Fundamentene i cybersituasjonsforståelse

Den andre store utfordringen er **cybersituasjonsforståelse**. Den hviler på tre fundament: Infrastrukturkunnskap, militære operasjoner og trusler. Først må vi ha kunnskap om egen infrastruktur, hvordan den er bygget opp og hva den er avhengig av, og hendelser i infrastrukturen. Vi må vite hvordan infrastrukturen er bygget opp, og vi må være i stand til å skille alvorlige angrep fra tilfeldige driftsforstyrrelser. Med dette er det mulig å forstå det andre fundamentet, hvordan militære operasjoner er avhengige av cyberdomenet. Det tredje fundamentet er forståelse og analyse av trusler mot Forsvarets infrastruktur. Kombinert på riktig måte vil disse fundamentene kunne gi cybersituasjonsforståelse.

Integrering av cyberaspekter (for eksempel våpensystemers avhengighet av spesifikke IKT-tjenester) i militær operasjonsplanlegging krever cybersituasjonsforståelse. Formidling av cybersituasjonsforståelse til de riktige beslutningstakerne gjøres gjennom et cybersituasjonsbilde. Produksjon av et slikt situasjonsbilde krever at Forsvaret evner å rekruttere og holde på personell med høy kompetanse i de aktuelle fagområdene, som

for eksempel skadevareanalyse, hendelseshåndtering og informasjonsforvaltning. Forsvarets rotasjonsordning lar seg svært dårlig kombinere med dette. Operasjonsplanleggerne må på sin side forstå hvordan hendelser i cyberdomenet påvirker militære operasjoner, og evne å planlegge med dette.

### Forsvarbar infrastruktur

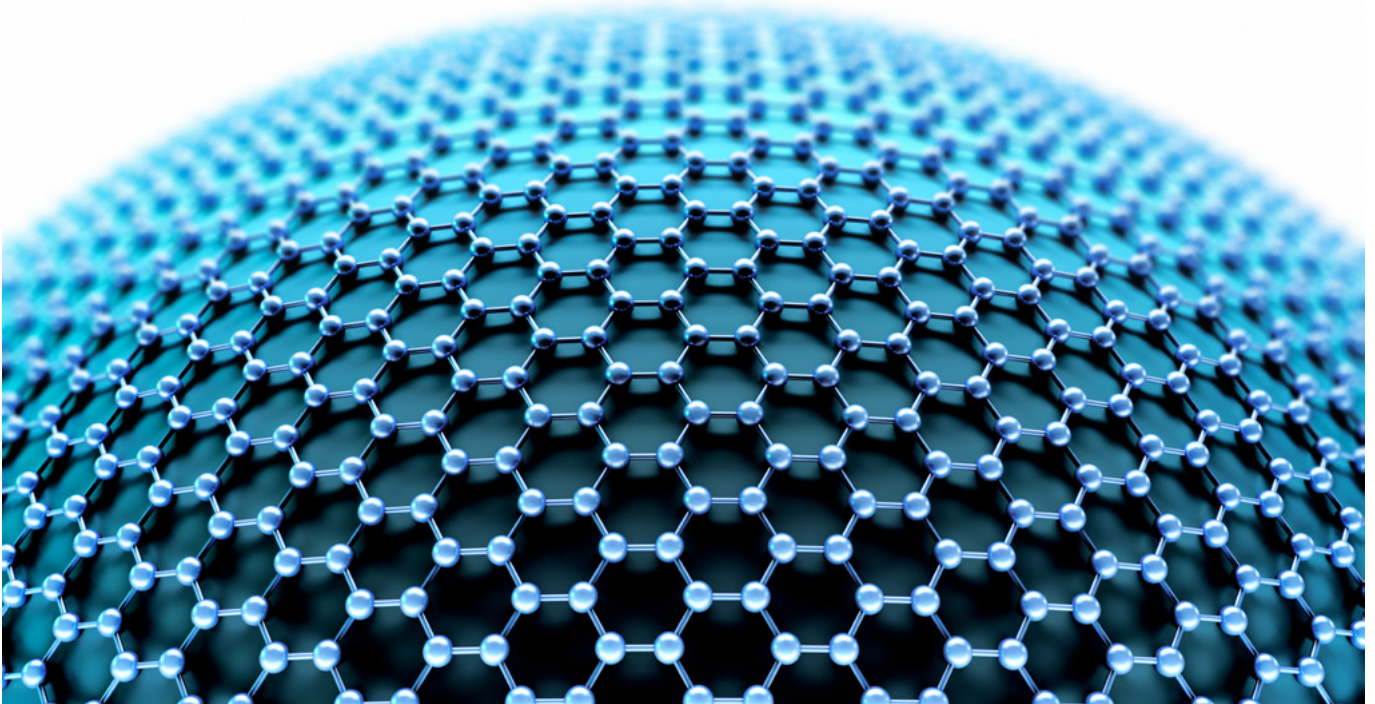
**Forsvarbarhet** er den tredje store utfordringen med cyberforsvar. Det er evnen til å motstå og håndtere trusler og angrep mot egen infrastruktur på en måte som opprettholder operativ evne. Forsvarbarhet oppnås ved å bygge infrastrukturen slik at en ved angrep, eller mistanke om kommende angrep, kan gjøre endringer som tillater fortsatt bruk.

Forsvarbar infrastruktur forutsetter langsiktig satsing ved anskaffelser. Den operative siden må legge til rette for at infrastrukturen enkelt kan endres, for det er først når teknologiske tiltak og militær virksomhet sees sammen at en driver cyberforsvar. Operativt personell lærer dette samvirket gjennom trening og øving. I dag er det et stort forbedringspotensial for å inkludere cyberhendelser i øvelser. Det å bygge opp evnen til å operere med en degradert infrastruktur

krever vilje til å inkludere dette i ulike typer øvelser hos alle nivåer i Forsvaret – på en helt annen måte enn i dag.

De tre store utfordringene henger sammen. Cybersituasjonsforståelse er en forutsetning for å kunne iverksette de riktige tiltakene på rett tidspunkt. Forsvarbarhet gir en betydelig større verktøykasse av tiltak. Uten cybersituasjonsforståelse forstår vi ikke hvordan cyberhendelser påvirker militære operasjoner, og uten forsvarbarhet er handlingsrommet begrenset. Uten en generell forståelse av cyberforsvar både i og utenfor hovedkvarterets stabsprosesser kan cyberforsvar vise seg vanskelig å dyrke fram.

# Bedre beskyttelse med nye materialer



Grafén er en nanopartikkel med potensial for nye materialer. Foto: Shutterstock

Forsvaret har behov for økt mobilitet og bedre beskyttelse av styrkene. Økt mobilitet kan oppnås ved å redusere mengden utstyr som tas med på et oppdrag, eller ved at eksisterende utstyr og komponenter erstattes med nye, lettere varianter som helst har bedre yteevne og et større anvendelsesområde. Økt mobilitet kan i mange sammenhenger gjøre behovet for beskyttelsesutstyr mindre – en beskytter seg ved å være et annet sted enn der konflikten utspiller seg. I noen sammenhenger har soldater likevel behov for å holde en stilling eller konfrontere en inntrenger direkte, og de må da ha den nødvendige beskyttelsen med seg.

Spesielt fotsoldatens utrusting bør bli lettere i framtiden. Utstyret til en fullt utrustet fotsoldat kan komme opp i en vekt på rundt 40 kilo, avhengig av oppdrag og funksjon. Soldater kan få varige fysiske skader av å bære og bruke slikt utstyr over lang tid. Selv en liten vektreduksjon på noen hundre gram for hver komponent kan totalt sett medføre en vesentlig lettere utrust-

ning. Små forbedringer og bruk av lettere materialer enn dem som tradisjonelt benyttes, kan gi det nødvendige fortrinnet i en stridssituasjon. Vekt betyr også mye for fartøy, kjøretøy og fly. Redusert vekt kan dessuten være positivt for mobiliteten, rekkevidden og operasjonsmønsteret til disse plattformene.

Et annet aspekt som indirekte påvirker den operative evnen, er å bruke mindre tid til inspeksjon og vedlikehold. Spesielt i fredstid vil et effektivt vedlikeholdssystem bidra til lavere driftskostnader og økt levetid for Forsvarets utstyr. Har Forsvaret også et kostnadseffektivt logistikksystem for etterforsyning av reservedeler, kan de spare store ressurser.

## Nye, lettere og bedre materialer

Tradisjonelt har de fleste plattformer og øvrig militært utstyr blitt laget av metall. Også i framtiden kommer Forsvaret til å benytte metaller som konstruksjonsmateriale i sine plattformer ettersom dette fremdeles er et svært anvendbart materia-



le. Det utvikles imidlertid lettere og bedre metaller, blant annet ulike legeringer. For å redusere vekten og skreddersy egenskapene til komponenter og utstyr blir nå en del av både sivil og militært utstyr erstattet med plastmaterialer (polymerer) og fiberkompositter. Fiberkompositter består i denne sammenhengen av glass- eller karbonfibre som er lagt inn i et plastmateriale (matrisen), for eksempel epoksy, som mange kjenner fra to-komponentlimet Araldit®. Fibrene tar opp det meste av lasten som påføres, spesielt i fiberretningen. Plastmaterialets oppgave er først og fremst å holde fibrene på plass, og å beskytte dem mot ytre påvirkninger. Sjøforsvaret har for eksempel i flere år operert sine hurtiggående fartøyer i Skjold-klassen. De er laget i glassfiberkompositt med et lettvekts kjernemateriale. Luftforsvarets nye NH90-helikopter har lastbærende konstruksjon i karbonfiberkompositt. Store deler av de nye F-35-jagerflyene er laget i kompositt. Også Hæren går i retning av å bruke mer kompositter framfor metall i sitt utstyr.

Bruken av lettvektsmaterialer vil bli viktigere for å beskytte personell og installasjoner. Ett konkret eksempel er soldat-hjelmen, laget i fiberkomposittmaterialet polyetylen, i Europa mest kjent under navnet Dyneema®. Der en tidligere valgte en tykk metallplate for beskyttelse, vil moderne beskyttelse i større grad ta i bruk keramiske materialer i kombinasjon med fibermaterialer som har høy ytelse, blant annet aramidfiber, mer kjent under navnet Kevlar®, og polyetylen. I tillegg til å erstatte de mer tradisjonelle materialene med lettere materialer, vil geometrisk utforming og kombinasjonen av materialer også kunne bidra til bedre og lettere beskyttelsesløsninger.

Metamaterialer er materialer som er satt sammen på en måte som ikke finnes i naturen. Denne materialtypen har fått mye oppmerksomhet de siste årene. Til forskjell fra kompositter, som også er satt sammen av materialer som ikke finnes i naturen, har metamaterialer et potensial blant annet innen kamuflasje, for å skjule objekter eller endre oppfatningen av hva som ses. Dette er kjent som signaturendring. Videre benyttes metamaterialer til neste generasjons antenner. Mulighetene for annen bruk er mange, men mer forskning trengs før løsninger med metamaterialer, utover antenneløsninger, blir relevante for Forsvaret.

### Nanoteknologi i materialer

Nanoteknologi har vært et stort forskningsfelt de siste tiårene. Innenfor materialteknologi kan nanoteknologi brukes som konstruksjonsmateriale eller beskyttelsesmateriale. Et nanokompositt er et materiale der partikler av nanostørrelse (en eller flere av partikkelens dimensjoner er cirka en tusendels millimeter) er blandet inn i et kontinuerlig medium, for eksempel et plastmateriale eller et lim. Partiklene har i seg selv ekstremt gode egenskaper, som høy stivhet, styrke og god elektrisk og termisk ledningsevne. Ved å fordele kun en liten prosentandel av disse partiklene i plastmaterialet, kan en oppnå mye bedre egenskaper for nanokomposittet enn for plastmaterialet alene.

Karbonnanorør ble oppdaget i 1991 og har siden vært en av de mest lovende partikkeltypene. Karbonnanorør består av sekskantede ringer av karbonatomer. Nanorørens geometri kan sammenliknes med hønsenetting som er rullet til sylindere, med en halvkuleform som lukker røret i hver ende. Det finnes både enveggede og flerveggede karbonnanorør (rør i rør). Nanorørene har i seg selv en relativt komplisert geometri og de har vist seg å være utfordrende å fordele jevnt utover i et plastmateriale. Derfor har grafén de siste årene steget opp som en ny aktuell kandidat. Grafén er en nanopartikkel som kan ses på som et utrullet envegget karbonnanorør. Forskjellige typer nanopartikler benyttes allerede i dag i ulike militære plattform-er og systemer, men det er fremdeles mange utfordringer for forskere å ta tak i.

### Additiv tilvirkning i felt

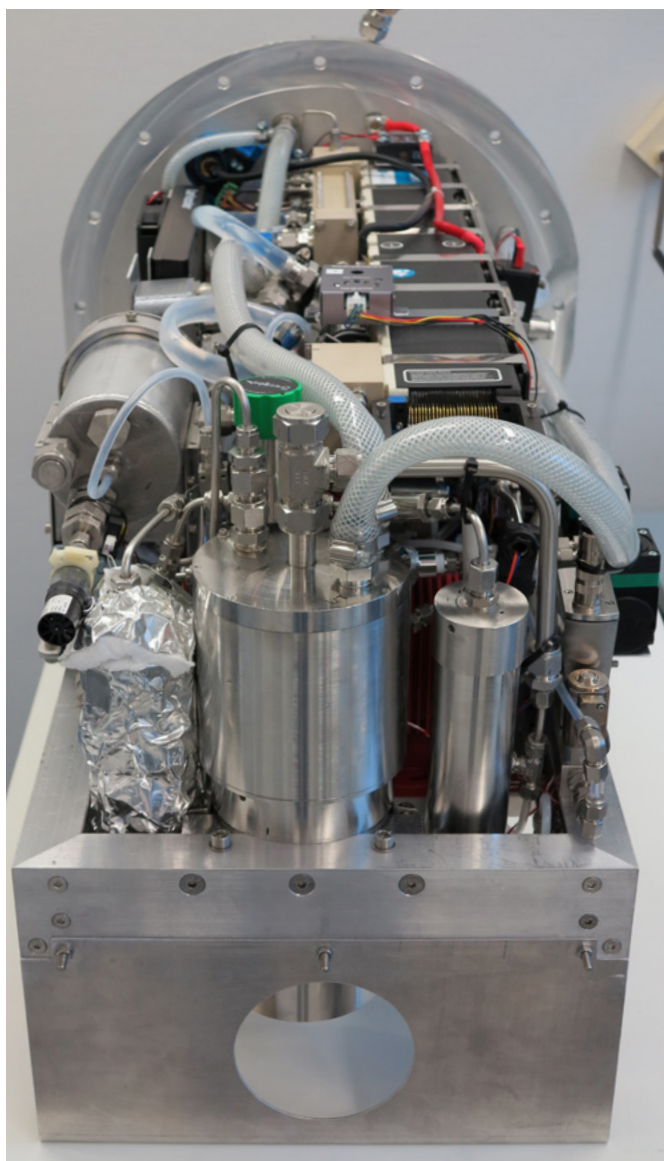
Additiv tilvirkning, bedre kjent som 3D-printing, er en produksjonsmetode som i seg selv ikke er ny, men metoden har de senere årene fått mer oppmerksomhet fordi "hjemme-3D-printere" har blitt tilgjengelige i mindre størrelse og til lavere pris. Tradisjonelle metoder for produksjon av deler tar ofte utgangspunkt i en stor massiv kloss av et materiale, som en deretter skjærer og freser til. I additiv produksjon bygges materialet opp lag for lag. Små dråper av smeltet materiale påføres et underlag på tilsvarende måte som blekk i en vanlig skriver, før det herdes, og bygger til slutt en tredimensjonal konstruksjon. Additiv tilvirkning gir nye muligheter for å lage mer komplekse konstruksjoner.

Forsvaret vil kunne spare både dyrbar tid og logistikk på å ha mulighet til å printe ut deler i felt framfor å vente på forsyning fra et sentrallager. Forsvaret i USA har allerede tatt i bruk denne produksjonsteknologien i felt. Under Nato-øvelsen Cold Response i februar 2016 testet Forsvarets spesialstyrker i samarbeid med FFI ut en containerløsning som en første demonstrasjon på 3D-printing i felt. Resultatene fra demonstrasjonen viste hvor godt ulike typer printere tåler å bli utsatt for svingende temperaturer og andre forhold i felt.

### Modeller gir bedre forståelse

Som annen simulering og modellering, vil gode materialmodeller og analyseverktøy også være viktige i framtiden. Modeller er viktige for å gjøre riktige vurderinger for vedlikehold, reparasjon og valg av materialer. Gode materialmodeller og modelanalyseverktøy fører til at vi sparer tid og penger som tidligere gikk til å gjennomføre eksperimentelle tester. Modellanalyse-ene gjør det også mulig å visualisere innsiden av materialene, og vise flere av mekanismene som opptrer. For fenomener der høye hastigheter inngår, for eksempel anslag av et prosjektil, er modellanalyser ofte eneste mulighet til å forstå hva som skjer i detalj før, under og etter anslaget. Dermed hjelper materialmodeller oss til å utvikle bedre beskyttelse for soldater og materiell. ■

# Strøm uten en tråd



FFI har utviklet dette brenselcelle-systemet for luftuavhengig drift i lukket rom på en ubemannet undervannsfarkost. Foto: FFI

Nesten all teknologi vi bruker er avhengig av strøm. Batterier gir strøm til utstyret Forsvaret trenger i felt der strømmettet er utilgjengelig. Litiumionbatterier (Li-ion) har åpnet for nye bruksområder for elektroniske enheter, mens brenselceller er et alternativ og supplement til batterier. De nye teknologiene fører imidlertid med seg nye sikkerhetsutfordringer. Hvordan kan Forsvaret utnytte disse teknologiene samtidig som sikkerheten er ivaretatt?

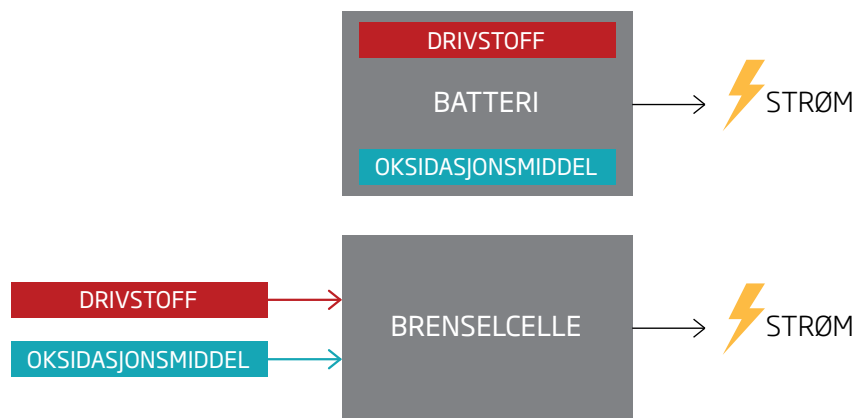
Li-ion har siden 1990-tallet vært nærmest enerådende som strømkilde for kommersiell forbrukerelektronikk. I løpet av de siste tiår har teknologien også hatt sitt inntog i større anvendelser. Li-ion brukes i dag i elektriske biler og store batteripakker installeres på ferger og skip. Brenselceller er ikke like utbredt som batterier, men flere systemer er tilgjengelige på markedet.

Forsvaret har bare i liten grad tatt i bruk disse teknologiene for strømforsyning. Brenselceller brukes ikke, og Sjøforsvarets ubemannede undervannsfarkost HUGIN er Forsvarets eneste ikke-bærbare plattform som er drevet med Li-ion. Dersom store litiumionbatterier og brenselceller skal innføres i Forsvaret, må Forsvaret ta hensyn til norske forhold. Kjennskap til plattform, doktriner og hvordan klima spiller inn på strømforsyningen er viktig. Militære systemer stiller også strengere krav til strømforsyningen enn sivile. Systemene skal være robuste nok til å håndtere ulike klimatiske forhold og direkte beskytning. Om strømforsyningen svikter, kan oppdraget måtte avbrytes eller plattform og mannskapets liv og helse settes i fare.

## Strømforsyning for militære plattformer

Flere av Forsvarets plattformer kan bli bedre med ny strømforsyningsteknologi:

**Ubåt.** Norges ubåter nærmer seg slutten av sin levetid og vil bli faset ut på 2020-tallet. Forsvarsdepartementets to strategiske samarbeidspartnere for nye ubåter tilbyr luftuavhengig framdrift (*air-independent propulsion*, AIP) basert på brenselceller. En av ubåtens fremste egenskaper er å kunne operere skjult, og AIP vil gi langt større utholdenhet enn det som er mulig med oppladbare blybatterier. FFI bidrar i arbeidet med å kartlegge og vurdere de ulike AIP-teknologiene. I tillegg studerer FFI muligheten for å erstatte dagens blybatterier med Li-ion. Vi forventer at det vil gi en operasjonell gevinst blant annet gjennom økt sprintkapasitet, og et redusert vedlikeholdsbehov vil kompensere noe for en større investeringskostnad. Sikkerhet for mannskap og ubåt er imidlertid det viktigste aspektet



Både brenselceller og batterier produserer strøm fra reaksjonen mellom et drivstoff og et oksidasjonsmiddel

Et batteri lagrer drivstoff og oksidasjonsmiddel internt, mens en brenselcelle får det tilført utenfra.

Hvilket av systemene som er mest egnet, avhenger av strømbehovet.

FFI ser på. Li-ion kan slippe ut giftig og brennbar gass ved en feilsituasjon. Dette må håndteres i en ubåt hvor det ikke er mulighet for å ventilere gassene og brann er svært alvorlig.

**Leopard 2 og CV 90.** Store militære kjøretøyer, som stridsvognen Leopard 2 og stormpanservognen CV90, er utstyrt med blybatterier. Disse brukes blant annet til å drive sensorer og annet elektronisk utstyr når hovedmotoren er avslått. Ved å erstatte blybatteriene med Li-ion kan mannskapet få lengre hvileperioder og de kan observere over lengre tid med hovedmotoren slått av. Ved å benytte en hjelpemotor framfor hovedmotor til lading av batterier vil denne kapasiteten økes ytterligere. Det vil også redusere forbruket av drivstoff. Transport av drivstoff i slagfeltet er både dyrt og risikabelt.

**Brigadens kommandoplass.** Brigadens kommandoplass har flere dieselaggregater som forsyner leiren med strøm. Ved å innføre store batteripakker for å håndtere svingninger i strømforbruket, kan Forsvaret redusere antall aggregater og drive de gjenværende mer optimalt. Det vil spare drivstoff og gi mulighet for å redusere støy i kritiske situasjoner. Brenselcellebaserede aggregater vil bidra ytterligere til dette, men teknologien er fremdeles umoden for militær bruk.

**Soldat i felt.** Soldater i felt bærer store mengder batterier, og soldatenes strømbehov vil sannsynligvis fortsette å stige i framtiden. De bruker allerede Li-ion, men utfordringen er

mangel på lademuligheter. Ved å bruke brenselceller og solceller til å lade batterier kan soldatene operere over lengre tid og samtidig redusere vekten på oppakningen.

**Autonome systemer.** Autonome systemer trenger strøm til sensorer. Enkelte systemer bruker også strøm til framdrift, og da vil rekkevidde og pålitelighet være essensielt. Litiumionbatteriene i Sjøforsvarets HUGIN AUV-er er utviklet med støtte fra FFI. AUV til bruk i blant annet etterretningsoperasjoner vil kreve utholdenhet på flere uker. Her peker brenselceller seg ut som det beste alternativet, og FFI har utviklet en prototyp tilpasset AUV.

### Framtiden for strømforsyning i Forsvaret

Innføring av nye systemer for strømforsyning i Forsvaret vil gi økt operativ evne og redusert forbruk av drivstoff. Det er imidlertid avgjørende at sikkerheten er ivaretatt. Sikker bruk av Li-ion og brenselceller krever innsikt i teknologienes egenskaper og Forsvarets behov. FFI har lang erfaring med batterisikkerhet og kan bistå Forsvaret i slike vurderinger. Litiumionteknologien er i dag så moden at den i større grad bør kunne tas i bruk i Forsvaret. Med riktig kunnskap og plattformtilpasset design er sikker bruk av Li-ion mulig også på større militære plattformer. Dermed kan fordelene ved denne teknologien komme til nytte også i Forsvaret. ■

## REFERANSER

- Beadle, A. W. & Diesen, S. (2015). Globale trender mot 2040-implikasjoner for Forsvarets rolle og relevans. *FFI-rapport 2015/01452*. Kjeller, Forsvarets forskningsinstitutt.
- Biscop, S. (2015). *Peace without money, war without Americas. Can European Strategy Cope?* London, Ashgate.
- Bruvoll, S. (2014). Situation dependent path planning for computer generated forces. *FFI-rapport 2014/01222*. Kjeller, Forsvarets forskningsinstitutt.
- Bruvoll, S., Løvild, R. A., Fauske, K. M., Kvernelv, V. Svendsen, G. K. & Hyndøy, J. I. (2015). Simulation-Supported Wargaming for Analysis of Plans. *NATO Modelling and Simulation Symposium*.
- Department of Defense (2012). *Sustaining U.S. Global Leadership. Priorities for 21st Century Defense*. Washington DC.
- EDA (2014). *EDTIB: EDA Analysis of Key Trends*. Brussel.
- EDA (2015). *High-level Group of Personalities on defence research issues statement*. Brussel.
- Elstad, A.-K. & Reitan, B. K. (2015). Mobile information platforms in the military domain. Ålesund, *Norsk konferanse for organisasjoners bruk av informasjonsteknologi (NOKOBIT)*.
- Etterretningstjenesten (2016). *Fokus 2016. Etterretnings-tjenestens vurdering av aktuelle sikkerhetsutfordringer*. Oslo.
- Fiott, D. (2015). European defence-industrial cooperation: from Keynes to Clausewitz. *Global Affairs vol 1, no. 2*.
- Forsvarets forskningsinstitutt (2015). *FFI-FAKTA: RIMFAX A Ground Penetrating Radar for NASA's next Mars Rover Mission*. Kjeller.
- Forsvarets forskningsinstitutt (2004). *Historie 3: Datateknologi*, Kjeller.
- Forsvarsdepartementet (2014). *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren "FDs cyberretningslinjer"*. Oslo.
- Forsvarssjefens fagmilitære råd (2015). *Et forsvar i endring*. Oslo, Forsvaret.
- Grimstvedt, E.S., Aronsen, M., m.fl. (2016). *FFI-RAPPORT 15/02442*. LINE EW-UAS An experimental unmanned system for coastal surveillance using ESM technology. Oslo, Forsvarets forskningsinstitutt.
- Gulichsen, S. (2015). Prinsipper for en bærekraftig forsvarsøkonomi. *FFI-rapport 2015/01432*. Kjeller, Forsvarets forskningsinstitutt.
- Hannay, J., Bråthen, K., Mevassvik, O. M. & Skjeltorp A. (2014). LVC Simulation for Land Operations Training, *NATO Modelling and Simulation Group Symposium*.
- Hove, K. & Lillekvelland, T. (2016) Defence specific inflation (DSI) of goods and services – a refinement of concepts and new estimates. *FFI-rapport 2016/00175*. Kjeller, Forsvarets forskningsinstitutt.
- Hove, K. & Lillekvelland, T. (2014). Defence investment cost escalation – a refinement of concepts and revised estimates. *FFI-rapport 2014/02318*. Kjeller, Forsvarets forskningsinstitutt.
- Luotsinen, L. J. & Løvlid, R. A. (2015). Data-Driven Behavior Modelling for Computer Generated Forces, *NATO Modelling and Simulation Group Symposium*.
- Løvlid, R. A., Alstad, A., Skogsrud, G., Bruvoll, S., Mevassvik, O. M. & Bråthen, K. (2013). Modelling battle command with contextbased reasoning. *FFI-rapport 2013/00861*. Kjeller, Forsvarets forskningsinstitutt.
- Posen, B. (2014). *Restraint. A New Foundation for U.S. Grand Strategy*. Cornell, Cornell University Press.
- Reitan, B. K., Elstad, A.-K., & Gran, C. J. (2016). En ny klasse kommando og kontroll informasjonssystemer (K2IS) – eksperimenter med smarttelefoner og samhandling. *FFI-rapport 2015/02298*, Kjeller, Forsvarets forskningsinstitutt.

Les mer på [ffi.no](http://ffi.no)

Ritchie, M., Fioranelli, F., Griffiths, H. D. & Torvik, B. (2015) Micro-drone rcs analysis. *Proceedings IEEE Radar Conference in South-Africa*.

Stanley-Lockman, Z. (2015). Defence & technology: the US between Silicon Valley and European allies. *Brief Issue 35*. Paris, EU Institute for Security Studies.

Thorvaldsen, T., Johnsen, B. B., Olsen T. & Hansen, F. K. (2015). Investigation of theoretical models for the elastic stiffness of nanoparticle-modified polymer composites. *Journal of Nanomaterials*.

Torvik, B., Olsen, K. E. & Griffiths, H. D. (2014). X-band measurements of radar signatures of large sea birds, *Radar Conference (Radar) 2014 International*.

Les mer på [ffi.no](http://ffi.no)

# FFIs nyhetsbrev kommer jevnlig

Les mer og abonner  
[ffi.no/nyhetsbrev](http://ffi.no/nyhetsbrev)





