VITEN

FORSKNINGSFAGLIG RAPPORT 3. 2016 FORSVARETS FORSKNINGSINSTITUTT

TEKNOLOGI I FELLESOPERASJONER

SCENARIO
Framtidens strid
side 14-15

EKSPERIMENT
med LINE-sensorer
side 17

NETTVERK
med UAV-er
side 24

FFI-RAPPORT 16/02316

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 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 samfunnssikkerhet. 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, ofte sammen med utfyllende rapporter og annet materiale.

Har du spørsmål om VITEN? Ta kontakt med oss: VITEN@ffi.no

Nye krav til teknologi og samhandling

Prop. 151 S (2015–2016), kjent som Langtidsplanen for forsvarssektoren, understreker at Forsvaret i framtiden får behov for større reaksjonsevne og mobilitet av militære avdelinger. Reaksjonstiden vil bli kraftig redusert, og kravet til rettidige beslutninger øker. Dette krever at Forsvaret får mer fleksible løsninger for å dele informasjon, og løsninger som også er motstandsdyktige for ulike former for angrep. Jo mer uoversiktlig en situasjon er, dess viktigere er evnen til å etablere en god felles situasjonsforståelse. I denne utgaven av VITEN skal vi se på hvor viktig dette vil bli for fellesoperasjoner i Forsvaret.

Ved FFI ser på vi på hvordan Forsvarets informasjonsinfrastruktur (INI) kan innrettes for å understøtte nettopp bedre informasjonsdeling. Vi tar utgangspunkt i informasjonen som fundament for militær operativ virksomhet. Dette innebærer at en mengde informasjonskilder kan koples til og fra ved behov, og analyseres og presenteres for brukerne. En slik tilnærming vil kunne bidra til bedre samhandling på tvers av nivåer i vårt eget forsvar, men også med allierte styrker. Nato legger for tiden ned mye arbeid i å gjøre dette mulig gjennom å utvikle standardiserte løsninger.

En framtidig informasjonsinfrastruktur for Forsvaret må også kunne støtte høymobile enheter på en god måte. Ubemannede luftfarkoster (UAV-er) og satellitter kan være med på å gjøre kommunikasjonsinfrastrukturen sterkere gjennom å tilby alternative, supplerende nettverk. UAV-er vil være et fleksibelt verktøy for å kunne tilby kommunikasjonstjenester der de er nødvendige for den til enhver tid pågående operasjonen.

I tillegg til robuste IKT-løsninger er også riktig trening og øving en viktig forutsetning for å effektivisere militær ledelse og for å kunne reagere hurtig og koordinert. I så måte vil moderne simuleringsteknologi og IKT-løsninger kunne spare både tid og kostnader.

Gode sensorer for overvåking er også viktig. FFI jobber i dag blant annet med hvordan passive radiofrekvenssensorer (RF-sensorer) kan bli brukt på satellitt for å peile skipenes navigasjonsradarer og sammenstille dem med de større skipenes Automatic Identification System (AIS). Et annet eksempel på et viktig område som FFI jobber med i dag, er elektronisk krigføring (EK), hvor målet er å kontrollere det elektromagnetiske spektrum for å øke strids- og overlevelsesevnen til egne styrker.

For at Forsvarets mange enheter skal kunne samhandle, må de kunne snakke sammen og dele informasjon internt, men også med våre allierte. Da må informasjon, og ikke systemer, være i sentrum. Forsvarets styrker og plattformer må også beskyttes mot angrep på best mulig måte. Dette er viktige forutsetninger for Forsvarets kampkraft i et nytt og uoversiktlig trusselbilde.

Anders Eggen

Sjef for avdeling
Cybersystemer og elektronisk krigføring
Forsvarets forskningsinstitutt

UTGIVER:
Forsvarets forskningsinstitutt

FORSIDE/ILLUSTRASJON:
FFI

REDAKTØR:
Wenche Gerhardsen

DESIGN:
Isabel A. Nordang

viten@ffi.no

BIDRAGSYTERE:
Ole Ingar Bentstuen
Karsten Bråthen
John-Ivar Christensen
Anders Eggen
Eli Gjørven
Raymond Haakseth
Hilde Hafnor
Bjørn Jervell Hansen
Ole-Erik Hedenstad
Tor-Odd Høydal
Berit Jahnsen
Vivianne Jodalen
Lars Landmark
Erlend Larsen
Bjørnar Libæk
Frode Lillevold
Ketil Lund
Robert H. Macdonald
Federico Mancini
Jonas Moen
Nils Nordbotten
Tore Smestad
Åshild Grønstad Solheim
Tore Ulversøy
Jan Erik Voldhaug

FOTO/ILLUSTRASJON:
FFI, Freepik.com

Trykk: Fladby as

Opplag: 2000
P ISBN: 978-82-464-2834-5
E ISBN: 978-82-464-2835-2

ABONNER PÅ
VÅRT NYHETSBREV:
ffi.no/nyhetsbrev

FØLG OSS PÅ:
Facebook
Instagram
ffi.no

Forsvarets forskningsinstitutt
Besøksadresse:
Instituttveien 20
2027 Kjeller

Postadresse:
Postboks 25
2027 Kjeller

Telefon:
63807130

MILJØMERKET
07 AURSKOG - 241 379

TEKNOLOGI I FELLESOPERASJONER

4 Introduksjon
6 Fra system til informasjon
9 Tre grep for bedre tilgang til informasjon
12 Ledelse og trening i framtiden
16 Passiv sensor som gir oversikt
21 Elektronisk krigføring i moderne operasjoner
23 En flyvende komponent i kommunikasjonsinfrastrukturen
26 Referanser

Hva vi gjør på teknologinivå får konsekvenser for den operative fleksibiliteten. Vi går fra tradisjonell systemtankegang til informasjon som fundament for militær virksomhet i teknologiforskningen.

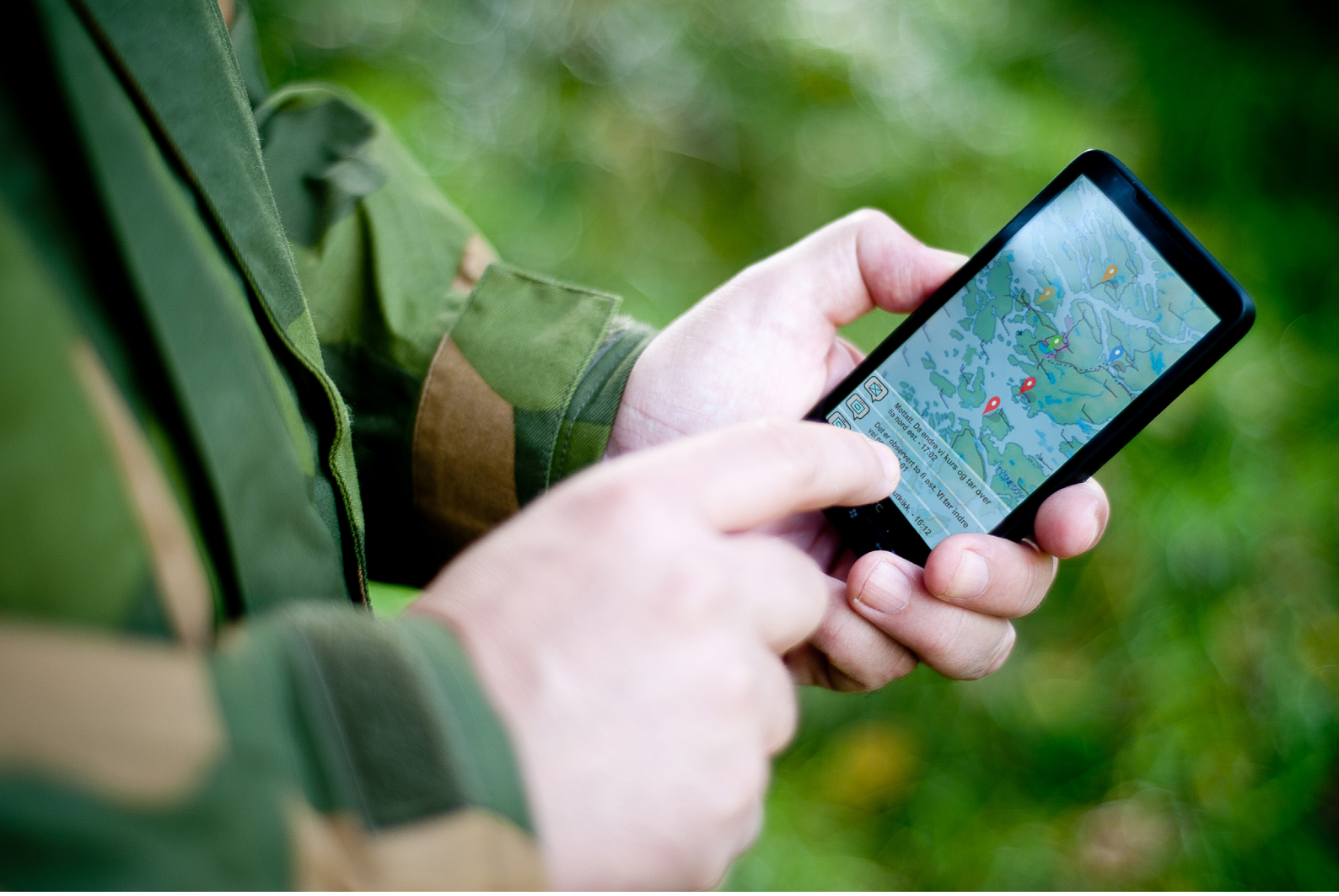
Fra system til informasjon

Etablering av god felles situasjonsforståelse forutsetter evnen til å innhente, dele og utveksle informasjon. Jo mer uoversiktlig og kompleks en situasjon er, dess større og mer sammensatt evne behøver vi for å etablere god nok situasjonsforståelse. Denne evnen kan vi ikke bare bestille. Vi må utvikle den. Teknologi, organisasjon og kultur er tre viktige faktorer. Evnen til å dele informasjon er avhengig av dem, og evnen utvikles i samspillet mellom de tre faktorene.

Forsvarets informasjonsinfrastruktur (INI) er vevd inn i alle prosessene i Forsvaret og er en sentral premissleverandør i arbeidet med å utvikle en mer gjennomgående organisatorisk evne til å utnytte informasjon «på kryss og tvers». Evne til å dele informasjon henger derfor ofte sammen med organisatorisk fleksibilitet.

Teknologien som premissgiver

Dagens informasjonsinfrastruktur gir ikke i tilstrekkelig grad det mulighetsrommet Forsvaret trenger for å kunne operere mer smidig og tilpassingsdyktig på virksomhetsnivå. INI-løsningene er per i dag for eksempel ikke dimensjonert for å håndtere et sterkt økende informasjonsbehov, informasjonsvolum eller



En ny klasse kommando- og kontrollsystemer (K2IS) bryter med den tradisjonelle informasjonsflyten for rapportering i Forsvaret. Det nye er at systemet bygger på direkte informasjonsdeling mellom soldatene, som får flere måter å dele informasjon på. Informasjonsdeling mellom mobile enheter er en del av dette. Fotomontasje: FFI

informasjonsmangfold. Forsvarets hierarki, kommunikasjonsstrukturer og arbeidsprosesser er ofte tydelig gjenspeilet i disse løsningene hvor tilgang til og deling av informasjon, som for eksempel databaser, dokumenter og meldinger, ikke uten videre kan gjøres utover systemgrensene.

FFI ser derfor på hvordan Forsvarets informasjonsinfrastruktur bør innrettes for å bidra til at Forsvaret får det mulighetsrommet de faktisk trenger for å øke evnen til å dele informasjon. Vi tar utgangspunkt i data eller informasjon som fundamentet for militær operativ virksomhet. Dette kaller vi datasentriske prinsipper, arkitekturer eller strategier.

Smarttelefonen er bygget rundt datasentriske prinsipper. Den brukes til alt – overalt – uavhengig av organisasjonen du tilhører eller situasjonen du befinner deg i. En mengde informasjonskilder kan kobles til og fra etter behov. Designet er globalt. Slike datasentriske prinsipper kan vi også utnytte i teknologidesign og nettverksløsninger i organisasjoner som har større og mer avanserte informasjonsbehov. Dette representerer et skifte i måten vi tenker, designer og organiserer teknologiløsninger i organisasjoner på. Skiftet går ut på å vektlegge data som fundament for organisasjonens virksomhet, mer enn på prosesser og strukturer. Dette betyr at vi skiller dataressursene fra informasjonssystemene, og gjør det mulig å utvikle nye konsepter for styring av informasjon. Ved en slik tilnærming reduserer vi også faren for å reprodusere gamle strukturer og prosesser i nye teknologiløsninger.

HVA ER?

Organisatorisk fleksibilitet

Begrepet fleksibilitet i arbeidslivet handler om alt fra friheten til å jobbe hvor som helst og når som helst til hvordan en organisasjon i stort klarer å tilpasse seg omgivelser i kontinuerlig endring. Militær fleksibilitet betyr at operative styrker må ha evnen til hurtig å omorganisere til flere typer oppdrag, også oppdrag som nærmest er umulig å forutsi.

Organisatorisk fleksibilitet er mulighetsrommet vi disponerer innenfor bestemte rammer. Hvis målet er å øke den operative fleksibiliteten, må vi se på om organisasjonen har de grunnleggende forutsetningene for å oppnå dette målet.

Informasjon i graderte nett

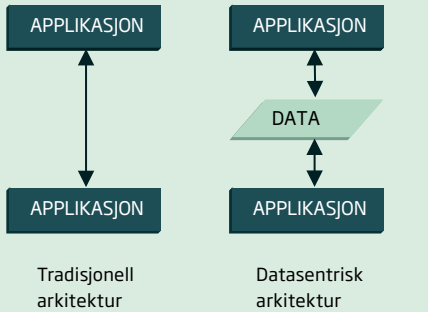
Ved FFI ser vi hvordan vi kan gå fra systembasert sikkerhetsstyring til sikker styring

Langtidsplanen for forsvarssektoren sier at

«Moderne krisehåndtering og krigføring kjennetegnes av korte tidslinjer, komplekse situasjonsbilder og stort informasjonsbehov. For å forbedre Forsvarets evne til å føre høyintensiv strid og håndtere kriser, må evnen til å fatte og iverksette rettidige beslutninger styrkes. Bedre situasjonsforståelse kan oppnås ved at data fra mange kilder sammenstilles i økende grad og gjøres tilgjengelig for brukere på ulike nivåer. Sensorer, våpen og plattformer knyttes sammen, uavhengig av forsvarsgren og våpenart, for å bidra til økt operativ evne. Evnen til å understøtte gjennomgående informasjonsutveksling fra stridsteknisk til strategisk nivå styrkes gjennom standardisering av kjernetjenester og fleksible løsninger for sikring og utveksling av informasjon.»

Prop. 151 S (2015–2016) s. 103

APPLIKASJONER KOMMER OG GÅR – DATAENE BESTÅR



av informasjon. I dag er digital informasjonssikkerhet knyttet til systemet, nettverket eller maskinen som informasjonen er en del av. Dagens sikkerhetslov er systembasert, og sikkerheten baseres på å beskytte grensene til systemene og nettverkene. Det betyr i praksis at selv om det bare finnes ett gradert informasjonsobjekt (for eksempel et dokument) i nettverket, blir all annen informasjon automatisk også en del av det graderte nettverket. Dermed blir mye ugradert informasjon utilgjengelig utenfor nettverket. En mer datasentrisk sikkerhetstilnærming kan bidra til å løse noen av disse utfordringene.

Vi kan flytte sikkerheten fra system- og nettverksnivå ned til informasjonsnivå. Da kan vi beskytte de enkelte dataelementene i stedet for å sikre hele systemet eller nettverket. Adgang til informasjonen blir dermed bestemt ut fra det enkelte informasjonsobjektet, ikke ut fra hvilket nettverk det er lagret på. Dersom et slikt datasentrisk sikkerhetskonsept blir realisert, vil det kunne bidra til en dramatisk bedre organisatorisk evne til militær informasjonsutveksling.

Automatisert informasjonsutveksling

Hvis vi kobler to applikasjoner sammen, har vi automatisert informasjonsutvekslingen mellom dem. Men applikasjonene skjønner ikke nødvendigvis meningsinnholdet i informasjonen som utveksles eller hvilken sammenheng den skal brukes i. Vi må derfor knytte metadata til informasjonen de utveksler. En slik merking av informasjon vil for eksempel være en del av løsningen i en datasentrisk sikkerhetsstrategi.

FFI ser på avanserte anvendelser av metadata. Ved å utvikle gode teknikker og metoder kan vi få til en betydelig høyere automatiseringsgrad av informasjonsintegrasjonen, tilgjengeligheten og analysen av informasjonen. Å få på plass slike automatiserte mekanismer i infrastrukturen vil kunne bidra mye til militær evne til informasjonsutveksling.

Ny klasse K2IS

Reell samhandlingsevne henger sammen med den reelle evnen til å utveksle og dele informasjon. Datasentriske løsninger kan gi betydelige bidrag til å legge til rette for dette gjennom etableringen av en ny klasse kommando- og kontrollsystemer (K2IS). Den nye klassen er fleksibel, åpen og bryter med den hierarkiske informasjonsflyten. Den inkluderer og involverer brukerne på nye måter. Vi snakker om systemer som har brukergenerert innhold, datasentrisk arkitektur, høy tilgjengelighet, er enkle i bruk og virker på mobile plattformer. Disse egenskapene er ennå ikke vanlige i militære systemer.

Sammen med Forsvaret har vi ved FFI eksperimentert med noen av de mest sentrale mekanismene i den nye klassen K2IS. Eksperimentene har omfattet organisatoriske, prosessuelle og tekniske problemstillinger ved slike systemer. Vi har belyst områder som Forsvaret i dag opplever som utfordrende og problematiske. Eksperimentene har vist at slike løsninger er teknologisk gjennomførbare uten store ressurser. Forskningen indikerer tydelig at denne klassen av K2IS kan få stor betydning for operativ evne til å dele informasjon.

Tre grep for bedre tilgang til informasjon

Ikke lås informasjonen til systemer. Etabler rammer for å koble egne systemer sammen med systemene til våre samarbeidspartnere. Lag en robust og sikker infrastruktur som støtter militære operasjoner i både fred og krig. Dette er grep som vil gjøre Forsvarets informasjonsinfrastruktur (INI) til en grunnleggende ressurs for Forsvaret på linje med våpensystemer.

Tradisjonelt har informasjonssystemer vært komplette: alle funksjoner, fra kommunikasjon og lagring og helt opp til grensesnittet mot brukeren, har vært inkludert. Slike systemer kaller vi silosystemer. De er utbredt i Forsvaret i dag. Selv om slike systemer fungerer bra til det de er ment å gjøre, fungerer de ofte dårlig i samspill med andre systemer. Data blir i stor grad låst inne, og kan ikke enkelt deles med andre informasjonssystemer. Det er heller ikke mulig å gjenbruke enkeltfunksjoner i andre sammenhenger. I silosystemer må alle funksjoner lages på nytt i hvert system.

Forsvaret har også en utfordring i krav til sikkerhet. Data med ulike graderingsbehov lukkes inne i separate sikkerhetsdomener. Dette begrenser muligheten til å utveksle informasjon i enda større grad.

Hva kan Forsvaret gjøre?

Mange av de funksjonene som i dag håndteres internt i applikasjoner, kan med fordel være fellestjenester i Forsvarets informasjonsinfrastruktur (INI). Slike funksjoner kan være lagring og gjenfinning av data, sikkerhetsfunksjoner, konvertering av data, karttjenester og samhandlingstjenester, som for eksempel e-post og chat.

På sikt bør derfor Forsvaret sørge for en overgang fra silosystemer til informasjonssystemer som kombinerer en funksjonsrik INI med et sett av mindre tjenester som kan settes sammen etter behov. På den måten kan Forsvaret raskt sette opp tilpassede informasjonssystemer for styrker i en fellesoperasjon.

Denne overgangen vil frigjøre dataene fra systemer og applikasjoner og gjøre dem mer tilgjengelige for de som trenger dem. Da vil innholdet og andre egenskaper ved selve dataobjektene, heller enn lagringssted eller opprinnelsesapplikasjon, kunne avgjøre hva de best kan brukes til. Å utnytte dataene på nye måter vil imidlertid også kreve nye sikkerhetsløsninger.

Hvordan samarbeide med andre

Forsvaret må være i stand til å samarbeide med andre, først og fremst andre Nato-land, men også med sivile partnere. Slikt samarbeid innebærer i dag å kople sammen systemer. Med modulære funksjoner og en INI med fellestjenester, vil vi i stedet utveksle informasjon mellom partnernes infrastrukturer. Alle applikasjoner vil da kunne snakke sammen gjennom disse. Nato legger for tiden mye arbeid i å gjøre dette mulig gjennom utvikling av standarder og definisjoner av felles kjernetjenester. Mye av dette arbeidet foregår innenfor Federated Mission Networking (FMN). Det er en Nato-satsing som skal legge til rette for raskt å sette sammen nye nettverk i internasjonale operasjoner. FMN inkluderer både prosesser og teknologiske rammer.

På sivil side er det spesielt nødetatene det er aktuelt å samarbeide med. I tillegg til å utveksle informasjon kan det være aktuelt å dele infrastruktur. Det vil si at Forsvaret stiller noe av sin infrastruktur til disposisjon for nødetatene, eller omvendt. Ved å samarbeide med sivile får Forsvaret fort utfordringer med sikkerhet fordi sivile etater normalt opererer på andre sikkerhetsnivåer. For å utveksle informasjon i et slikt samvirke, trenger

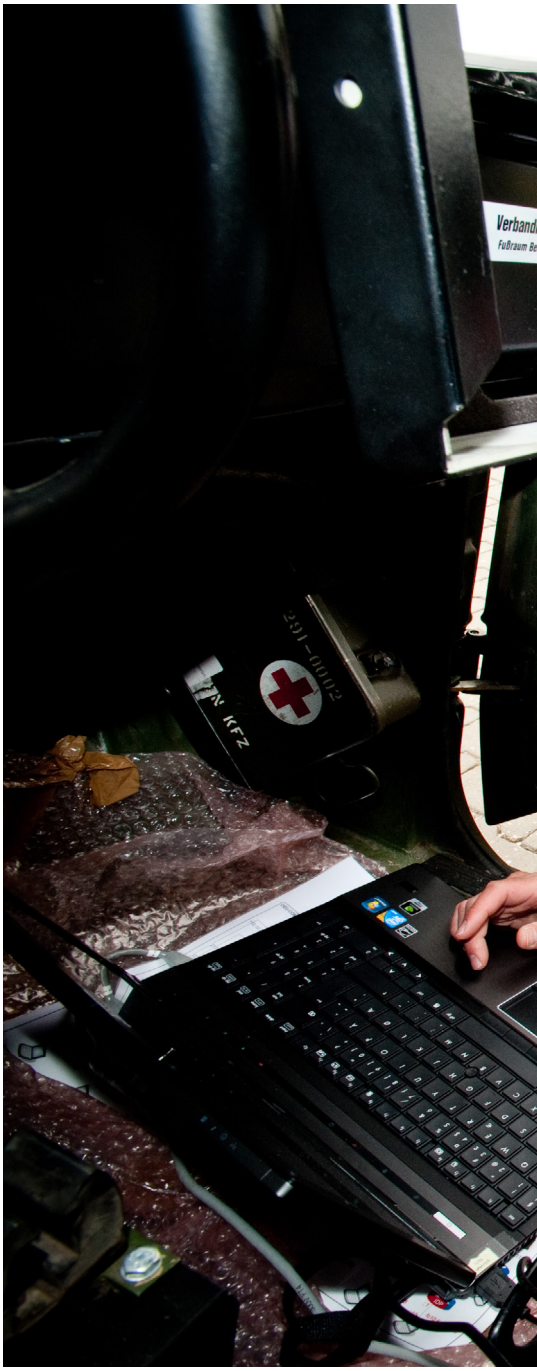
vi mekanismer som kan koble sammen eksisterende systemer og infrastruktur. Disse mekanismene må kunne utveksle informasjon på en sikker og effektiv måte.

Hvordan sikre informasjon og infrastruktur

Militære systemer har i stor grad vært fysisk adskilte i ulike sikkerhetsdomener. En høyere grad av sammenkobling, både internt og til eksterne, har en pris: Sannsynligheten for at en fiende klarer å bryte seg inn i våre systemer øker, og konsekvensene av uønskede hendelser kan forverres ved at større deler av infrastrukturen rammes. Denne sikkerhetsrisikoen må vi redusere til et akseptabelt nivå slik at Forsvaret fortsatt kan oppnå den økte operative effekten som en mer utbredt informasjonsdeling kan gi, uten at INI blir så sårbar at det blir for risikabelt å bruke den i praksis.

Dette krever nye sikkerhetsløsninger for hvordan informasjonens konfidensialitet, integritet og tilgjengelighet kan beskyttes når den ikke lenger er knyttet til spesifikke applikasjoner eller systemer. Den første artikkelen i denne utgaven av VITEN beskriver hvordan merking av informasjon er en måte å løse dette problemet på. En slik løsning er imidlertid avhengig av en infrastruktur som kan og vil bruke merking på riktig måte. For eksempel vil noen systemer måtte kontrollere all informasjon som går inn og ut av våre nettverk og sørge for at bare den som er merket for deling slippes ut. Samtidig må vi stole på at de andre interne systemene merker informasjonen riktig. Dette stiller høye krav til tilliten vi må ha til disse systemene og byr på helt nye sikkerhetsutfordringer.

Systemene som er i bruk i dag er verken tilrettelagt for merking eller for å fungere i en sammenkoblet infrastruktur. Derfor har vi konsentrert oss om å sikre de nye mekanismene som skal kontrollere informasjonsflyten mellom systemene så godt som mulig, og vi tillater foreløpig bare utveksling av noen få utvalgte datatyper vi har god kontroll over. Hadde disse systemene vært helt sikre, ville det i prinsippet ikke vært behov for noen sikker sammenkoblingsløsning utover beskyttelse mot menneskelige feil. Slike feil er forøvrig også en stor utfordring. Hvis en autorisert bruker bevisst eller ved en feil merker sensitive data slik at de likevel slippes ut, er det lite systemene kan gjøre for å hindre en lekkasje. Mer avanserte mekanismer basert på maskinlæring og analyse av dataene er en lovende tilnærming som FFI forsker på. En slik tilnærming kan bli aktuell i framtiden.



Forskerne Ketil Lund, Trude Hafsøe Bloebaum og Jan Erik Voldhaug jobber med å installere IKT-systemer i et tysk militært kjøretøy under et eksperiment med det flernasjonale forskningsprosjektet Coalition Networks for Secure Information Sharing (CoNSIS) i Greding i Tyskland i 2013. Målet er blant annet å forenkle deling av data mellom nasjoner. Foto: FFI

Ledelse og trening i framtiden

For å klare å gjennomføre operasjoner i lys av alle de nye utfordringene vi står overfor, må Forsvaret fornye sine kommando- og kontrollsystemer og endre måten de gjennomfører ledelsestrening på.

Ingen vet sikkert hva den neste konflikten vil handle om. Den kan komme raskt og vil sannsynligvis ikke gi rom for å bruke lang tid på oppsett og utplassering, langt mindre anskaffelse av løsninger innen informasjons- og kommunikasjonsteknologi (IKT). Forsvarets IKT-løsninger må derfor kunne brukes i en rekke ulike scenarioer, de må være raskt klare til bruk, og de må kunne understøtte en rask oppskalering fra fred til krise og krig. Sammenkobling av ledelsesverktøy og treningssystemer legger til rette for en betydelig kompetanseheving, og gjør det mulig «to train as you fight». Bare gjennom en vellykket kombinasjon av personell og materiell, kan Forsvaret omsette ny teknologi i operativ effekt.

For å være best mulig rustet mot den neste trusselen må Forsvaret løpende ta i bruk ny teknologi når den blir tilgjengelig. Utviklingen av sivile IKT-løsninger går svært raskt sammenliknet med spesialiserte militære IKT-produkter. Militær teknologi er ofte kostbar. Dermed får løsningene lang levetid, men de blir også etter hvert utdaterte. Bruk av sivil teknologi tilpasset militært bruk der det er mulig, kan gi betydelig raskere innfasing av nye funksjoner også i militære anvendelser.

Militært personell og forskere eksperimenterer sammen om framtidens ledelse i FFIs stridslaboratorium. Foto: FFI

HVA ER?

Syntetisk ledelsestrening

Bruk av moderne simuleringsteknologi og IKT-løsninger sparer tid og kostnader i trening og øving. IKT-baserte trenings- og ledelsesverktøy er integrert. Det betyr at ledelses- og stabstrening gjennomføres med de samme IKT-løsningene som under planlegging og ledelse av operasjoner. Når en gitt ledergruppe trener, kan de simulere underliggende og samhandlende styrker slik at disse ikke trenger å delta i treningen. Innen få år vil simuleringsteknologi sørge for at de som trener, ikke vil merke forskjell på om de leder virkelige eller simulerte styrker. De vil utveksle planer, gi ordre og motta rapporter på samme måte, uavhengig av om de forholder seg til virkelige eller simulerte aktører. Ledere og staber som samarbeider både nasjonalt og internasjonalt, kan gjennomføre ledelsestrening fra sine hjemmebaser.

HVA ER?

Samhandling i nettverk

For å effektivisere den operative virksomheten har Forsvaret utarbeidet en plan for hvordan samhandling i nettverk bør videreutvikles de neste femten årene. Samhandling i nettverk betyr at tekniske systemer og menneskelig kompetanse virker sammen på en slik måte at styrkene gir størst mulig operativ effekt. Når flere og nye typer sensorer, våpensystemer og beslutningsstøttetjenester blir inkludert i informasjonsinfrastrukturen, vil mengden tilgjengelig informasjon øke betydelig sammenliknet med i dag. Effektiv omsetting av informasjon til beslutninger krever forbedring innenfor en rekke områder i Forsvaret. Det trengs helhetlige IKT-løsninger og løsninger for annet materiell, og det er nødvendig å utvikle Forsvarets organisasjon, lederskap og personell. Forsvaret, støttet av FFI, arbeider med en konseptuell løsning for et helhetlig taktisk ledelsessystem for landdomenet. Det skal bidra til utviklingen av samhandling i nettverk.

Scenario: strategisk overfall

Vi tar utgangspunkt i et mulig scenario: Norge er utsatt for et strategisk overfall fra Russland. Figuren viser hvordan dette kan utspille seg om femten år. Russisk marineinfanteri, støttet av luft- og sjøstridskrefter, har angrepet flere befolkningssentre og ødelagt viktig infrastruktur i Finnmark og Nord-Troms. USA er i ferd med å deployere en ekspedisjonsstyrke til Trøndelag for å hente ut forhåndslagret materiell, for så å rette innsatsen mot Nord-Norge. I løpet av kort tid skal norske og amerikanske styrker planlegge og gjennomføre en landsetting og forflytting av de amerikanske styrkene. Dette skjer i et Norge preget av hardt fiendtlig press og stor usikkerhet i den sivile befolkningen. Hver time teller.

Ofte deltar ulike nasjonale styrker, internasjonale styrker og sivile samarbeidspartnere i Forsvarets operasjoner. I framtiden vil disse styrkene operere enda tettere sammen. Norske og allierte enheter vil operere samstemt mot ett felles mål. I vårt scenario sikrer lokale HV-avdelinger først oppsetting av den amerikanske styrken, deretter deployering til operasjonsområdet i samarbeid med nasjonale og allierte luft- og sjøstridskrefter. Sjef for Nasjonal territoriell kommando planlegger, leder og koordinerer overføringsoperasjonen på vegne av krigshovedkvarteret. Ved ankomst til operasjonsområdet i Troms, overtar sjef for Brigade Nord ansvaret for den amerikanske enheten, som deretter deltar sammen med norske avdelinger i kampen mot fienden. En slik operasjon krever kompetent personell som har trent og øvd på å samhandle effektivt både innad i egen avdeling og sammen med de andre aktørene. IKT gjør effektiv ledelse av de norske og amerikanske styrkene mulig, og bidrar samtidig til kontakt med sivile aktører.

Noen av de nye utfordringene for Forsvaret

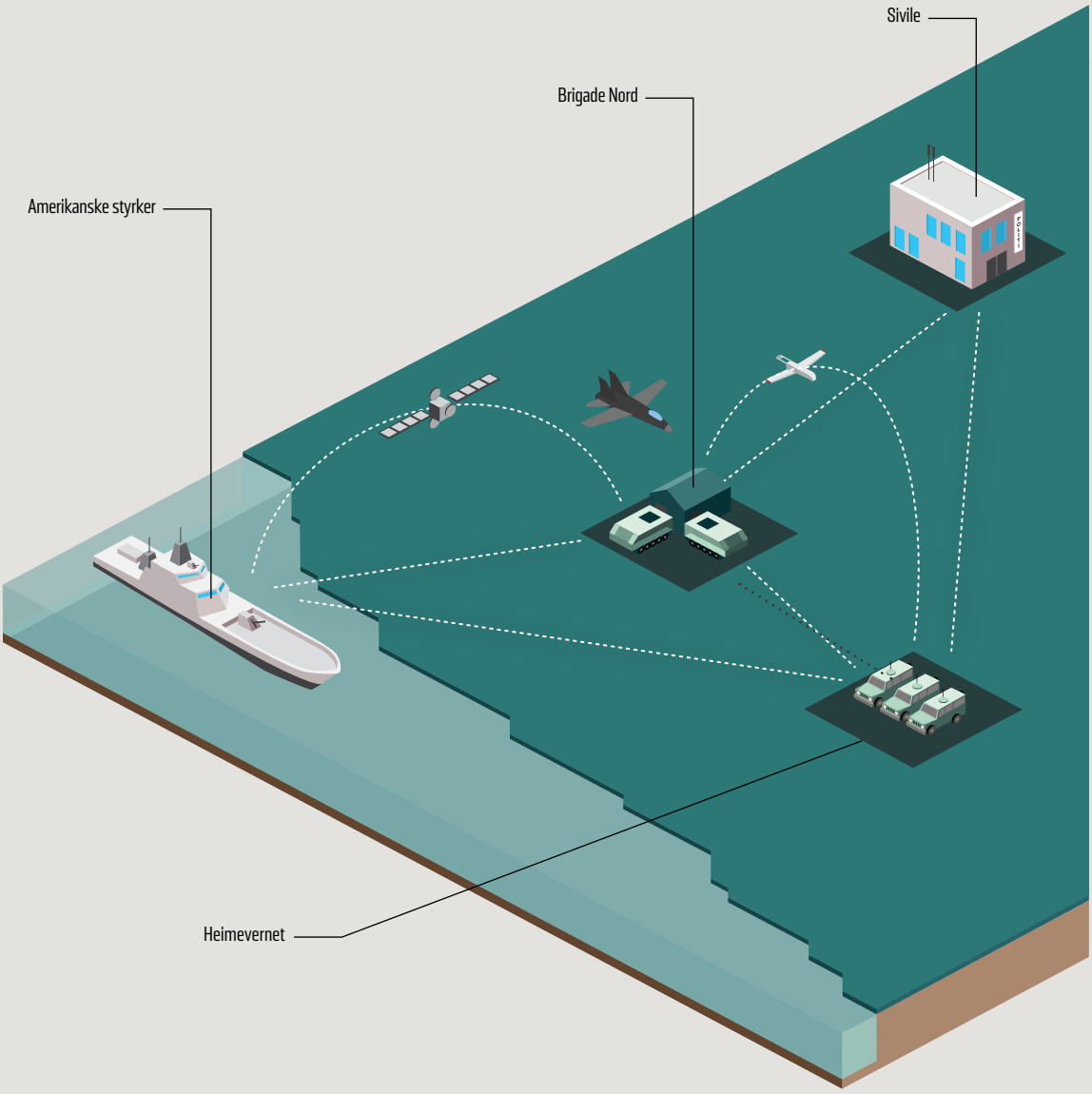
- Mer komplekse trusler
- Større informasjonsmengder
- Kortere klartider
- Større krav om tilpassing til ulike typer oppgaver og styrkesammensetning
- Høyere tempo i planlegging og gjennomføring av operasjoner

Parallell integrert planlegging: Planleggingsverktøy og digitale planer som benyttes på tvers av avdelingene, gjør det mulig for geografisk atskilte avdelinger å drive planlegging sammen. Styrkene er trent i fellesoperasjoner og Nato-operasjoner slik at de kan planlegge effektivt. Simulering blir benyttet for å støtte krigsspill slik at styrkene kan vurdere alternative handlemåter og videreutvikle planen. Avdelingene utveksler resultater fra simulering av planen. De får lettere en felles forståelse av planen, og lederen har et verktøy for å formidle sin intensjon.

Felles simulert spill av planen: Alle involverte aktører deltar i et distribuert spill hvor planen øves før gjennomføring. Dette kan for eksempel foregå når amerikanske styrker er på vei til land.

Løpende koordinering direkte mellom ledere: Samhandlingsverktøy gir ledere anledning til å kontakte hverandre umiddelbart ved koordineringsbehov, uansett hvor de befinner seg eller hvor de er på vei.

FRAMTIDENS STRID



Informasjonsinfrastrukturen: Inneholder ulike kommunikasjonsteknologier. Styrkene kan dele situasjonsbilder, planer, ordrer, etterretning og annen informasjon under både trening og operasjoner. Det er behov for helhetlig og effektiv drift og vedlikehold av IKT-løsninger, og for en riktig balanse mellom tilgang til og beskyttelse av informasjon.

Tilpassede IKT-verktøy: Tilgjengelig for de som trenger det, der de trenger det og når de trenger det – under operasjoner, i utdanning, trening og øving. IKT-løsningene for militært bruk må takle fiendtlige trusler og andre utfordringer. Samtidig må de være fleksible nok for alle aktuelle oppgaver. Sivil teknologi utnyttes også. Utviklingen mot tettere samhandling i nettverk gjør at mengden tilgjengelig informasjon øker. Tilpassede IKT-verktøy for situasjonsforståelse og ledelse hjelper militære staber og ledere med å utnytte denne informasjonen for å oppnå best mulig operativ effekt.

Utnyttelse av ressurser til fellesoperasjonens beste: Avdelingene avgir egne ressurser til fellesoperasjonen, slik at de kan utnyttes optimalt. Styrkene er trent til å bidra med og til å utnytte ressurser. Gjennom mengdetrening er de også bedre rustet til å tilpasse seg uforutsette endringer under operasjonen. Mengdetrening er bare praktisk og økonomisk mulig å få til med syntetisk ledelsestrening. Kompetanse og tett samarbeid gjennom felles trening, planleggingsprosess og løpende koordinering legger grunnlag for den nødvendige tilliten mellom styrkene.

Felles, oppdatert og tilpasset situasjonsbilde: Hver leder mottar informasjon til sin brukerenhet i henhold til sitt informasjonsbehov. Informasjon frigis og flyter sømløst mellom avdelinger og nasjoner og til og fra sivile etater etter behov, men innenfor gjeldende sikkerhetspolicyer. Situasjonsbildet vil være det samme uavhengig av om det er bare virkelige, bare simulerte eller en blanding av virkelige og simulerte stryker og aktører som deltar. IKT-løsningene holder orden på alt dette for ikke å skape farlige situasjoner.

Passiv sensor som gir oversikt

I lufta, på havet og langs kysten trenger vi bedre oversikt. Passive sensorer hjelper oss med det. Nye konsepter er nå modne for å bli prøvd ut i praksis.

Da radarer ble operative i begynnelsen av andre verdenskrig, ble det samtidig oppfunnet og tatt i bruk passive radiofrekvenssensorer (RF-sensorer) som lytter på radarsignaler. Slike sensorer ble kjent som Electronic Support Measures (ESM). Fram til midten av 1970-tallet var Norge langt framme i utvikling, produksjon og operativ bruk av ESM.

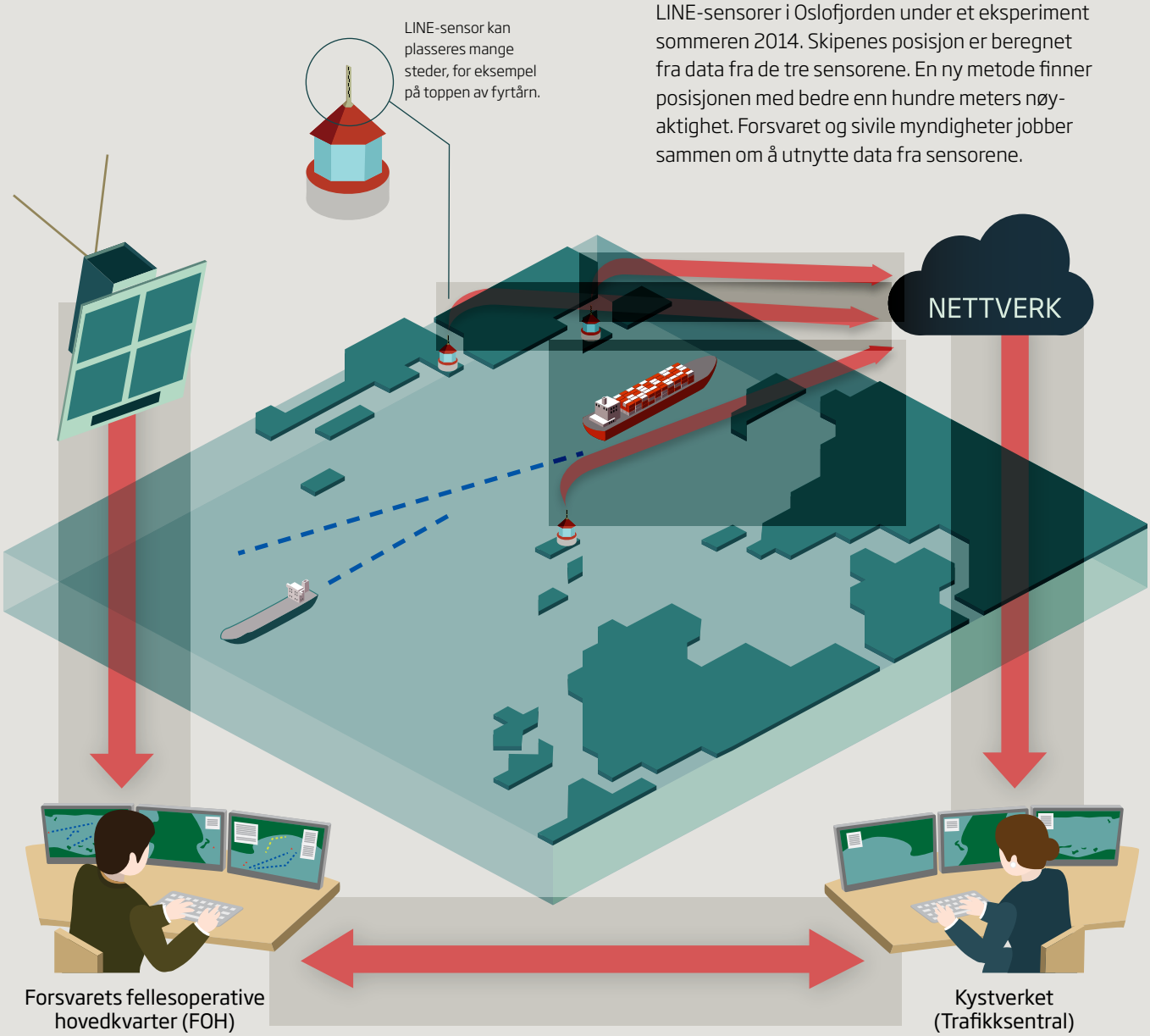
Store endringer skjer nå i Forsvaret og Nato fordi nettverksdeling på tvers av tradisjonell organisering har blitt mulig. De to norske mikrosatellittene med Automatic Identification System (AIS), AISSat-1 og AISSat-2, har ført til et meget godt sivilt-militært samarbeid om overvåkingsinformasjonen som disse samler inn om skipstrafikken.

RF-sensorer i militær luftovervåking

Et FFI-prosjekt som ble avsluttet i 1993, stimulerte til forskning på passive RF-sensorer for tidligvarsling av flyangrep ut fra scenarioer i den kalde krigen. FFI fortsatte å forske på problemstillinger rundt situasjonsoversikt i luftrommet. En tidlig inspirasjonskilde var det omfattende passive sensornettverket som Warszawapaktlandene hadde bygget opp bak det tidligere jernteppet. Systemet fant radarer og andre signalkilder ved å måle tidsforskjellen mellom mottak av radarpulser på sensorer som lå noen titalls kilometer fra hverandre. Systemet var basert på en imponerende tsjekkisk teknologiutvikling fra tidlig på 1960-tallet. Engelske Dr. Peter Emmett omtalte denne bragden i Air Power Review i 2002. Han påstod at Nato ville ha fått en forferdelig lærepenge hvis den kalde krigen hadde resultert i luftkrig på 1980-tallet.

Eksperiment med LINE-sensorer

Her ser vi hvordan RF-sensorer finner sivile skips-radarer med en mikrosatellitt og et sensornettverk langs kysten. Kartet viser utplasseringen av tre LINE-sensorer i Oslofjorden under et eksperiment sommeren 2014. Skipenes posisjon er beregnet fra data fra de tre sensorene. En ny metode finner posisjonen med bedre enn hundre meters nøy-aktighet. Forsvaret og sivile myndigheter jobber sammen om å utnytte data fra sensorene.



Antennen til LINE er en enkel konstruksjon, men har høy ytelse. Metoden LINE er basert på gjør konstruksjonen mindre kompleks.

Ubemannede fly er klare til flyving med LINE sensorlast i skroget under en operativ test av LINE på Ørland flystasjon i november 2015. Fra venstre ser vi to representanter fra selskapet Maritime Robotics AS og til høyre står forsker Eirik Skjelbreid Grimstvedt fra FFI. Foto: FFI

ESM i norsk historie

På 1970-tallet opererte Sjøforsvaret over 70 installasjoner for Electronic Support Measures (ESM). Disse varutviklet av Sjøforsvarets Forsyningskommando, med støtte av FFI, og produsert av norsk industri. Det var både enkle og avanserte systemer beregnet på Marinens fartøyer, Kystartilleriets anlegg og Kystvakten. Hovedformålet var å detektere, klassifisere og finne peiling til forskjellige typer fartøymonterte radarer i kystfarvann. Krav til økt ytelse medførte for stor økonomisk risiko til at industrien turte å satse på å videreutvikle dem.

Passive radiofrekvenssensorer

En klassisk inndeling av passive RF-sensorer etter økende kompleksitet:

1. **Radarvarsler**
Avgjør om en radarbelysning utgjør en trussel mot en selv.

2. **ESM-sensor**
Karakteriserer radarer i et område for taktiske vurderinger.

3. **ELINT-sensor**
Samler inn radardata for analyse av teknologi og trusler.

HVA ER?

Automatic Identification System (AIS)

AIS er et antikollisjonshjelpemiddel som større fartøy er pålagt å benytte. Fartøy med AIS-utstyr sender ut og mottar informasjon om identitet, posisjon, kurs, fart og mye mer over maritim radio. AIS gir nå Kystverket og andre statlige etater oversikt over skipstrafikken.

Forsvaret fornyer snart landets radarer for luftromsovervåking. I tillegg til nye radarer blir også passive RF-sensorer vurdert benyttet. Disse kan finne ut hvilke flytyper radarene observerer ut fra egenskapene til signalene som flyene sender ut. Dette vil gi en langt raskere og rimeligere gjenkjenning enn visuell inspeksjon fra et oppsendt jagerfly. I luftvern kan også egnede passive RF-sensorer ha en viktig rolle, ved å oppdage og lokalisere kildene for radarsignaler. Viktige fiendtlige radarsignaler er "målfotografering" med Synthetic Aperture Radar/Ground Moving Target Indication (SAR/GMTI) og forstyrelse (jamming) av våre luftvernradarer.

Støtte til maritim overvåking

FFI foreslo et konsept for lokalisering av skip fra en mikrosatellitt ved deteksjon av deres navigasjonsradarer allerede i 2001. Dette er nå videreutviklet til en mikrosatellitt som både har AIS og passiv RF-sensor. Den forventer vi at kan gi god støtte til annen maritim overvåking. Det kan trolig også passiv lokalisering av skipsradarer fra ubemannede fly, såkalte *unmanned areal vehicles* (UAV). FFI demonstrerte at dette lar seg gjøre med enkel og rimelig teknologi høsten 2015.

Overvåking med AIS er avhengig av skipperens velvillige medvirkning til å bli overvåket. Overvåking basert på skipenes navigasjonsradar er i langt mindre grad det, siden skipperen vil kvie seg for å slå av sin navigasjonsradar. Disse to kildene sammen kan derfor gi et mer pålitelig sjøbilde og kan faktisk utpeke skip som har feil i sin AIS-informasjon. Det gjelder både utilsiktede feil og tilsiktet manipulasjon.

Kystovervåking og sikrere navigasjon

Studenter fra Høgskolen i Oslo viste at de kunne lokalisere Bastøferja ved Horten med to sensorer som benyttet en ny krysspeilingsmetode i 2006. De viste dette med data fra ESM-eksperimentsensoren ESMEX som hadde gjort måling av tidsforskjeller i mottak av signaler fra navigasjonsradarer på disse sensorene. Høsten 2007 foreslo FFI kystovervåkingssensorer med dette måleprinsippet.

FFI startet med å utvikle en testsensor kalt Liten navigasjonsradar ESM (LINE) i 2010. Den demonstrerte lokalisering av skip i sann tid ved Ørland under Nato-øvelsen Unified Vision i juni 2012. En masterstudent ved Høgskolen i Vestfold, veiledet av FFI, benyttet nye data samlet inn ved Horten i 2013 i sin masteroppgave. Avhandlingen anslo at sensorer med omtrent tjue kilometers avstand kan følge skipstrafikk langs Finnmarkskysten.

Prototypen LINE 3 er snart klar. Den kan gjøre alle målinger som mikrosatellitter trenger for å peile og skille det store antallet skipsradarer som en satellitt vil observere fra opp til 2800 kilometers avstand i 600 kilometers høyde. En forenklet, industrialisert LINE 3 vil trolig bli svært rimelig og kan utplasseres langs kysten i et stort antall. Dette sensornettverket blir helt uavhengig av GPS og andre satellittbaserte systemer, som er svært lette å forstyrre. I et samarbeidsprosjekt i Nordsjøområdet utreder og tester forskerne nå landbaserte systemer for sikrere navigasjon. Dette er i tråd med visjonen til International Maritime Organization (IMO) om sikker e-navigasjon. LINE kan være en aktuell kandidat.

Nye anvendelser

Forskere som jobbet med geolokalisering og identifikasjon fra fly, analyserte og testet "LINE-metoden" og mange andre geolokaliseringsmetoder på de to norske flyene Hugin og Munin (DA-20 Jet Falcon), spesialfly for elektronisk krigføring, i årene 2006–2011. Flyene var også sentrale i forsøk under utviklingen av Cooperative ESM Operations (CESMO) i Nato, hvor Norge bidro tungt. Initiativet til CESMO ble tatt i alliansen etter dens svake innsats mot luftvernradarene til Milosevic i krigen på Balkan. Militære plattformer med CESMO kan nå raskt krysspeile fiendtlige radarer. Det norske Forsvaret er i front i denne utviklingen.

Skipslokalisering med passiv RF-sensor fra en mikrosatellitt og kystovervåking med LINE er nå moden for å bli prøvd ut i praksis. Det er også spennende anvendelser for passive RF-sensorer i luftovervåking og luftvern. Slike sensorer vil gi oss bedre situasjonsforståelse i fred, krise og i krig, og de kan innebære utvikling av spennende nisjeprodukter for norsk industri.

HVA ER?

Elektronisk krigføring

- En militær kapasitet og fellesressurs for hele Forsvaret
- Elektromagnetisk energi brukes for å utnytte og kontrollere det elektromagnetiske spektret i både offensive og defensive operasjoner
- Kan deles inn i tre hovedfunksjoner:
    1. Innhenting og identifikasjon av elektromagnetisk utstråling
    2. Bruk av elektromagnetisk energi for å redusere eller forhindre en motstanders bruk av det elektromagnetiske spektret
    3. Tiltak for å sikre egne styrkers bruk av det samme spektret
- Teknologitrender på feltet omfatter software-definerte systemer og maskinlæring, som kan benyttes til å forbedre deteksjon, gjenkjenning og klassifisering av signaler. Andre maskin-intelligensteknikker, som logisk resonnering, kan brukes til beslutningsstøtte for elektronisk krigføringsoperatører og for at systemer skal kunne operere autonomt.

HVA ER?

Software-definerte systemer

Tradisjonelt har systemene for radiofrekvens (RF) i radiokommunikasjon, radar og elektronisk krigføring vært laget med en fast funksjon og til en dedikert oppgave. Ett eksempel er kommunikasjonssystemet for et gitt frekvensområde med fast implementerte kommunikasjonsprotokoller.

I løpet av de siste tiårene har generelle, programmerbare plattformer for RF-signaler gradvis fått mer prosesseringskraft. Dette gjelder spesielt fra og med introduksjonen av programmerbar hardware, hovedsakelig field-programmable gate array (FPGA). Disse digitale RF-systemene kalles i dag for software-definerte systemer.

Software-definerte systemer kan erstatte flere dedikerte systemer, og de kan brukes med den funksjonaliteten som situasjonen krever. Systemet digitaliserer RF-signaler så tett som mulig til antennene. Bruken av de digitale signalene er definert av hvilke dataprogrammer som til enhver tid kjører på systemet. Disse programmene skal kunne stoppes eller startes i software, akkurat som appene på en mobiltelefon, slik at de kan assistere de skiftende behovene til en operatør.

Elektronisk krigføring i moderne operasjoner

Betydningen av elektronisk krigføring i moderne høyteknologiske operasjoner er åpenbar i dagens konflikter. Både i Ukraina og i Syria er det rapportert at Russland tar i bruk elektronisk krigføring. Har USA og Nato sovet i timen om elektronisk krigføring?

Bruk av elektronisk krigføring i moderne militære operasjoner påvirker i stor grad både stridsevnen og overlevelsesevnen til egne styrker. For å opprettholde kampkraften er det viktig å forstå hvordan egne styrker kan bruke elektronisk krigføring og hvordan de kan forberede seg på å stå imot en motstander som bruker elektronisk krigføring.

Samarbeid og trening må til

Nasjonal kompetanse på elektronisk krigføring (EK) krever satsing på fagfeltet for å følge med i den teknologiske utviklingen. Denne kompetansen kommer ikke av seg selv, men er et resultat av langvarig samarbeid og trening.

I Norge er vi avhengig av et tett samarbeid, både nasjonalt og internasjonalt, for å opprettholde kompetansen. Forsvarets EK-støttesenter (FEKS) på Rygge har som hovedoppgave å sørge for at elektronisk krigføring bidrar til å øke forsvarsavdelingenes totale overlevelsesevne og dermed kampkraft. En viktig forutsetning for stridsevne og kampkraft er informasjonsoverlegenhet i det elektromagnetiske stridsmiljøet. Det vil si ulike former for trådløse signaler brukt i kommunikasjon, radar, navigasjon og elektro-optikk. FFI samarbeider tett med FEKS og Etterretningstjenesten. Vi drar nytte av å være et lite land med korte avstander, både geografisk og organisatorisk.

For å etterprøve teknikker og taktikker er det nødvendig å trene jevnlig og verifisere at disse fungerer gjennom praktiske forsøk. FFI har en rekke mobile verktøy for dette. Vi gjennomfører jevnlig forsøk, både nasjonalt og internasjonalt, i tett samarbeid med Forsvaret. Slike forsøk demonstrerer og verifiserer operativ effekt og er nødvendig for å gi brukerne tiltro til EK-systemene.

Det er naivt å tro at vi får operere uhindret i det elektromagnetiske stridsmiljøet i framtiden. Derfor er det meget viktig å trene blant annet radaroperatører, radiosamband, luftvern og store våpensystemer for å kunne møte utfordringene når en motstander tar i bruk elektronisk krigføring. Dette kan for eksempel være jamming, peiling, posisjonering og innsamling av informasjon. Derfor er det essensielt å ha tilgang til nasjonale EK-ressurser og verktøy for å kunne gi troverdig trening til Forsvaret. Det gjelder på land, til sjøs og i luften. Elektronisk krigføring er også i høyeste grad en fellesoperativ ressurs og trenger derfor tilstrekkelig oppmerksomhet i Forsvarets fellesoperative hovedkvarter

(FOH), som er ansvarlig for både operative ressurser og trening.

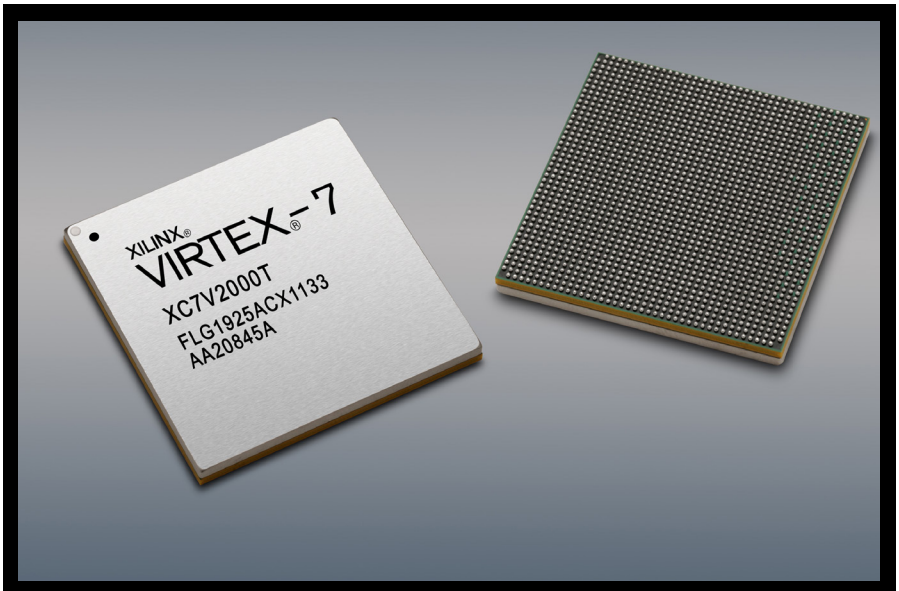
Teknologien bak

Elektronisk krigføring er teknologiintensiv, og utviklingen er basert på den nyeste og mest avanserte teknologien innenfor en rekke fagfelt. Også systemer for elektronisk krigføring drar nytte av den svært hurtige utviklingen av datamaskiner generelt, når vi kan bruke kommersielle produkter for digital regnekraft og signalbehandling. Det kommersielle markedet leder over det militære på ytelsen til prosessering av digitale data. Hovedutfordringen for militære anvendelser er å utnytte den til enhver tid tilgjengelige regnekraften i størst mulig grad.

FFI-forskningen innen elektronisk krigføring støtter alle forsvarsgrener gjennom studier, modellering, konseptutvikling og teknologiutvikling. Målet vårt er å utnytte teknologien for å oppnå både defensiv og offensiv operativ nytte av elektronisk krigføring. Software-definerte systemer er et eksempel på ny teknologi som understøtter utviklingen av elektronisk krigføring (se faktaboks side 20).

Betydningen for Forsvaret

Kampkraft og bærekraft er bærebjelker i den nye langtidsplanen for forsvarssektoren, Prop. 151 S (2015–2016). Elektronisk krigføring er svært viktig for å opprettholde kampkraft. Det har blitt spesielt tydelig gjennom Russlands utstrakte bruk av elektronisk krigføring i Ukraina og Syria. Fagfeltet elektronisk krigføring kan sees på som en slags forsikringspolise for å kunne opprettholde stridsevnen og kampkraften. I kampen om det elektromagnetiske spektret har elektronisk krigføring en avgjørende rolle å spille. Den som vinner denne kampen, vil ha et stort fortrinn i dagens og framtidens konflikter.



FIELD-PROGRAMMABLE GATE ARRAY (FPGA) har introdusert en digital revolusjon innen flere typer radiofrekvenssystemer (RF-systemer). Disse kretsene ble først produsert på 1980-tallet og er mye raskere enn vanlige datamaskinprosessorer på mange regneoppgaver. FPGA-er kan brukes til passivt å skanne for spesielle typer radiosignaler, og også som radar eller til å jamme kommunikasjonssignaler. Dette kalles multifunksjons rekonfigurerbare RF-systemer. Dersom systemet i tillegg har elektronisk styrte antenner, kan de forskjellige radiofunksjonalitetene føres i forskjellige retninger. For eksempel kan skanning av radiosignaler skje i en retning og kommunikasjon i en annen. Bildet viser en FPGA-krets brukt på kretskortet til siste generasjon av FFIs eksperimentelle radarjammer, EKKO III.

En flyvende komponent i kommunikasjonsinfrastrukturen

Framtidens forsvar vil stille høye krav til samhandling mellom teknologisk avanserte og svært mobile avdelinger. Ubemannede luftfarkoster har potensial til å bli viktige komponenter i Forsvarets framtidige kommunikasjonsinfrastruktur.

FFI har forsket på mobile og ubemannede luftfarkoster, kjent som *Unmanned Aerial Vehicles* (UAV), i drøyt tjue år. I løpet av de siste ti årene har vi sett at UAV-er har blitt en viktig komponent i krigføring, blant annet i Midtøsten. Samtidig har UAV-er for forbrukermarkedet, også kjent som droner, falt dramatisk i pris, og brukervennligheten har økt betraktelig. De kan ha mange forskjellige nyttelaster, og dermed dekke ulike behov. Vi skal se på UAV-er som brukes til å støtte Forsvarets kommunikasjonsbehov.

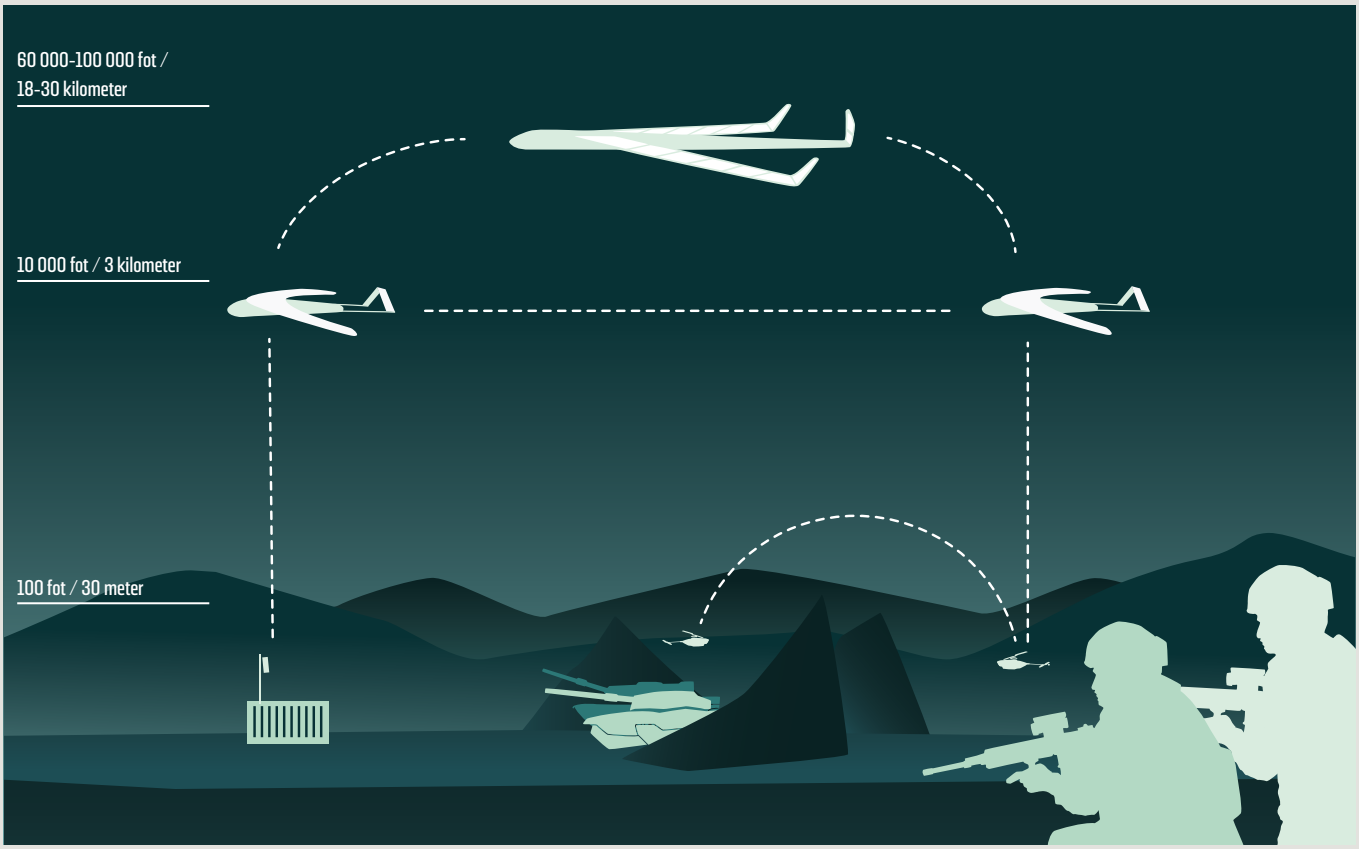
Mange bruksområder for UAV

En UAV kan være alt fra bittesmå helikoptre på noen få gram til fly på størrelse med passasjerfly. De kan være alt fra fjernstyrte til fullstendig autonome. Ulike plattformer gir ulike muligheter, og det er både utfordrende og begrensende å klassifisere dem. Vi kan likevel skissere noen scenarier hvor UAV-er kan benyttes til kommunikasjon for Forsvaret.

Store UAV-er kan fly høyt, opp mot tretti kilometer over bakken, og holde seg svevende i flere måneder eller år ved for eksempel å bruke solenergi eller brenselceller. Et mindre antall slike UAV-er kan være en strategisk ressurs for å sikre informasjonsutveksling over hele fastlandet og havområder som Barentshavet. De minste UAV-ene kan operere autonomt og

Nettverk med UAV-er

UAV-er i ulike høydesjikt og med ulik plattformytelse utgjør her et felles nettverk. Dette nettverket kan støtte taktisk kommunikasjon mellom bakkeenheter i et operasjonsområde. Det kan samtidig øke evnen til strategisk ledelse ved å forsterke den landsdekkende kommunikasjonsinfrastrukturen.



Langtidsplanen for forsvarssektoren sier at

«INI skal dimensjoneres for et økt informasjonsvolum. Automatiserte beslutningsstøtteverktøy for sammenstilling og analyse av informasjon fra flere kilder skal utnyttes i større grad. For å etablere tilgang til INI i områder med behov for bedre kapasitet, spesielt i nordområdene, vil det brukes en kombinasjon av stasjonære, deployerbare og mobile systemer. Det vil også være aktuelt med økt bruk av eleverte plattformer som bemannede og ubemannede luftplattformer og satellitter.»

Prop. 151 S (2015–2016) s. 103

være en integrert del av utrustningen til enkeltsoldater eller kjøretøy, og gi dem bedre kommunikasjonsmuligheter. Litt større UAV-er kan understøtte kommunikasjon innad i operasjonsområdet til en avdeling, for eksempel en bataljon eller en brigade, hvor de autonomt kan skifte posisjoner etter avdelingens behov. Et annet konsept er bruk av mange UAV-er samtidig i en sverm. Slik kan vi lage et robust luftbårent nettverk hvor UAV-ene samarbeider for å oppnå et mål som de ikke klarer å oppnå hver for seg.

UAV i infrastrukturen

Forsvarets kommunikasjonsinfrastruktur (FKI) er en fellesbetegnelse på Forsvarets systemer for nettverk og overføring som brukes til kommunikasjon av Forsvaret og enkelte andre aktører. Ved å bruke en felles kommunikasjonsinfrastruktur kan Forsvaret dele informasjon mellom sine mange enheter. Vi trenger kommando og kontroll med alle enheter. I tillegg må sensorinformasjon for situasjonsforståelse formidles til beslutningstakerne, og mellom ulike avdelinger og forsvarsgrener. Det er også behov for samhandling og koordinering mellom elementer på samme nivå.

Tradisjonelt har ulike deler av Forsvaret anskaffet kommunikasjonsløsninger etter behov. Disse behovene har resultert i ganske forskjellige løsninger som har gjort kommunikasjon mellom organisatorisk adskilte strukturelementer vanskelig. Hver enkelt teknologi har fysiske styrker og begrensninger som gjør at én teknologi hverken kan eller bør benyttes overalt. Derfor består FKI av en rekke ulike systemer.

Langtidsplanen for Forsvaret slår fast at behovet for utveksling og behandling av informasjon vil øke stort framover. Dette betyr at kommunikasjonsinfrastrukturen må få høyere overføringskapasitet. Det økte behovet for overføringskapasitet kan på taktisk side tilfredsstilles gjennom å benytte høyere og utvidede frekvensbånd, som vil kreve frisikt mellom radioene. En UAV vil gi mulighet for å oppnå frisikt mellom sender og mottaker på større avstander enn tradisjonelle radiosystemer. Alternative løsninger, som satellittkommunikasjon eller et meget godt utbygd system av bakkebaserte mobilstasjoner, vil ikke ha den samme fleksibiliteten og kan innebære mye høyere kostnader enn UAV-er som kan settes inn etter behov.

UAV-er kan være med på å gjøre kommunikasjonsinfrastrukturen sterkere ved å tilby alternative, supplerende nettverk. Forsvaret må forvente at kommunikasjonsinfrastrukturen kan være et aktuelt mål for en avansert fiende. I nordområdene er infrastrukturen generelt lite utbygd, og både satellittkommunikasjon og langtrekkende radiokommunikasjon (HF-kommunikasjon) har særskilte utfordringer i disse områdene. En UAV vil kunne supplere andre løsninger, spesielt for kommunikasjon mellom avdelinger innad i en region. Rundt deployerte baser, for eksempel i Afghanistan, har det vist seg å være utfordrende å etablere en kommunikasjonsinfrastruktur i nærområdet. UAV-er kan enkelt dekke disse behovene.

Utfordringer som må løses

Det er flere utfordringer vi må løse før en UAV kan brukes som en komponent i FKI. Kostnader til anskaffelse og drift må ned. Spesielt må krav til kompetanse og personellressurser være lave. Posisjonering av UAV-ene er viktig, og bør helst kunne skje autonomt. I tillegg er det flere utfordringer med å plassere en radiosender høyt relativt til andre radioer. Dette gjelder både for nettverksteknologier og frekvensplanlegging. En UAV kan også være lett å oppdage for en fiende, både elektromagnetisk og visuelt. Den kan for eksempel avsløre at det er militære avdelinger på bakken. Det er trusler mot en UAV i hele spekteret fra elektronisk krigføring til direkte fysiske våpenvirkninger. Derfor blir det viktig å se på hvordan vi kan utnytte moderne antenner og radioteknologi for å redusere sporbarheten fra en fiende.

Været vil være en stor utfordring, spesielt for små og mellomstore UAV-er. Energiressurser er en utfordring for farkoster som skal være lenge i lufta. På våre breddegrader er solenergi mindre tilgjengelig. Det er helt nødvendig med forskning for å studere om solenergi vil fungere i våre nordområder. Bruk av UAV i Forsvaret avhenger også av at vi sammen med sivile og militære luftfartsmyndigheter kan hindre at regelverket rundt bruk av ubemannede fly blir en unødvendig bremsekloss.

UAV-er kan benyttes til å realisere fleksible kommunikasjonsplattformer og kan dermed spille en viktig rolle i Forsvarets framtidige kommunikasjonsinfrastruktur. Gevinstpotensialet vil kunne være særlig stort dersom Forsvaret utvikler seg mot en struktur basert på mindre enheter med høy grad av mobilitet.

REFERANSER

Emmett, P. (2002). Silent trackers: The Spectre of Passive Surveillance in the Information Age. *Air Power Review, Vol 5, No 2/2002.*

Engebråten, R. (2013). Ship Navigation Radar Tracking by Onshore Sensors for Coast Surveillance. *Masteroppgave ved Høgskolen i Vestfold.*

EU INTERREG IVb North Sea Region Programme project (2015). *ACCSEAS Baseline and Priorities Report, Issue 3/2015.*

Garvik, Ø. (2009). *Bølger som våpen – Elektronisk krigføring i Sjøforsvaret 1945-1995.* Sjømilitære samfunds forlag.

Gjørven, E., Johnsen, F. T., Fongen, A., Bloebaum, T. H. & Reitan, B. K. (2014). Towards NNEC – Breaking the interaction barrier with collaboration services. *FFI-rapport 2014/00943 .* Kjeller, Forsvarets forskningsinstitutt.

Grimstvedt, E.S., Aronsen, M. & fler. (2016). LINE EW-UAS An experimental unmanned system for coastal surveillance using ESM technology. *FFI-rapport 15/02442*. Kjeller, Forsvarets forskningsinstitutt.

Grønvold, L., Oftebro, S. (2006). Labview-program for lokalisering av båter med tidsinformasjon fra to sensorer. *Hovedprosjekt ved Høgskolen i Akershus.*

IMO Maritime Safety Committee (2009). Strategy for the Development and Implementation of e-Navigation. R*eport of the Maritime Safety Committee on its 85th Session, MSC 85/26/Add.1, Annex 20.* London.

Karlsen, L. H., Reitan, B. K. (2014). CEI – et sosialt taktisk rapporteringssystem: Teknisk beskrivelse av Android klient for smarttelefon og nettbrettstøtte til CEI-systemet. *FFI-notat 2014/00526.* Kjeller, Forsvarets forskningsinstitutt.

Nordbotten, N. A., Mancini, F., Farsund, B. H., Haakseth, R., Hegland, A. M. og Lillevold, F. (2015). Information sharing across security domains. *FFI-rapport 15/00456*. Kjeller, Forsvarets forskningsinstitutt.

Proposisjon til Stortinget 151 S (2015–2016), *Kampkraft og bærekraft – Langtidsplan for forsvarssektoren.* Oslo, Forsvarsdepartementet.

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.

Størdal, J-M (2016). Kampen om moderne våpen. *Kronikk i Dagens Næringsliv 1/11/2016.*

FFIs nyhetsbrev kommer jevnlig

Les mer og abonner
ffi.no\nyhetsbrev

FFI Forsvarets forskningsinstitutt

FFI Forsvarets forskningsinstitutt