FFI Forsvarets forskningsinstitutt

21/01819

FFI-RAPPORT

Hvordan kan ny IKT gjøre Forsvaret bedre?

Jan Erik Voldhaug
Bjørn Jervell Hansen
Ketil Lund
Anders Mykkeltveit
Martin Rytir
Ole Ingar Bentstuen

Hvordan kan ny IKT gjøre Forsvaret bedre?

Jan Erik Voldhaug
Bjørn Jervell Hansen
Ketil Lund
Anders Mykkeltveit
Martin Rytir
Ole Ingar Bentstuen

Forsvarets forskningsinstitutt (FFI) 11. november 2021

Emneord
IKT
Stordata
Satellittkommunikasjon
5G

FFI-rapport
21/01819

Elektronisk ISBN
978-82-464-3378-3

Engelsk tittel
Improving the Norwegian Armed Forces by exploiting modern information and communication technology

Godkjennere
Trude H Bloebaum, *forskningsleder*
Espen Skjelland, *administrerende direktør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Norge står overfor en krevende sikkerhetspolitisk situasjon. Forsvaret spiller en avgjørende rolle for å skape sikkerhet for staten, befolkningen og samfunnet, og det er avgjørende at Forsvaret moderniseres og videreutvikles kontinuerlig.

Moderne IKT (informasjons- og kommunikasjonsteknologi) er nødvendig for å understøtte Forsvarets operative evne. Samtidig har Forsvaret i dag delvis utdaterte IKT-løsninger. Problemstillingen som ligger til grunn for rapporten er hvordan teknologisk utvikling innen IKT kan gjøre Forsvaret bedre i stand til å løse sine oppgaver. Rapporten har som ambisjon å peke på muligheter og gi råd til Forsvarets ledelse om utnyttelse av IKT, og dermed bidra til at Forsvaret løser oppgavene sine bedre og mer effektivt.

Rapporten beskriver utvikling innenfor fire utvalgte teknologiområder innen IKT, som vi mener kan få vesentlig betydning for Forsvarets utvikling, og hvilke muligheter denne utviklingen medfører. De fire områdene er: 1) Automatisert analyse av informasjon, 2) Skyteknologi, 3) Femte generasjons mobilteknologi (5G) og 4) Langtrekkende høyhastighetskommunikasjon.

Deretter skisseres fire eksempler på hvordan disse mulighetene kan komme Forsvaret til gode. Eksemplene beskriver også mulige gevinster og utfordringer, herunder risikoer og kostnader, for Forsvaret. De fire eksemplene tar for seg i) effektiv og sikker IKT-infrastruktur, ii) samvirke i totalforsvaret, iii) mobilitet og hurtighet i militære operasjoner og iv) utnyttelse av sensordata. Rapporten fokuserer på operativ virksomhet fremfor virksomhetsstyring, ettersom militære operasjoner er Forsvarets aller mest krevende oppgaver og også det som i størst grad skiller Forsvaret fra andre virksomheter.

Ut fra identifiserte gevinster og utfordringer, utleder rapporten en rekke anbefalinger som vi mener kan gjøre Forsvarets bedre. Anbefalingene er samlet i kapittel 5, og omhandler strategiske veivalg, fremskaffelser av materiell, utvikling av kompetanse og samarbeid med andre organisasjoner.

Det er viktig å være klar over at denne rapporten har fokus på teknologi og teknologiske muligheter, og at rapporten kun har studert et utvalg av teknologiområder. Anbefalingene i rapporten bør leses i denne konteksten.

Summary

Information and communications technology is a pivotal part in the development of the Norwegian Armed Forces. This report investigates how the evolution within the field of information and communications technology can help make the Norwegian Armed Forces solve their tasks better and more efficiently.

The report describes the technological development within four areas and the opportunities the development can give. The four areas are 1) exploitation of big data, 2) cloud technology, 3) fifth generation mobile network (5G), and 4) ubiquitous high-speed communication.

Consequently, the report lays out four examples on how these opportunities can benefit the Norwegian Armed Forces, describing possible gains, risks and costs. The four examples consider i) efficient and secure ICT infrastructure, ii) cooperation with civil crisis management actors, iii) mobility in military operations, and iv) exploitation of sensor data.

From the identified gains, risks and costs the report derives a number of recommendations that we believe will improve the ability of the Norwegian Armed Forces to solve their most demanding tasks. The recommendations include both acquisition of material, development of competency and cooperation with other actors. We stress that this report focuses on technology and that the report only considers selected areas within the field of information and communications technology and possible use of these in the Norwegian Armed Forces. The recommendations in the report must be read in this context.

Innhold

Forord

Rapporten er skrevet som et samarbeid mellom seks pågående FFI-prosjekter som alle studerer informasjons- og kommunikasjonsteknologi til bruk i Forsvaret. De seks prosjektene er:

- Forsvarets bruk av det digitale og elektromagnetiske rom
- Informasjonsintegrasjon for et moderne forsvar
- Kommando, kontroll og teknologi i fellesoperasjoner
- Kommunikasjonsløsninger for effektivt samvirke i militære operasjoner
- Moderne tjenesteinfrastruktur for Forsvaret
- Robust trådløs kommunikasjonsteknologi

Rapporten har til hensikt å gjøre prosjektenes studier tilgjengelig for et bredere publikum og å komplettere leveransene fra prosjektene.

Kjeller, 11. november 2021

Jan Erik Voldhaug, Bjørn Jervell Hansen, Ketil Lund, Anders Mykkeltveit, Martin Rytir
og Ole Ingar Bentstuen.

1 Innledning

1.1 Bakgrunn og problemstilling

Norges sikkerhetspolitiske situasjon er krevende. Ikke siden slutten av den kalde krigen har Norge og våre allierte stått overfor et slikt omfang av samtidige sikkerhetsutfordringer.[1] Forsvaret spiller en avgjørende rolle for å skape sikkerhet for staten, befolkningen og samfunnet, og det er avgjørende at Forsvaret moderniseres og videreutvikles kontinuerlig for å opprettholde sin evne til å løse sine oppgaver.

Den teknologiske utviklingen går nå svært hurtig og skjer med en hastighet og potensiell effekt på samfunnet som har likhetstrekk med en teknologisk revolusjon.[2] Flere omtaler dette som «den fjerde industrielle revolusjon». Dette begrepet ble definert av Klaus Schwab, som den foreløpig siste av fire teknologiske og fundamentale industrielle omveltninger etter introduksjonen av dampkraft på 1700-tallet, elektrisitet på 1800-tallet og informasjons- og kommunikasjons-teknologi (IKT) og elektronikk på 1900-tallet.[3]

Samtidig som den teknologiske utviklingen går svært hurtig reduseres skillet mellom sivil og militær teknologi,[4] og den omfattende teknologiutviklingen vil derfor også påvirke Forsvaret. Forsvarets forskningsinstitutt (FFI) har studert teknologiske trender som vil påvirke Forsvarets militære operasjoner i fremtiden, og IKT er en fellesnevner for flere av trendene som trekkes frem i studien.[5] IKT er også en fellesnevner for flere av trendene i Natos vurdering av teknologier og deres potensielle påvirkning på Natos militære operasjoner.[6] [7]

Moderne IKT-løsninger er nødvendig for å understøtte Forsvarets operative evne og for effektiv gjennomføring av virksomheten i forsvarssektoren.[8] Samtidig har Forsvaret i dag delvis utdatert materiell og IKT-løsninger,[9] og forsvarssektoren er ikke tilstrekkelig i stand til å utnytte ny teknologi.[10]

Det planlegges med en betydelig satsning på IKT i Forsvaret i perioden 2021–2028, og om lag 20 milliarder kroner skal i perioden brukes på investeringer innen IKT-området.[11] I tillegg til investeringskostnader kommer driftskostnader. Studier gjennomført av FFI fant at forsvars-sektoren i perioden 2014–2018 hadde årlige driftskostnader på om lag 3,5 milliarder kroner

[1] Forsvarsdepartementet (2020a): Prop. 14 S (2020–2021) Evne til forsvar – vilje til beredskap. Langtidsplan for forsvarssektoren.
[2] Svendsen-utvalget (2020): Økt evne til å kombinere menneske og teknologi. Veier mot et høyteknologisk forsvar.
[3] Schwab, Klaus (2015): The Fourth Industrial Revolution – What It Means and How to Respond, Foreign Affairs, Dec 2015.
[4] FFI (2020): Teknologiske trender Muligheter og utfordringer for fremtidens forsvar. FFI-fakta.
[5] Andås, Harald (2020): Emerging technology trends for defence and security. FFI-rapport 20/01050.
[6] Nato omtaler dette som *Emerging and disruptive technologies.*
[7] Nato Science & Technology Board (2020): Science & Technology Trends 2020-2040. NATO UNCLASSIFIED.
[8] Forsvarsdepartementet (2020a).
[9] Forsvaret (2018): Digitaliseringsstrategi for Forsvaret.
[10] Forsvarsdepartementet (2019): IKT-strategi for forsvarssektoren.
[11] Forsvarsdepartementet (2021): Framtidige anskaffelser til forsvarssektoren 2021–2028. Kap. 4.5 Cyberdomenet.

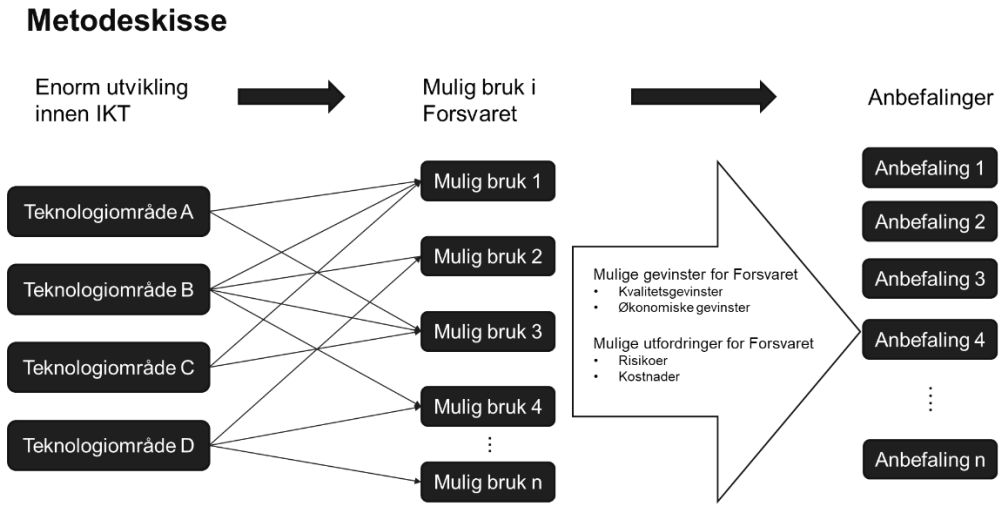
knyttet til IKT,[12] og at om lag 1600 årsverk i 2018 var tilknyttet forsvarssektorens IKT-virksomhet.[13] I tillegg kommer kostnader knyttet til Forsvarets våpenplattformer, som kampfly, fartøyer og kampvogner, hvor IKT i økende grad er en integrert del.

Problemstillingen som ligger til grunn for rapporten, er hvordan teknologisk utvikling innen IKT kan gjøre Forsvaret bedre i stand til å løse sine oppgaver. Det synes å være bred enighet, også i Forsvaret, om at IKT er viktig, og det er ikke vanskelig å finne utsagn om dette – heller ikke i styrende dokumenter. Det kan imidlertid være vanskelig å bryte ned denne innsikten i konkrete veivalg. Denne rapporten har som ambisjon å peke på muligheter og gi råd til Forsvarets ledelse om utnyttelse av IKT, og dermed bidra til at Forsvaret løser oppgavene sine bedre og mer effektivt.

Studien søker å besvare tre spørsmål: i) Hvordan kan utvalgte teknologiområder bidra til å gjøre Forsvaret bedre? ii) Hvilke gevinster kan Forsvaret oppnå ved å ta i bruk ny IKT?, og iii) Hva kan/bør Forsvaret gjøre på kort sikt for å høste disse gevinstene?

1.2 Metode og avgrensninger

Rapporten tar utgangspunkt i utviklingen innen IKT og hvilke muligheter denne utviklingen medfører. Deretter skisseres noen tilnærminger for hvordan Forsvaret kan utnytte disse mulighetene. Til slutt utledes anbefalinger ved å vurdere mulige gevinster og utfordringer ved de ulike tilnærmingene. Fremgangsmåten er skissert i figur 1.1.



Figur 1.1 Prinsippskisse av studiens fremgangsmåte.

[12] Arnfinnsson, Brynjar, Elisabeth Elman og Sondre Hansen Eriksen (2020): Hvor mye bruker forsvarssektoren på IKT? FFI-rapport 20/00806. BEGRENSET.
[13] Kvalvik, Sverre mfl. (2019): Hvordan skape økonomisk handlingsrom i den nye langtidsplanen? – potensial for forbedring og effektivisering 2021–2024. FFI-rapport 19/01934.

IKT er et omfattende område, og for å gjøre studien håndterbar har det vært nødvendig å gjøre betydelige avgrensninger. Vi har valgt ut fire teknologiområder som vi mener vil kunne ha vesentlig betydning for Forsvaret utvikling:

1) Automatisert analyse av informasjon
2) Skyteknologi
3) Femte generasjons mobilteknologi (5G)
4) Langtrekkende høyhastighetskommunikasjon

De fire teknologiområdene er valgt ut etter to kriterier: i) Det har vært, eller er, en fundamental utvikling innenfor området, og ii) FFI har gjennomført, eller er i ferd med å gjennomføre, teknologistudier innenfor området. Dette er altså kun et utvalg, og det kan være andre områder som kan påvirke Forsvaret i vel så stor grad. For å belyse utviklingen har vi for hvert av de fire områdene studert utviklingen som har skjedd eller er i ferd med å skje. Fokuset er på teknologisk utvikling, men vi har også sett på utvikling innen andre områder, for eksempel generell samfunnsutvikling, som for noen områder også har vært en viktig drivkraft. For alle områdene har vi identifisert muligheter som utviklingen medfører.

For å vurdere hvordan Forsvaret kan dra nytte av teknologiutviklingen har vi studert eksempler på hvordan de identifiserte mulighetene kan utnyttes. Forsvaret utfører en lang rekke oppgaver, og det har ikke vært mulig i rammen av denne studien å vurdere hele Forsvarets virksomhet. Bruksområdene er definert ved å ta utgangspunkt i noen av føringene for Forsvarets utvikling i langtidsplanen for forsvarssektoren. Langtidsplanen vektlegger blant annet utvikling av totalforsvaret, og peker på langtrekkende presisjonsvåpen som en av de viktigste påvirkningene på utviklingen av Forsvarets struktur.[14] Videre presiserer langtidsplanen at Forsvaret skal utvikle en robust IKT-infrastruktur og i større grad skal utnytte automatiserte verktøy for sammenstilling og analyse av informasjon. Gjeldende langtidsplan viderefører fornyingen av Forsvarets IKT som beskrevet i foregående langtidsplan.[15]

Vi har valgt å fokusere på operativ virksomhet. Grunnen er at militære operasjoner er Forsvarets aller mest krevende oppgaver, og også det som i størst grad skiller Forsvaret fra andre virksomheter. Det er imidlertid også et potensiale for å digitalisere støttevirksomheten i Forsvaret, uten at det er videre behandlet i denne rapporten.[16]

For å utlede anbefalinger har vi identifisert og sammenstilt gevinster og utfordringer ved de ulike eksemplene vi har studert. Vi skiller i denne rapporten mellom økonomiske gevinster og kvalitetsgevinster som beskrevet i Forsvarsdepartementets (FD) veileder for gevinstrealisering[17]. Økonomiske gevinster er gevinster som gir besparelser som synes i regnskap og budsjetter, og som måles i kroner. Slike gevinster kan være å utføre oppgaver billigere eller å unngå kostnadsøkninger. Kvalitetsgevinster er gevinster som ikke kan måles i kroner, men som medfører økt

[14] Forsvarsdepartementet (2020a).
[15] Forsvarsdepartementet (2016): Prop. 151 S (2015–2016) Kampkraft og bærekraft. Langtidsplan for forsvarssektoren.
[16] Kvalvik, Sverre mfl. (2019).
[17] Forsvarsdepartementet (2020b): Veileder for gevinstrealisering i forsvarssektoren.

kvalitet på ett eller flere områder. For Forsvaret kan slike gevinster være at man utfører oppgaver bedre eller raskere, eller at Forsvaret får nye evner. Fokuset i rapporten er på kvalitetsgevinster, og vi har verken beregnet økonomiske gevinster eller kostnader i detalj.

Det er viktig å være klar over at denne rapporten har fokusert på teknologi og teknologiske muligheter, og at rapporten kun har studert et utvalg av teknologiområder. Anbefalingene i rapporten bør leses i denne konteksten. Vi erkjenner at det også er andre faktorer som påvirker hvordan Forsvaret utnytter teknologiutviklingen, for eksempel økonomi og juridiske forhold, uten at det er analysert i denne studien.

1.3 Målgruppe og leseveiledning

Rapporten er primært skrevet for beslutningstakere og personell som jobber med investering og langtidsplanlegging i forsvarssektoren, herunder FD og ledelsen i Forsvaret, Forsvarsmateriell (FMA) og ulike driftsenheter i Forsvaret. Sekundært er rapporten skrevet for offentligheten og beslutningstakere i totalforsvaret.

Kapittel 2 beskriver utviklingen innenfor fire teknologiområder og hvilke muligheter denne utviklingen medfører. I kapittel 3 beskriver vi hvordan Forsvaret kan utnytte de nye mulighetene. I kapittel 4 vurderer vi muligheter og gevinster samt kostnader og risikoer ved tilnærmingene beskrevet i kapittel 3, og kommer med anbefalinger. Kapittel 5 oppsummerer rapporten med fokus på anbefalinger.

2 Utvikling innen IKT

I dette kapittelet beskrives utviklingen innen de fire utvalgte teknologiområdene samt hvilke muligheter utviklingen har ført med seg. Beskrivelsene fokuserer på teknologisk utvikling, men enkelte forhold ved samfunnsmessig utvikling berøres også. De fire teknologiområdene er automatisert analyse av informasjon (kapittel 2.1), skyteknologi (kapittel 2.2), femte generasjons mobilteknologi (kapittel 2.3) og langtrekkende høyhastighetskommunikasjon (kapittel 2.4).

2.1 Automatisert analyse av informasjon

Teknologiområdet «Automatisert analyse av informasjon» dekker teknologi og metoder som gjør datamaskiner enda bedre i stand til å hjelpe mennesker med å utnytte informasjonen som ligger i store datamengder, og dermed ta bedre beslutninger. Utviklingen innen dette området er først og fremst påvirket av utviklingen innen fagfeltene kunstig intelligens (AI – *Artificial Intelligence*) og stordata. Ingen av disse fagfeltene er entydig definert, men vil i denne rapporten forstås som beskrevet under.

Fagfeltet kunstig intelligens, eller AI, dreier seg om teknologi som brukes til å realisere såkalte AI-systemer, også kalt kunstig intelligente systemer. Slike systemer utfører handlinger basert på tolkning og behandling av data, for å oppnå et gitt mål. Enkelte systemer kan også endre sin oppførsel gjennom å analysere og ta hensyn til hvordan tidligere handlinger har påvirket omgivelsene.[18] Dette innebærer at man innen AI kan finne teknologier som legger til rette for automatisering av informasjonsanalyse.

Begrepet *stordata* kan karakteriseres ved hjelp av de såkalte tre V-ene: *Volume*, *Velocity* og *Variety*. Stordata er data av forskjelligartet natur (*Variety*), som kommer i store mengder (*Volume*) og/eller har hyppig oppdateringsfrekvens (*Velocity*), og som et resultat av dette ikke lar seg effektivt håndtere eller bearbeide ved hjelp av tradisjonelle metoder.[19] Stordata som fagfelt dreier seg derfor om teknologi som legger til rette for håndtering av data med disse karakteristikkene. Dette henger sammen med AI på den måten at teknikkene innen feltet stordata bidrar til at man er i stand til å håndtere informasjonen som skal analyseres, spesielt når denne informasjonen kan karakteriseres ved hjelp av én eller flere av de tre V-ene.

2.1.1 Utvikling

Automatisert analyse av informasjon krever at datamaskiner utfører tunge beregninger på store mengder informasjon, og den teknologiske utviklingen innenfor dette teknologiområdet er først og fremst påvirket av utviklingen innen prosessorteknologi. Når man i dag kan håndtere mye større datamengder raskere enn før, skyldes det at utviklingen av enkeltprosessorer fortsatt følger *Moores lov*, samt store fremskritt når det gjelder parallell prosessering.

Moores lov ble fremsatt av Gordon Moore i 1965, og sier at antall transistorer på et areal fordobles hver 12. måned (i 1975 justert til hver 24. måned). Denne prediksjonen viser seg å fortsatt holde, til tross for hyppige spådommer om at de fysiske lovene før eller senere vil gjøre den ugyldig. Den praktiske konsekvensen av Moores lov er at man får en kontinuerlig økning av prosesseringskraft, noe som kan utnyttes til å prosessere stadig mer data på stadig kortere tid. En annen konsekvens er at den økte prosesseringskraften kan implementeres på stadig mindre enheter som for eksempel mobiltelefoner.

I tillegg til stadige forbedringer av enkeltprosessorer, er det også en utvikling innen parallell prosessering. Parallell prosessering er evnen til å fordele prosesseringsjobben (og dataene) på flere prosessorer på en slik måte at beregninger kan gjøres parallelt. Utviklingen er primært knyttet til nye algoritmer som kan utnytte den tilgjengelige prosessorkraften på en effektiv måte.[20]

Sammen med utviklingen innen prosesseringskraft, har mulighetene til å utnytte store datamengder blitt forsterket gjennom en eksplosjon av verktøy som deles med åpen kildekode og som dermed er fritt tilgjengelig. Spesielt er det god tilgang på skalerbare lagringsløsninger og verktøy

[18] Kommunal- og moderniseringsdepartementet (2020): Nasjonal strategi for kunstig intelligens.
[19] Stolpe, Audun, Bjørn Jervell Hansen og Jonas Halvorsen (2019): Stordatasystemer og deres egenskaper. FFI-rapport 18/01676.
[20] Zhang, Yunquan mfl. (2016): Parallel processing systems for big data: a survey. Proceedings of the IEEE, vol. 104, no. 11.

for å behandle store datamengder. Flere selskaper som håndterer store datamengder, som for eksempel Google, Facebook og LinkedIn, deler sine verktøy åpent. På den måten får de gratis hjelp med videreutvikling av verktøyene og med å håndtere feil, mens resten av verden får gratis tilgang på kraftige verktøy.

De nevnte utviklingstrekkene har vært en katalysator for utviklingen av algoritmer for automatisert analyse av informasjon, noe som er tydelig innenfor AI og spesielt den delen av AI som benevnes som maskinlæring[21]. Økt prosesseringskraft gir for eksempel mulighet for å designe nye algoritmer for maskinlæring.

Lovende resultater tilrettelagt av teknologiutviklingen, for eksempel selvkjørende biler,[22] har også økt viljen blant myndigheter og investorer til å bruke ressurser på utnyttelse og ytterligere utvikling, noe som blant annet kan sees i USA der myndighetenes investeringer innenfor AI-feltet i 2021 forventes å nå 6 milliarder USD.[23] Økte investeringer gir i sin tur utvikling, ikke minst som en følge av at fagfeltene klarer å tiltrekke seg talentfulle utviklere og forskere.

2.1.2 Nye muligheter

Den teknologiske utviklingen, med den påfølgende utviklingen av algoritmer og bruksmåter, betyr at verktøykassa som kan brukes for automatisert analyse av informasjon er fylt opp med nye verktøy. Blant de nye mulighetene som springer ut av denne utviklingen, er disse to de mest fremtredende:

Avansert bildeprosessering. En eksplosjon i antallet bilder som er fritt tilgjengelig via internett har, sammen med økningen i prosesseringskraft og stadig forbedrede algoritmer, lagt til rette for avansert automatisert bildeprosessering. Den nærmest ubegrensede tilgangen på data har gjort det mulig å trene AI-modeller ved hjelp av maskinlæring i stor skala. For eksempel er det vist at automatiserte systemer basert på maskinlærte modeller i begrensede tester kan diagnostisere hudkreft bedre enn eksperter.[24]

Automatisert tekstprosessering. På samme måte som for bilder, er internett en rik kilde til tekstdata for trening av modeller. Dette har ført til kraftig forbedrede verktøy for tekstprosessering. For eksempel har man sett at prosesseringsoppgaver som gjenkjenning av objekter og identifisering av følelser og meninger uttrykt i tekst, såkalt sentimentanalyse, har nådd en kvalitet som gjør dette brukbart i automatisert analyse.[25] I tillegg har automatisk oversettelse mellom forskjellige språk nådd en kvalitet som gjør den brukbar til begrensede oppgaver som å forstå

[21] Maskinlæring er en AI-disiplin der modeller av verden trenes opp gjennom å lære av eksempler. Et eksempel er å trene opp en modell av biler basert på millioner av bilder av biler slik at denne modellen kan benyttes til å gjenkjenne biler i nye bilder.
[22] Business Insider (2019): DeepMind is teaching Google's self-driving cars to get smarter and spot pedestrians better.
[23] National Defense (2021): Federal AI Spending to Top $6 Billion.
[24] Esteva, Andre mfl. (2017): Dermatologist-level classification of skin cancer with deep neural networks. *Nature*, vol. 542, no. 7639.
[25] Young, Tom mfl. (2018): Recent trends in deep learning based natural language processing. IEEE Computational intelligence magazine, vol. 13, no. 3.

meningen i skrevne tekster, selv om kvalitetsforskjellen sammenlignet med menneskelige oversettere fortsatt er merkbar.[26]

2.2 Skyteknologi

Innen IKT brukes ofte begrepet tjeneste om funksjoner som leveres av programvare, og det finnes en formell definisjon av begrepet.[27] Det finnes imidlertid ikke en tilsvarende entydig definisjon av hva skytjenester er, heller ikke et fast sett med standarder som slike tjenester må møte. I stedet er det vanlig å definere skytjenester i form av et sett med egenskaper som slike tjenester må inneha. Disse egenskapene er:

- generell tilgang til tjenestene via nettverk, som vil si at tjenestene nås med standard utstyr som PC, nettbrett eller mobiltelefon koplet til et nettverk (vanligvis internett)
- selvbetjent oppsett, det vil si at brukeren i stor grad kan administrere tjenestene uten å involvere leverandøren
- ressurssamling, som betyr at ressursene[28] fremstår for brukeren som samlet i ett «punkt», selv om det i virkeligheten kan være tusenvis av datamaskiner som leverer tjenestene
- rask og automatisk dekking av ressursbehov, slik at det for brukeren fremstår som tilnærmet ubegrensede ressurser; betaling etter forbruk

For flere detaljer om egenskaper ved skytjenester henviser vi til Lund mfl. (2021).[29]

Opprinnelsen til skytjenester kan spores helt tilbake til stordatamaskinene på 1950- og 60-tallet. Den gangen var datamaskiner svært dyre, og det kunne derfor være lønnsomt for flere virksomheter å gå sammen om felles maskinvare. Det var likevel først mange år senere, som en følge av utvikling både innen teknologi og marked, at grunnlaget for det vi i dag kjenner som skytjenester har blitt lagt. I løpet av de siste 10 til 15 årene har skytjenester fått svært stor utbredelse, og vi ser at også offentlig sektor i stadig økende grad tar i bruk slike tjenester. Eksempelvis sier Digitaliseringsrundskrivet[30] at «*Virksomheter som etablerer nye eller oppgraderer eksisterende fagsystemer eller digitale tjenester, eller endrer eller fornyer avtaler knyttet til drift, skal vurdere skytjenester på linje med andre løsninger.*»

Skytjenester er ikke basert på én bestemt teknologi, og det er heller ingen teknologier som er unike for slike tjenester. Likevel har teknologiutviklingen vært avgjørende for at skytjenester har kunnet oppstå. Når vi i denne rapporten snakker om skyteknologi, mener vi de teknologiene som muliggjør skytjenester.

[26] Maucec, Mirjam Sepesy og Gregor Donaj (2019): Machine Translation and the Evaluation of Its Quality. Recent Trends in Computational Intelligence, 2019.
[27] Reference Architecture Foundation for Service Oriented Architecture Version 1.0. Hentet fra https://docs.oasis-open.org/soa-rm/soa-ra/v1.0/cs01/soa-ra-v1.0-cs01.pdf
[28] Med ressurser mener vi her prosesseringskraft, lagringsplass for data og overføringskapasitet i nettverk.
[29] Lund, Ketil, Frank T. Johnsen og Arild Bergh (2021): Bruk av skytjenester i Forsvaret – muligheter og utfordringer, FFI-rapport 21/00136.
[30] Kommunal- og moderniseringsdepartementet (2019): Digitaliseringsrundskrivet.

2.2.1 Utvikling

En svært viktig teknologisk faktor er utviklingen av virtualisering. Virtuelle datamaskiner består av programvare som emulerer[31] fysiske datamaskiner, og én fysisk datamaskin kan dermed kjøre en rekke virtuelle maskiner samtidig. Disse virtuelle maskinene er helt uavhengige av hverandre, de kan emulere forskjellige typer maskinvare og de kan kjøre forskjellige operativsystem. Virtualisering muliggjør dermed langt bedre utnyttelse av fysiske datamaskiner.

En spesiell form for virtualisering er såkalte *containere*. Ved hjelp av containere kan det som tidligere var store applikasjoner[32] nå deles opp i et antall uavhengige mikrotjenester[33], hvor hver mikrotjeneste kjøres i hver sin container. En rekke slike containere kan så kjøre på samme datamaskin. Container-konseptet har eksistert siden 1979, men det var først med lanseringen av såkalte Docker-containere[34] i 2013 at bruken skjøt fart. Bruk av containere gjør det enklere å utvikle og vedlikeholde applikasjoner. Applikasjoner som er bygget med disse verktøyene og prinsippene, kalles gjerne *cloud native*[35] og danner grunnlaget for mange av dagens skytjenester.

Distribuert sky innebærer at geografisk adskilte maskiner samarbeider om å levere skytjenester. Eksempelvis er det i en del tilfeller et poeng at prosesseringen foregår nær brukeren, såkalt *edge computing*. Edge computing legger til rette for å redusere forsinkelse eller øke robustheten gjennom å være uavhengig av nettverksforbindelse til et sentralt datasenter. Bruk av distribuert sky og edge computing spiller også en vesentlig rolle i 5G, se kapittel 2.3.

En annen viktig teknologisk faktor er utviklingen av verktøy for automatisert styring og administrasjon av maskinvareressurser i datasentre, også kjent som såkalt hyperkonvergert[36] og dynamisk infrastruktur[37]. Dette gjør at en rekke fysiske datamaskiner kan samarbeide om å kjøre et antall virtuelle maskiner. Maskinvareressursene kan til enhver tid settes inn der det er behov for dem, og kjørende virtuelle maskiner kan flyttes mellom fysiske maskiner.

Andre viktige teknologiske faktorer er fremveksten av internett, som gjør det enkelt å kople seg opp mot datasentre nesten helt uavhengig av hvor man befinner seg, og utviklingen av konseptet *Infrastructure as Code* (IaC)[38] som innebærer at en IKT-infrastruktur bestående av programvare, datamaskiner og kommunikasjonsnettverk, kan bygges automatisk.[39]

[31] Å emulere maskinvare innebærer at spesiell programvare brukes til å etterlikne en fysisk datamaskin. Operativ-systemet og applikasjonene som kjører på den emulerte maskinen, vil normalt ikke kunne skille den fra en fysisk datamaskin.
[32] Med begrepet applikasjon menes i denne rapporten dataprogram som skal løse spesielle oppgaver eller gi en bestemt type informasjon. For eksempel Microsoft Word, Forsvarets kommando- og kontrollsystem NORCCIS, eller det militære logistikksystemet LOGFAS.
[33] Mikrotjenester innebærer at det som før var én stor applikasjon med mange funksjoner, i stedet deles opp i en rekke små, uavhengige moduler (mikrotjenester) som kommuniserer med hverandre, og som hver utfører én eller noen få av den opprinnelige applikasjonens funksjoner.
[34] Docker (2020): Docker.
[35] Cloud Native Computing Foundation (2018): Cloud Native Computing Foundation («CNCF») Charter.
[36] DataCenter Knowledge (2015): Understanding the Different Kinds of Infrastructure Convergence.
[37] Webopedia (2020): Dynamic infrastructure.
[38] IBM (2019): Infrastructure as Code (IaC).
[39] Ibid.

Det ligger også en forretningsmodell til grunn for utbredelsen av skytjenester. Selv om en organisasjon kan eie og drive sine egne datasentre, er den vanligste løsningen at en ekstern part leverer disse tjenestene. Det innebærer at kunden (en organisasjon eller en privatperson) kjøper tilgang til tjenester i stedet for selv å måtte investere i maskin- og programvare. Den eksterne leverandøren har ansvar for innkjøp, drift og oppdatering av maskin- og programvare samt for oppgaver knyttet til håndtering av sikkerhet.

Den eksterne leverandøren kan spesialisere seg på drift av datasentre for skytjenester og dermed oppnå svært effektiv drift. Med høy grad av standardisering av tjenestene og en stor kundemasse å fordele driftsutgiftene på, er det mulig å levere tjenestene til lav pris. Det er imidlertid også mulig å benytte en såkalt privat sky, hvor kunden har sitt eget datasenter, men hvor leverandøren har ansvaret for driften av dette. De store leverandørene av skytjenester setter inn store ressurser på å sørge for god sikkerhet rundt tjenestene de leverer.[40]

Bruken av skytjenester har vokst raskt. Per i dag er markedet verdt mer enn 210 milliarder USD på verdensbasis, og prognoser fra Gartner estimerer at det skjer en økning på mer enn 40 % i løpet av de neste to årene. [41] Koronapandemien har også bidratt til en ytterligere vekst.[42]

2.2.2 Nye muligheter

Utviklingen innen skyteknologi gir en rekke muligheter. Bruk av virtualisering muliggjør langt høyere utnyttelse av fysisk maskinvare og gjør det enklere å utvikle og vedlikeholde applikasjoner. Dette muliggjør lavere kostnader og bedre applikasjoner. Ved at man dynamisk og nærmest instantant kan flytte arbeidslaster mellom ulike maskinvareressurser oppnås økt pålitelighet ved at man ikke berøres av svikt i enkeltmaskiner. Ved å kombinere dette med store datasentre oppnås elastisiteten[43] som gir en illusjon av ubegrensede dataressurser. For brukerne innebærer dette at selv små datamaskiner som en mobiltelefon kan ha et stort antall tjenester tilgjengelig i form av skytjenester. I tillegg vil tjenestene oppleves som svært pålitelige og raske.

Ved å kjøpe tjenester fra leverandører som spesialiserer seg på leveranse av skytjenester, slipper en virksomhet å investere i og drifte egen maskinvare. I stedet kan den konsentrere seg om sin egen kjernevirksomhet. Store leverandører som driver effektivt vil kunne levere tjenester til en pris som gjør det lønnsomt for et foretak å kjøpe skytjenester fremfor å investere i et eget datasenter.[44] Slike leverandører som setter inn store ressurser på sikkerhet vil også trolig kunne levere sikrere tjenester enn mange organisasjoner med egne datasentre. Ved å benytte distribuert sky, hvor en rekke små datasentre samarbeider om å levere skytjenester, kan man oppnå lave forsinkelser og høy pålitelighet.

[40] Sensei Enterprises (2018): Google Cloud's Defense In Depth Includes Physical Security.
[41] Gartner (2020): Gartner Top Strategic Technology Trends for 2021.
[42] Canalys (2020): Global cloud services market Q2 2020.
[43] Elastisitet innebærer at regnekraften i de fysiske datamaskinene kan settes inn der det er behov. Hvis en virtuell maskin plutselig trenger mer regnekraft, kan den flyttes over til en kraftigere datamaskin. Dette skjer raskt, automatisk og uten at det merkes i den virtuelle maskinen.
[44] Riktignok kan prismodellene for leverandører av skytjenester være svært komplekse, og det kan være krevende å beregne på forhånd hva kostnadene faktisk vil bli.

2.3 Femte generasjons kommersiell mobilteknologi (5G)

5G er en samling teknologier som muliggjør datakommunikasjon tilpasset bruk i ulike situasjoner med svært ulike krav til overføringshastighet, pålitelighet og lav forsinkelse for mobile brukere.

Kommersiell mobilteknologi har utviklet seg gjennom flere teknologigenerasjoner. Da andre generasjons mobilteknologi (GSM)[45] ble tatt i bruk for omtrent 30 år siden, var formålet med mobilnettene å tilby tale overalt. For tredje (3G) og fjerde (4G) generasjons mobilteknologi har økt databruk vært hovedfokus for teknologiutviklingen. De nærmeste årene vil mobilteknologien tas i bruk innen langt flere bruksområder og i langt større skala enn i dag, som en følge av innføring av femte generasjons mobilteknologi (5G). Første fase av 5G er i ferd med å tas i bruk i de kommersielle mobilnettene, men teknologien vil utvikles vesentlig de neste årene.

2.3.1 Utvikling

Den meste utbredte mobilteknologien i dag er 4G. 4G tilbyr relativt høy overføringshastighet til smarttelefoner og andre personlige enheter, eller til 4G-bredbåndsmodem som gir trådløs dekning i hus, hytter og andre lokasjoner. 4G inneholder tilpasninger for andre typer brukerutstyr enn mobiltelefoner, for eksempel strømmålere i private hjem og gatebelysning.[46] Det at slike enheter kobles til internett gir mulighet for smart overvåking og styring av ulike enheter.

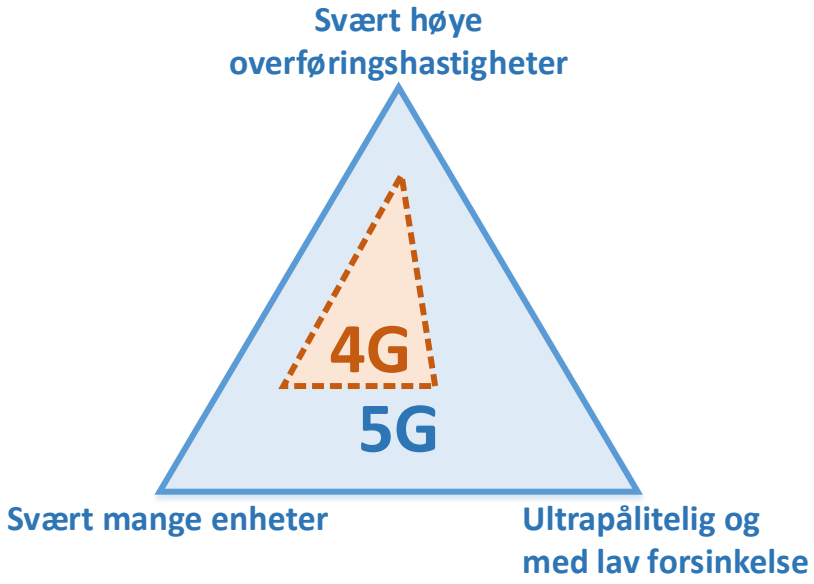
4G kan benyttes til mye, men samtidig går utviklingen innen IKT raskt og kravene til hva mobilnettene forventes å levere ser ut til å akselerere. Som følge av dette har den internasjonale telekommunikasjonsunion (ITU) definert en visjon for neste generasjons mobilnett (IMT 2020)[47] som inneholder krav i tre dimensjoner:

- *Svært høye overføringshastigheter*. 5G skal gi mulighet for vesentlig høyere overførings-hastigheter enn 4G.
- *Svært mange enheter*. Det skal være mulig å ha svært mange tilkoblede enheter selv på mindre geografiske områder. Dette er drevet av forventningene om at «alt» i fremtiden vil være tilkoblet internett. 5G skal støtte langt flere enheter enn 4G.
- *Ultrapålitelig og med lav forsinkelse*. Dette er en type tjeneste til brukere og enheter som har spesielle behov for at kommunikasjonen alltid virker eller som krever at det går svært kort tid fra informasjon sendes til den mottas.

5G er mobilbransjens svar på kravene fra ITU.[48] Figur 2.1 viser ITUs visjon for 5G og illustrerer at 4G bare i begrenset grad oppfyller denne visjonen. Det er viktig å være klar over at 5G fortsatt

[45] Global System for Mobile Communication (GSM) var en europeisk standard. I for eksempel USA ble andre teknologier enn GSM brukt.
[46] Disse teknolgiene heter Narrowband IoT og LTE-M.
[47] ITU-R (2015): IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond. Recommendation ITU-R M.2083-0 (09/2015).
[48] Bransjen har samlet seg i organisasjonen 3GPP som utarbeider fritt tilgjengelige standarder for mobilnettene. Arkitekturen til 5G er spesifisert i 3GPP, Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2 (Release 16), 3GPP TS 23.501 V16.7.0 (2020-12).

er i utvikling, og ny funksjonalitet som vil bidra til å innfri kravene fra ITU vil bli tilgjengelig de kommende årene.[49] I første fase av 5G er fokuset mest på svært høye overføringshastigheter.



Figur 2.1 Illustrasjon av de tre dimensjonene i ITU sin visjon for 5G, og hvordan 5G går lengre i disse dimensjonene enn 4G. Hva som faktisk blir tilgjengelig avhenger blant annet av etterspørselen i markedet.[50]

5G er ikke en enkeltstående teknologi, men snarere en samling av teknologier. Noen av disse er spesielt utviklet for 5G mens andre er utviklet for annen bruk og tatt i bruk i 5G. Vi gir her en oversikt over hva som er nytt med 5G og hva som vil bli teknisk mulig de kommende årene.

Med 5G innføres en ny radioteknologi som brukes på den trådløse forbindelsen mellom basestasjonene og brukerutstyret – 5G New Radio (NR). 5G NR benytter flere frekvensområder enn 4G, noe som sammen med moderne antenneteknologier[51], muliggjør svært høye overføringshastigheter. Disse hastighetene er dog bare tilgjengelig ved relativt kort avstand mellom basestasjon og brukerutstyr. De aller høyeste overføringshastighetene vil kun være tilgjengelig i byer, der det er kort avstand mellom basestasjonene, eller på avgrensede områder der det er etablert dekning av spesielle grunner.

For å kunne håndtere svært mange tilkoblede enheter, benyttes egne protokoller og tilpasninger i de lavere frekvensene for å kunne utvide dekningen for enheter som sender små mengder data. En sensor som ikke flytter på seg kan gi nettverket beskjed om at den er i «dvalestatus» og da slipper den å bruke strøm på å holde forbindelsen til nettet ved like. Slike tilpasninger gjør det

[49] 3GPP utgir med ca 1,5 års mellomrom nye versjoner (Releases) av standardene. Mye av funksjonaliteten i 5G kom i Release 15 fra 2019, mens Release 16 fra 2021 er offisiell kandidat for å bli godkjent av ITU som IMT 2020.
[50] Figuren er basert på ITU-R (2015).
[51] Som *Massive* MIMO. MIMO er en forkortelse for multiple-input and multiple-output. MIMO innebærer at antennen på basestasjonen er satt sammen av en gruppe av mange antenner som virker sammen for å kunne sende og motta flere signaler samtidig.

mulig at batteriene i disse enhetene kan vare i flere år. Støtte for svært mange tilkoblede enheter er ventet å bli tilgjengelig i de kommersielle mobilnettene når de innfører 5G-nett som fungerer uavhengig av 4G.

Kommunikasjon over 5G som er ultrapålitelig og med lav forsinkelse er den teknisk mest krevende dimensjonen å realisere, siden det forutsetter at mobilnettene bygges på nye måter.[52] I tillegg til radionettet inneholder et komplett 5G-nett, og andre mobilnett, et transportnett som hovedsakelig består av fiberforbindelser mellom basestasjonene og resten av verden, samt det såkalte *kjernenettet* som inneholder funksjoner for å holde styr på abonnenter og fordele datastrømmene til riktig mottaker. 5G NR inneholder funksjonalitet som gjør overføringen av data mellom brukerutstyr og basestasjon mer robust mot feil under overføringen, ved at eventuelle feil oppdages fort og at data som går tapt kan sendes på nytt.

Tradisjonelt har mobilnettene hatt noen få sentraler som alle datastrømmene har gått gjennom. I et langstrakt land som Norge kan det for brukere som krever lav forsinkelse være nødvendig å beholde informasjonen i kanten av transportnettet, nær brukerne, i stedet for å sende informasjonen via sentraler i andre deler av landet. For å støtte dette har 5G tatt i bruk teknologien *edge computing*, se også kapittel 2.2.1. Bruk av edge computing i 5G vil si at et lokalt lite datasenter er plassert i kanten av 5G-nettet og gjør at brukeren opplever lav forsinkelse.

Som vi nettopp har sett skal 5G-nettverkene støtte mange forskjellige typer brukere med til dels ulike og motstridende behov. Det vil ikke være mulig å møte alle disse behovene samtidig for alle brukerne. Med 5G innføres derfor såkalte nettverksskiver (*Network Slices*). Nettverksskiver åpner opp for at tjenester kan tilpasses ulike brukergrupper på ulike måter. I tillegg til egenskapene diskutert over har 5G noen nye sikkerhetsmekanismer sammenlignet med 4G og en nettverksskive kan brukes for å gi høyere sikkerhet eller prioritet for enkelte brukergrupper.[53] Bruk av nettverksskiver omtales gjerne som skivedeling.

Offentlige 5G-nett eies av en mobiloperatør, og alle som ønsker det kan kjøpe abonnement på mobiltjenester levert av disse nettene på kommersielle vilkår.[54] Noen brukergrupper kan ha så høye krav til for eksempel sikkerhet at de ønsker seg et helt frittstående nettverk som ikke deles med andre brukere, et såkalt privat 5G-nett. Disse nettene kan være geografisk begrenset til for eksempel en fabrikk eller en havn. Private 5G-nett forutsetter at det settes av egne frekvenser, og Nasjonal kommunikasjonsmyndighet (NKOM) sendte i juni 2021 ut et forslag på høring om at enkelte frekvenser vil bli satt av til private 5G-nett.[55]

Det sterke fokuset på 5G gjør den til en driver for utvikling av nye tekniske løsninger og standarder. Et område hvor 5G utgjør en slik driver er innen styring og kontroll (*management*) av

[52] 5G Americas (2018): New Services and Applications with 5G Ultra-reliable and low latency communications. 5G Americas whitepaper, November 2018.
[53] Farsund, Bodil Hvesser og Anne Marie Hegland (2020): 5G i Forsvaret – muligheter og sikkerhetsutfordringer. FFI-eksternnotat 20/01206.
[54] I Norge har vi i dag tre offentlige mobilnett eid av operatørene Ice, Telenor og Telia. Alle mobilnettene er i ferd med å bli oppgradert til 5G. Abonnement kan kjøpes fra disse operatørene eller av såkalte mobile virtuelle nettverksoperatører som også benytter disse mobilnettene.
[55] Nasjonal kommunikasjonsmyndighet (2021): Høring av lokale 5G-nett i 3,8-4,2 GHz-båndet. Høring. 9. juni 2021.

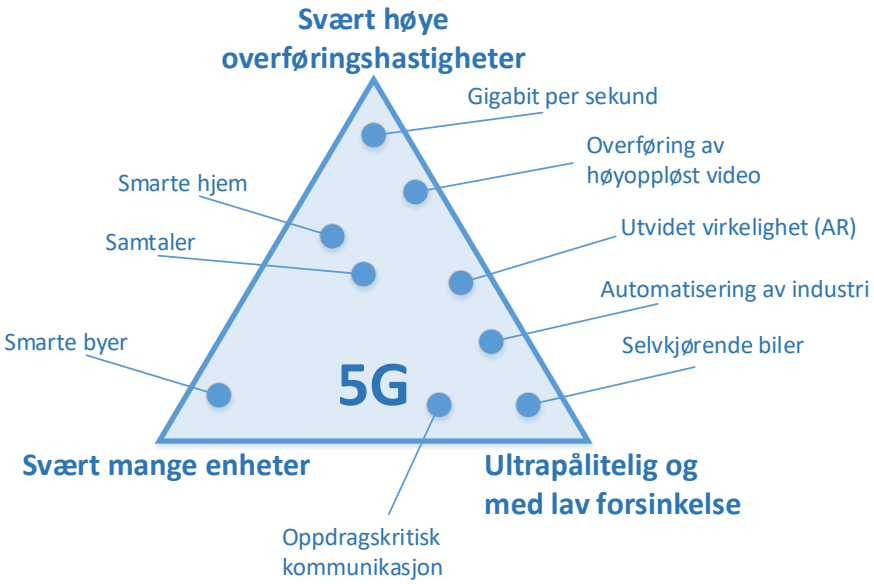
kommunikasjonsnettverk. Fordi nettene skal kunne tilpasses så mange ulike brukere må management foregå automatisert, og det tas også i bruk kunstig intelligens for å styre 5G-nettene. Det utvikles også grensesnitt (API-er) hvor brukere løpende kan tilpasse tjenestene sine gjennom selvbetjening.

2.3.2 Nye muligheter

Utviklingen innen 5G gir mange nye muligheter. Figur 2.2 viser noen muligheter som ITU ser for seg i sin visjon. Det er naturligvis mulig at det oppstår nye behov de nærmeste årene som blir langt viktigere enn mulighetene som er vist i figuren.

På overordnet nivå vil vi fremheve følgende muligheter:

- Det blir mulig å overføre store datamengder slik som flere samtidige strømmer av høyoppløst video.
- Svært mange enheter av ulik form og størrelse kan kobles sammen. Et 5G-nett kan for eksempel benyttes til å samle inn informasjon fra et stort antall sensorer som kan plasseres ut for kortere eller lengre tidsperioder.
- Funksjonaliteten kan tilpasses ulike behov til forskjellige brukergrupper, enten ved bruk av skivedeling eller gjennom utnyttelse av private 5G-nett.



Figur 2.2 Eksempler på nye muligheter som 5G gir.

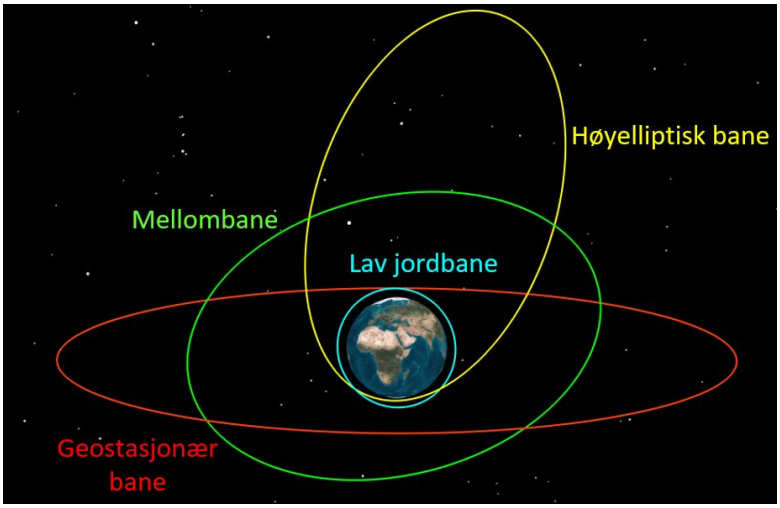
I hvilken grad alle behov i figur 2.1 vil bli dekket av 5G, avhenger ikke bare av hvilken teknologi som er utviklet. Det er også et spørsmål om hvilke brukergrupper som har vilje til å betale for å få realisert de ulike løsningene. Utstyrsleverandører og nettverksoperatører må vurdere om de ulike typene brukere har stor nok betalingsvilje til at investering i utvikling av nettverksutstyr og

tilpasning av mobilnettene vil lønne seg. Usikkerheten om hva som er lønnsomt å legge til rette for ser ut til i størst grad å gjelde dimensjonen «Ultrapålitelig og med lav forsinkelse».

2.4 Langtrekkende høyhastighetskommunikasjon

Med langtrekkende høyhastighetskommunikasjon mener vi i denne rapporten teknologi som muliggjør datakommunikasjon med høy overføringshastighet over svært lange avstander uten bruk av jordbundne løsninger som fiber og radiolinje. Teknologien omfatter satellittsystemer og andre eleverte kommunikasjonsreléer.

Utstrakt bruk av kommersiell mobilteknologi, beskrevet i kapittel 2.3, har ført til at det nå forventes at høyhastighetskommunikasjon er tilgjengelig overalt. Forbrukere forventer å kunne overføre store mengder data i form av bilder, websider og video uten ventetid. Trådløs høyhastighetskommunikasjon krever enten kort avstand eller tilnærmet fri sikt mellom sender og mottaker. I kommersielle mobilnett bygges det følgelig svært tett med basestasjoner, slik at typisk avstand mellom basestasjon og bruker er fra noen hundre meter til noen få kilometer. Denne type utbygging er lite lønnsom utenfor befolkede områder og umulig over havområdene. En løsning som gir dekning over store avstander er å bruke reléer i stor høyde, da dette gir fri sikt til reléet fra store områder. Avhengig av høyde over bakken kan dette være en satellitt eller en flyvende farkost. Satellitter kan gå i ulike satellittbaner rundt jorda, med ulike egenskaper knyttet til dekning, omløpstid og signalforsinkelse og dermed kostnader og bruksområde, se figur 2.3 og tabell 2.1.



Figur 2.3 Ulike typer satellittbaner.

2.4.1 Utvikling

Omfattende kommersialisering av romteknologi sammen med teknologisk utvikling har nå gjort det mulig å lage satellitter mye billigere enn tidligere. Dette gjelder særlig for mindre satellitter i lav jordbane, hvor satellittene utsettes for mindre kosmisk stråling og dermed kan bygges ved

hjelp av billigere komponenter. Selv satellitter på størrelse med en skoeske kan gi svært nyttige tjenester, som for eksempel de norske AIS[56]-satellittene.[57]

Tabell 2.1 Typiske egenskaper ved ulike typer satellittbaner.

	Geostasjonær	**Høyelliptisk**	**Mellombane**	**Lav jordbane**
Høyde over bakken [km]	35 786	1000–40 000	8 000–22 000	500–2 000
Omøpstid [timer]	~24[58]	~12–24	8–12	1,5–2
Forsinkelse [ms]	~540	~200–600	~120	~30
Antall satellitter for global dekning	3 for dekning mellom ~±81° N/S	2 for kontinuerlig dekning av nordområdene	~24	~66++
Eksempelsystem	Satellitt-TV	ASBM[59]	Navigasjons-systemet GPS	Kommunikasjons-systemet Iridium

Satellittoppskyting blir billigere og mer tilgjengelig både på grunn av konkurranse blant operatørene av større raketter, som for eksempel SpaceX og ArianeSpace, og på grunn av nye selskaper som sikter direkte mot småsatellittmarkedet, for eksempel Electron og Virgin Galactic. Kombinert med lave kostnader for å bygge satellitter gjør dette det mulig å lage nye satellitter tilpasset oppgavene mye raskere enn tidligere, og satellitter kan dermed erstattes raskere.

Utvikling av antenner med såkalt elektronisk strålestyring gjør det mulig å lage billigere bruker-terminaler enn tidligere. Elektronisk strålestyring innebærer at antennen ikke har noen bevegelige deler, samtidig som strålen kan pekes elektronisk mot satellitten i løpet av et brøkdels-sekund. Slike antenner er særlig relevant for terminaler som kan kommunisere mens de er i bevegelse, for å kommunisere med satellitter som flytter seg på himmelen og for sømløst å bytte mellom for-skjellige satellitter.

Økt behov for kapasitet fører til bruk av stadig høyere frekvensbånd.[60] Bruk av høyere frekvenser og optisk kommunikasjon kan også bidra til økt robusthet. For eksempel vil optiske intersatellitt-linker[61] kraftig kunne forbedre dekningsområdet av satellittkonstellasjoner i ikke-geostasjonære baner ved å gjøre dem mindre avhengig av et stort antall kostbare bakkestasjoner.

Billigere satellitter, samt pengesterke investorer som Amazon, SpaceX og andre, fører til at flere nye systemer for satellittkommunikasjon nå er på vei til å realiseres. Felles for disse systemene er at de ikke benytter geostasjonær bane, men i stedet høyelliptiske og, lav- og mellombaner. Noen

[56] AIS (Automatic Identification System) er et automatisk identifikasjonssystem for skipstrafikk.
[57] Kystverket (2020): AIS Norge.
[58] Geostasjonære satellitter står stille på horisonten sett fra bakken.
[59] ASBM (Arctic Satellite BroadBand Mission) er et kommende norsk statseid kommunikasjonssystem for bredbånd i Arktis. https://www.regjeringen.no/no/aktuelt/etablerer-bredbandskommunikasjon-i-nord/id2661494/
[60] Ka-bånd (20/30 GHz), Q-bånd (40/50 GHz), W-bånd (70/80 GHz) og optisk kommunikasjon.
[61] Intersatellittlinker brukes til kommunikasjon mellom satellitter.

systemer, som Starlink fra SpaceX eller Kuiper fra Amazon, skal bestå av flere tusen satellitter hver, mens andre "bare" av noen hundre.[62] [63] Systemene Starlink fra SpaceX, satellitt-konstellajonen til OneWeb, og LightSpeed fra Telesat er trolig mest relevante for bruk i Norge, da disse har konkrete planer for å tilby dekning i norske områder. I tillegg kommer ASBM fra Space Norway AS og geostasjonære satellitter med oppgradert funksjonalitet, som for eksempel Viasat-3. På militær side har utviklingen også startet i USA med Blackjack[64] og Space Development Agency Transport Layer[65].

Innenfor atmosfæren har ubemannede luftfartøyer, eller UAV (Unmanned Aerial Vehicle), av forskjellige størrelse blitt et vanlig verktøy, både for militære og sivile formål, og bruken antas å øke fremover.[66] Militære styrker i minst 100 land har nå tatt i bruk bevæpnede eller ubevæpnede UAV-er, og et økende antall land har brukt dem i kamphandlinger.[67] Som for satellitter er trenden å gå fra tyngre enheter mot mindre og billigere enheter. Plattformutvikling på dette området er også svært nyttig for deres bruk som kommunikasjonsrelé.

2.4.2 Nye muligheter

Utviklingen innen dette teknologiområdet fører til drastisk økning av tilgjengelig overførings-hastighet på steder uten godt utbygd bakkebasert infrastruktur. Selv om mye av denne økningen vil skje på lavere breddegrader enn de Norge ligger på, vil også dekning i nordområdene forbedres kraftig. Slik kapasitetsøkning vil typisk medføre kraftig reduksjon i pris for enkeltbrukere.

Satellitter i lav- og mellombane er nærmere jorda enn satellitter i geostasjonære baner, noe som medfører at radiosignalene bruker kortere tid mellom bakken og satellittene. Økt bruk av slike satellitter fører dermed til lavere forsinkelse for brukerne av systemene. I stedet for en typisk forsinkelse på 540 ms vil man oppleve forsinkelser på 100 ms og lavere. Lavere forsinkelse åpner for nye muligheter spesielt ved bruk av autonome enheter, men også for andre applikasjoner, som telemedisin, som krever rask respons. En del vanlig brukte kommunikasjonsløsninger og -proto-koller er også følsomme for forsinkelse og vil ikke fungere hvis de brukes over forbindelser med høy forsinkelse. Kombinasjonen av høy overføringshastighet og lav pris gjør det derfor mulig å bruke satellittkommunikasjon som reserve for, eller erstatning for, bakkebaserte løsninger basert på radiolinjer og optisk fiber. Ved bruk av optiske intersatellittlinker kan denne erstatningen bli konkurransedyktig på forsinkelse og overføringshastighet også over veldig lange avstander.

Billigere brukerterminaler som klarer å kommunisere i bevegelse, i kombinasjon med lavere pris for tjenestene, vil føre til at satellittkommunikasjon ikke bare kan benyttes på store fly og fartøyer, men også på små (og muligens autonome) fly, båter og kjøretøy i stor skala.

[62] Spacenews (2021a): FCC approves Starlink license modification.
[63] Spacenews (2020): Amazon's Kuiper constellation gets FCC approval.
[64] Airforce Technology (2020): Project Blackjack: DARPA's LEO satellites take off.
[65] Spacenews (2021b): DoD space agency to award multiple contracts for up to 150 satellites.
[66] Business Insider (2021): Drone technology uses and applications for commercial, industrial and military drones in 2021 and the future.
[67] Defensenews (2021): Weapons of the future: Trends in drone proliferation.

Ved å benytte flere systemer som hver for seg er bygget opp rundt flere satellitter, for eksempel i lav- og mellombane, vil kommunikasjonsløsningen kunne være mer robust enn hvis den er basert på et lite antall store og dyre satellitter.[68] Et system basert på flere satellitter vil kunne fortsette å fungere tross utfall av et mindre antall satellitter uten betydelige konsekvenser. Satellitter i slike systemer kan også lettere og raskere erstattes, både på grunn av lavere pris og billigere og enklere oppskyting med mange oppskytingsmuligheter selv på kort varsel.[69] Bakketerminaler som lett klarer å bytte mellom forskjellige kommunikasjonssatellitter vil bli tilgjengelige og kan dermed øke robustheten ytterligere.

Selv med et stort antall forskjellige systemer og tjenester tilgjengelig fra både sivile og militære aktører, vil det alltid være behov som ikke er fullstendig dekket av disse. En av de store fordelene med den pågående utviklingen blir muligheten for å lage egne satellittløsninger tilpasset spesielle behov til en lav kostnad. De norske AIS-satellittene er et godt eksempel. Andre er forskjellige typer satellitt-IoT[70], for eksempel SWARM, som tilbyr svært billig overføring av veldig små datamengder til mottakere på noen få centimeter ved bruk av satellitter som veier bare 400 gram.[71]

Det har vært en viss interesse for å tilby kommunikasjonsløsninger basert på lette flyvende plattformer (UAV-er) som flyr høyt i atmosfæren, blant annet fra Facebook (Aquila), Google Loon/Raven Aerostar og Thales (Stratobus). I skrivende stund ser det ut som de fleste av disse initiativene er kansellert eller stoppet på grunn av enten umoden teknologi eller for store kostnader. Disse typer plattformer er dessverre lite egnet for bruk i norske områder på grunn værforholdene i høyere atmosfæriske lag.[72]

Utviklingen av tyngre flyvende plattformer som fungerer som relé foregår fortsatt, og noen kostbare løsninger, som for eksempel BACN[73] på den ubemannede Global Hawk[74], har vært i militær bruk i noen år allerede. En annen løsning er å bruke noe lettere og billigere plattformer som opererer sammen i større antall, men i lavere høyder enn UAV-ene omtalt i forrige avsnitt.[75] En slik løsning er også gunstig på grunn av kort avstand mellom UAV-ene og kort avstand til bakken. De korte avstandene gjør det mulig å bruke høye radiofrekvenser som kan utnytte atmosfærens egenskaper for bedre robusthet mot elektronisk krigføring[76] og samtidig tilby høy kapasitet.

[68] Harrison, Todd mfl. (2021): Defense against the dark arts in space – Protecting Space Systems from Counterspace Weapons. Center for Strategic & International Studies (CSIS) Report, February 2021.
[69] Harrison, Todd mfl. (2021).
[70] Satellitt-IoT (Internet of Things) bruker satellitter til å overføre små mengder informasjon fra et stort antall billige små terminaler, disse kan for eksempel være sporingsbrikker.
[71] Swarm (2021): Swarm.
[72] Jodalen, Vivianne mfl. (2019): Kommunikasjon i nordområdene – beskrivelse av utvalgte teknologier. FFI-rapport 19/00628. BEGRENSET.
[73] Northrop Grumman (2021a): Battlefield Airborne Communications Node (BACN).
[74] Northrop Grumman (2021b): Global Hawk.
[75] Hamilton, Thomas og David Ochmanek (2019): Operating Low-Cost Reusable Unmanned Aerial Vehicles in Contested Environments. RAND Corporation.
[76] Ibid. kap. 5.

3 Mulig bruk i Forsvaret

Dette kapittelet beskriver fire eksempler på hvordan Forsvaret kan dra nytte av teknologiutviklingen og mulighetene som er beskrevet i kapittel 2. Eksemplene omhandler effektiv og sikker IKT-infrastruktur (kapittel 3.1), samvirke i totalforsvaret (kapittel 3.2), mobilitet og hurtighet i militære operasjoner (kapittel 3.3) og utnyttelse av sensordata (kapittel 3.4).

3.1 Effektiv og sikker IKT-infrastruktur

For at Forsvaret skal kunne gjennomføre sine operasjoner på en mest mulig effektiv og sikker måte, trengs det en IKT-infrastruktur som knytter de ulike avdelingene og hovedkvarterene sammen. En IKT-infrastruktur består av programvare, datamaskiner og kommunikasjonsnettverk og tilbyr grunnleggende funksjoner som flytting, lagring og prosessering av data. I dag har Forsvaret en omfattende IKT-infrastruktur som består av et landsdekkende kommunikasjonsnettverk og en rekke forskjellige informasjonssystemer[77] fordelt på mange lokasjoner. I tillegg til slike stasjonære komponenter har Forsvaret en rekke mobile komponenter som kan brukes til å forsterke infrastrukturen i operasjonsområder.

Å legge til rette for sikker og effektiv samhandling mellom ulike typer militære styrker og hovedkvarterer på ulike kommandonivåer både i fred, krise og krig stiller svært høye krav til IKT-infrastrukturen. Infrastrukturen skal fungere under krevende forhold og den skal gjøre det mulig å utveksle sikkerhetsgradert informasjon på ulike nivåer. I de mobile delene av infrastrukturen er utfordringene ekstra store ved at flere komponenter til enhver tid vil kunne være i bevegelse.

Forsvaret benytter i dag til dels IKT-løsninger som fungerer isolert og autonomt. Løsningene dekker lokale behov, men ytelsen er begrenset av den lokale maskinvaren og programvaren. Det benyttes flere ulike IKT-løsninger i ulike deler av Forsvaret, og det er ofte etablert egne IKT-løsninger for hvert graderingsnivå med ulike oppsett av maskinvare og egne programvareversjoner. Dette gjør det ekstra krevende å drifte løsningene på en effektiv måte. Før Forsvaret kan starte en operasjon må det ofte planlegges nøye hvordan informasjonssystemene skal konfigureres ut i fra hva slags samhandling som skal foregå og hvem som skal delta i operasjonen. IKT-løsningene er ikke nødvendigvis klargjort for å kunne omkonfigureres under en operasjon, og det kan dermed være vanskelig å legge til rette for nye mønstre for samhandling som måtte oppstå mens en operasjon pågår.

3.1.1 Forbedring av Forsvarets IKT-infrastruktur ved bruk av skyteknologi og 5G

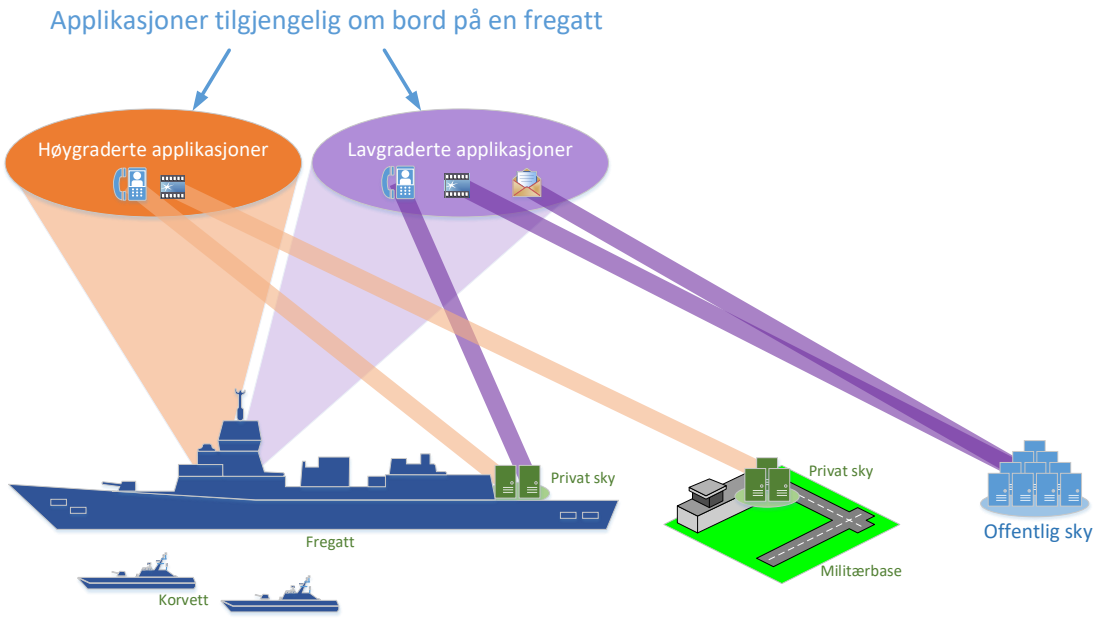
Som beskrevet i kapittel 2.2, innebærer virtualisering at virtuelle datamaskiner emulerer oppførselen til fysiske datamaskiner slik at flere virtuelle datamaskiner med ulike applikasjoner kan kjøre på samme fysiske maskinvare. Kommunikasjonsnettverk kan også virtualiseres ved at den

[77] Med informasjonssystemer mener vi her datamaskiner og programvare som er satt sammen for å fungere som ett system.

samme infrastrukturen leverer flere virtuelle nettverk.[78] Brukerne ser sine egne virtuelle datamaskiner og sitt eget nettverk og er ikke klar over virtualiseringen.

I bunnen vil vi fortsatt ha de fysiske nettverkene og datamaskinene, men oppå denne fysiske infrastrukturen kan vi bygge flere virtuelle infrastrukturer (både datamaskiner og nettverk) som deler de fysiske ressursene. De virtuelle informasjonssystemene vi da får trenger ikke være lokalisert til ett geografisk sted, slik mange av dagens informasjonssystemer er. Dette kan utnyttes på flere måter, for eksempel kan de samme tjenestene gjøres tilgjengelig om bord på en fregatt og i et hovedkvarter.

Figur 3.1 viser hvordan applikasjoner brukt på en fregatt kan leveres fra ulike geografiske steder gjennom bruk av virtualisering. Ovalene øverst i figuren illustrerer to virtuelle nettverk som tilhører hvert sitt graderingsnivå. Brukerne ombord på fregatten kan bruke applikasjonene uavhengig av hvor maskinvaren som leverer applikasjonene befinner seg – her eksemplifisert med en liten privat sky om bord på fregatten, en noe større privat sky som befinner seg i en militærbase eller i en svært stor offentlig sky[79]. Strekene ned til de ulike skyene indikerer hvor en applikasjon leveres fra men brukerne slipper å forholde seg til hvor applikasjonene faktisk kjører.



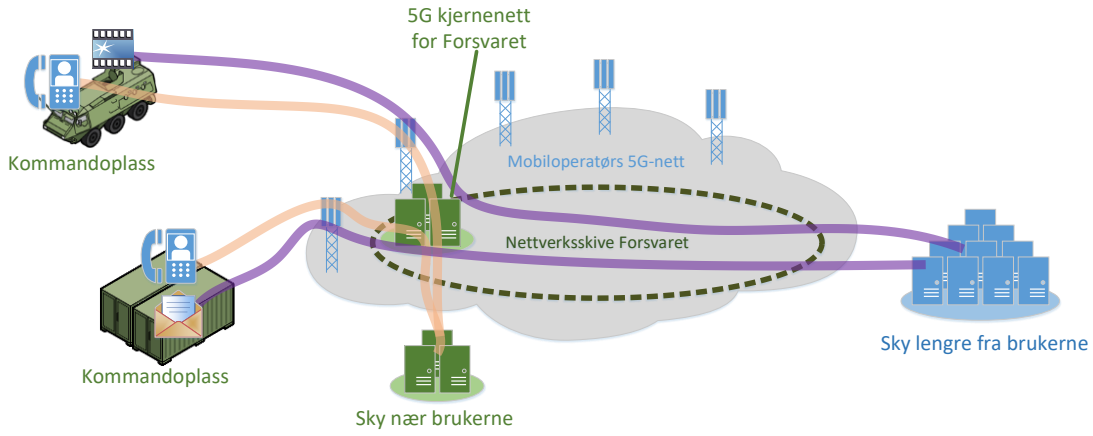
Figur 3.1 Eksempel. Applikasjoner tilgjengelig på en fregatt kan leveres fra ulike lokasjoner ved hjelp av virtualisering.

I eksempelet benytter den lokale maskinvaren ombord på fregatten skyteknologi og fungerer sømløst sammen med de større skyene. En privat sky ombord brukes til applikasjoner som er

[78] Chowdhury, N. M. Mosharaf Kabir og Raouf Boutaba (2009): Network virtualization: state of the art and research challenges. IEEE Communications Magazine, vol. 47, no. 7, s. 20–26, July 2009.
[79] Med offentlig sky menes skytjenester som tilbys av en kommersiell leverandør, hvor selve skyen er tilgjengelig for alle mens tilgangen til tjenestene kan begrenses til ønsket brukergruppe.

oppdragskritiske, mens andre applikasjoner kan kjøres fra sentrale skyer. Med skyteknologi, som vi introduserte i kapittel 2.2, kan applikasjoner enkelt flyttes mellom ulike datasentre. Dersom situasjonen endrer seg, kan andre applikasjoner enn tidligere bli oppdragskritiske. Forsvaret kan da raskt gjøre endringer på hvilke applikasjoner som leveres fra der brukerne befinner seg. I situasjoner der kommunikasjon mellom fregatt og land skulle falle ut, vil brukerne på fregatten ikke miste tilgang til applikasjonene som er kritiske. Dersom fregatten opererer i en fartøygruppe – og det finnes kommunikasjon mellom fartøyene – kan de mindre fartøyene få tilgang til de samme applikasjonene som fregatten benytter.

En del applikasjoner kan fungere lokalt, men mange applikasjoner benyttes til samhandling og informasjonsdeling mellom personell på ulike lokasjoner. Her er gode kommunikasjonsløsninger avgjørende. Når en fartøygruppe opererer langt til sjøs vil satellittkommunikasjon være den mest aktuelle teknologien, og nye konstellasjoner som beskrevet i kapittel 2.4, gjør satellittkommunikasjon til en enda mer aktuell løsning i fremtiden. I landdomenet vil 5G kunne være en av de primære kommunikasjonsløsningene Forsvaret benytter da dekningen fra de offentlige mobilnettene er god. Ved å benytte 5G kan man oppnå høy overføringskapasitet mellom brukere og applikasjoner som befinner seg på forskjellige lokasjoner. Som beskrevet i kapittel 2.3, gir 5G New Radio (NR) mulighet for langt høyere overføringshastigheter enn tidligere generasjoner mobilteknologi.



Figur 3.2 *Egen nettverksskive for Forsvaret etablert i 5G-nettet til en mobiloperatør. Nettverksskiven knytter Forsvarets oppdragskritiske tjenester til en sky nær brukerne mens andre tjenester kjøres i en sky lengre fra brukerne.*

5G legger også til rette for utnyttelse av edge computing som nevnt i kapittel 2.3. Der tidligere generasjoner av mobilteknologien sendte alle data via sentrale lokasjoner hos nettverksoperatøren, blir det med 5G mulig å sende data direkte til applikasjoner som kjøres fra en sky som befinner seg nær brukeren, som vist i figur 3.2. Dette kan realiseres ved å utnytte en egen nettverksskive for Forsvaret i mobiloperatørens 5G-nett. En nettverksskive er, som beskrevet i kapittel 2.3, en måte å levere ulike tjenester til ulike brukergrupper. Ved hjelp av edge computing og skivedeling kan Forsvarets tjenester fungere selv om forbindelsene inn til operatørens sentrale

datasenter skulle falle ut. En forutsetning for at dette skal fungere er at mobiloperatøren etablerer et komplett lokalt 5G-kjernenett i Forsvarets nettverksskive.

For å oppnå robusthet benytter Forsvaret flere ulike kommunikasjonsløsninger. I fremtiden vil det bli mulig å benytte andre tilknytningsmuligheter til en 5G-nettverksskive enn NR. For eksempel kan en mobil kommandoplass benytte fiber eller Wi-Fi for å koble seg til mobiloperatørens 5G-nett og dermed nå Forsvarets nettverksskive i 5G-nettet.

Forsvaret kan oppnå flere fordeler ved å benytte skyteknologi og 5G i infrastrukturen som beskrevet i dette kapittelet. Skyteknologi gjør at tjenester kan kjøres sentralt og dermed reduseres omfanget på maskinvare som må bringes ut i felt, hvor det ofte kan være begrenset tilgjengelighet av oppbevaringsplass, kjøling og strøm. Virtualisering og skyteknologi bidrar til variantbegrensning av maskinvare siden kommandoplasser kan bruke samme type maskinvare. Enhetlig maskinvare og gjennomgående bruk av skyteknologi vil også kunne forenkle drift og vedlikehold av informasjonssystemene og redusere behov for lokalt tilgjengelig personell med kompetanse på ulike systemer. Ved at Forsvaret tar i bruk en egen nettverksskive i 5G-nettet blir det mulig å utnytte lokale skyer når brukerne er tilkoblet mobilnettet. Ved å benytte lokale skyer kan Forsvaret høste fordeler fra skytjenester samtidig som man unngår utfordringer knyttet til avhengigheter til noen få sentrale lokasjoner.

3.2 Samvirke i totalforsvaret

Digitaliseringsstrategien for Forsvaret sier at *«[s]amfunnsoppdraget krever økt deling av informasjon på tvers og bedre samhandling med myndigheter og andre samfunnsaktører*» og *«[det er] behov for gode samhandlingsløsninger for å raskt få oversikt over situasjonen og koordinere på tvers*».[80]

Totalforsvaret innebærer at både sivile og militære ressurser kan nyttes til å løse utfordringer mot både samfunns- og statssikkerheten, og videreutvikling av totalforsvaret er et av tiltakene regjeringen har identifisert for å styrke forsvaret av Norge.[81] I totalforsvarskonseptet legges det vekt på gjensidig støtte og samarbeid mellom sivile og militære aktører, og at Forsvaret har blitt mer integrert med sivilsamfunnet med tanke på blant annet kompetanse, tjenester og teknologi.[82] For Forsvarets del innebærer dette å bidra i håndteringen av samfunnssikkerhetsutfordringer også i fred og de lavere krisenivåene. I de senere år har vi sett flere eksempler på at Forsvaret har bistått i hendelser i sivilsamfunnet, for eksempel i forbindelse med Viking Sky-hendelsen i 2019[83] og kvikkleireskredet i Gjerdrum ved årsskiftet 2020/21[84].

[80] Forsvaret (2018).
[81] Forsvarsdepartementet (2020c): Prop. 1 S (2020–2021).
[82] Forsvarsdepartementet og Justis- og beredskapsdepartementet (2018): Støtte og samarbeid: En beskrivelse av totalforsvaret i dag.
[83] Direktoratet for samfunnssikkerhet og beredskap (2020a): Evaluering av Viking Sky-hendelsen. Rapport.
[84] Forsvaret (2021): Åpnet Forsvarets verktøykasse under redningsarbeidet i Gjerdrum.

Ved større hendelser er det gjerne mange myndigheter, virksomheter og etater som må samarbeide. Det er derfor etablert et sett med grunnleggende prinsipper for arbeidet med samfunnssikkerhet og beredskap, og disse dekker områdene ansvar, nærhet, likhet og samvirke.[85]

I en operasjon med flere aktører er det gjerne et stort behov for informasjonsutveksling for å koordinere innsatsen samt etablere og vedlikeholde et felles situasjonsbilde, og dermed muliggjøre tilstrekkelig samvirke. Under Viking Sky-hendelsen var nettopp etableringen av et felles situasjonsbilde en utfordring på grunn av utilstrekkelig informasjonsutveksling. I evalueringsrapporten trekkes det at de ulike aktørene hadde ulike kommunikasjonssystemer frem som en viktig årsak til dette. Mange av aktørene hadde riktignok tilgang til Nødnett[86], og ved å formidle informasjon i form av tale, kunne disse bidra til bygging av et felles situasjonsbilde. I etterkant av redningsaksjonen tok flere av de involverte til orde for at flere aktører innen redning og beredskap burde få tilgang til Nødnett for å sikre bedre samhandling.[87]

Dagens Nødnett er imidlertid primært et talesamband, og det har svært begrenset kapasitet for overføring av data.[88] I Viking Sky-eksempelet betød dette at situasjonsbildet som ble bygget ikke kunne deles over Nødnettet annet enn i muntlig form. Årsaken til at talesamband alene ikke er tilstrekkelig er at ulike aktører i totalforsvaret benytter ulike informasjonssystemer. FFI har tidligere vist at det er en rekke såkalte «silo-utfordringer» mellom de ulike statlige aktørene i totalforsvaret, og dette er med på å vanskeliggjøre informasjonsdeling.[89] Evalueringsrapporten etter Gjerdrum-skredet trekker frem at aktørene i innsatsområdet ikke hadde tilstrekkelige og egnede digitale verktøy for samhandling, og i tillegg hadde aktørene informasjonssystemer som i liten grad kommuniserte med andre aktørers informasjonssystemer.[90]

Mange organisasjoner, herunder aktører i totalforsvaret, vil normalt kjøre sine informasjonssystemer på et «lukket nettverk»[91] som bare organisasjonens ansatte har tilgang til. Et slikt nettverk kan være fullstendig isolert eller det kan være koplet mot internett (normalt med en form for innloggingsmekanisme). Dersom flere totalforsvarsaktører skal samarbeide og utveksle data i dag, vil dette i de fleste tilfeller måtte skje over internett, noe som innebærer at dataene må beskyttes mot uautorisert innsyn. Hvor god denne beskyttelsen er, avhenger av sikkerhetsmekanismene som benyttes under overføringen. Eksempelvis er vanlig e-post ikke ende-til-ende-kryptert, med mindre sender og mottaker benytter samme e-postleverandør. Beskyttelsesmekanismer som såkalte VPN-tunneler (*Virtual Private Network*) kan gi langt bedre beskyttelse, men forutsetter at aktørene blir enige om hvilken standard eller produkt som skal brukes.

[85] Justis- og beredskapsdepartementet. (2020). Meld. St. 5 (2020–2021). Samfunnssikkerhet i en usikker verden.
[86] Nødnett er et kommunikasjonssystem for nød- og beredskapsaktører i Norge. Nødnett eies og forvaltes av Direktoratet for samfunnssikkerhet og beredskap (DSB).
[87] Direktoratet for samfunnssikkerhet og beredskap (2020a).
[88] Mykkeltveit, Anders og Anne Pernille Hveem (2021): Forsvarssektorens mulige tilnærminger til fremtidig løsning for nød- og beredskapskommunikasjon. FFI-rapport 21/00379. Unntatt offentlighet.
[89] Endregard, Monica mfl. (2019). Vurdering av Trident Juncture 2018. FFI-rapport 19/01791. BEGRENSET.
[90] Hovedredningssentralen (2021): EVALUERING – Redningsaksjonen og den akutte krisehåndteringen under kvikkleireskredet på Gjerdrum. Rapport til Justis- og beredskapsdepartementet 1. juni 2021.
[91] Ofte kalt intranett.

Utfordringen er altså at aktørene som skal utveksle informasjon må bli enige både om hvilke formater som skal benyttes, og hvordan dataene skal beskyttes.

Flere av informasjonssystemene Forsvaret benytter er underlagt strenge sikkerhetskrav og mulighetene for sammenkopling med andre aktørers verktøy er svært begrenset. I praksis er derfor toveis datautveksling mellom informasjonssystemene til Forsvaret og til øvrige totalforsvarsaktører ofte ikke mulig. Man er i stedet avhengig av å ha alle aktørene på et felles nettverk, som tilfredsstiller nødvendige sikkerhetskrav. Nasjonalt BEGRENSET nett (NBN) er et eksempel på et slikt nettverk.[92]

3.2.1 Distribuert skyteknologi og 5G for bedre samvirke i totalforsvaret

I en operasjon som involverer totalforsvaret (heretter kalt et totalforsvarsoppdrag), kan aktørene etablere et oppdragsspesifikt nettverk ved hjelp av skyteknologi og 5G. Et slik oppdragsspesifikt nettverk vil være et virtuelt nettverk som er tilgjengelig for deltakende aktører. Sett fra brukernes synspunkt har dette mange likhetstrekk med et lukket, organisasjonsinternt nettverk som beskrevet i kapittel 3.2. Et slikt nettverk kan inkludere både tjenester fra de store leverandørene av skytjenester og informasjonssystemer for den enkelte totalforsvarsaktør. Fordi alt er virtuelt kan de samme fysiske datamaskinene og nettverkene benyttes for alle de oppdragsspesifikke nettverkene. Tilgang skjer fra PC-er (med sikker innlogging) og fra mobiltelefoner.

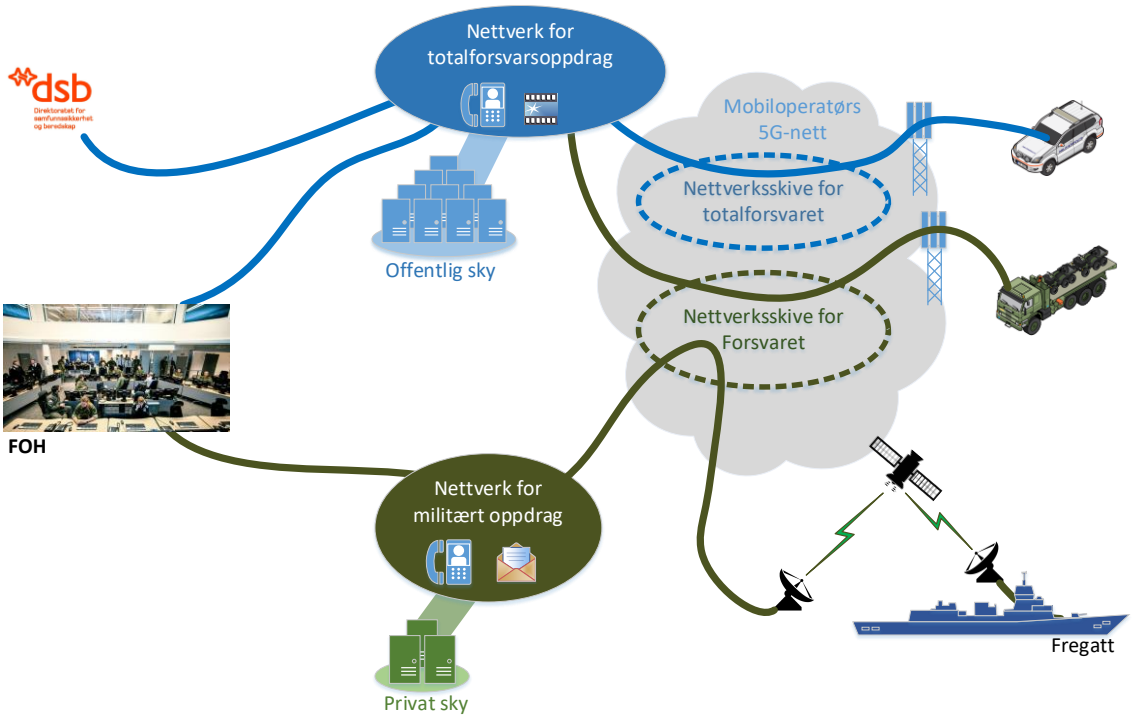
Fremtiden til dagens Nødnett er uavklart per i dag, ettersom drifts- og vedlikeholdsavtalen går ut i 2026 (kan forlenges med ytterligere fem år ved behov).[93] Regjeringen åpnet i 2017 for at fremtidige kommunikasjonsløsninger for nød- og beredskapsetater og Forsvaret vil kunne leveres av kommersielle mobiltilbydere.[94] Arbeid med nytt Nødnett er igangsatt, og en konseptvalgutredning er gjennomført.[95] Dersom et nytt Nødnett baseres på 5G og bruk av skivedeling, vil man få tilsvarende fordeler med god dekning gjennom bruk av de offentlige mobilnettene og mulighet for tilgang med vanlige mobiltelefoner. I tillegg vil den samme mobilinfrastrukturen kunne brukes både til Nødnett og til oppdragsspesifikke nettverk, og de kan knyttes sammen ved behov. Et slikt oppdragsspesifikt nettverk vil dermed utgjøre et eget selvstendig nettverk med høyhastighetskommunikasjon, mobiltilgang og med alle nødvendige applikasjoner tilgjengelig der Forsvarets personell som deltar i totalforsvarsoppdraget kan benytte en egen nettverksskive som vi diskuterte i kapittel 3.1.1.

I kapittel 2.2 beskrev vi også teknologi som gjør det mulig å automatisk etablere hele nettverk med alle nødvendige applikasjoner. I evalueringsrapporten etter redningsaksjonen på Gjerdrum sies det: «*Når en katastrofe inntreffer vil man forholde seg til en lang rekke forhåndsplanlagte tiltak i tillegg til at enkelte elementer må improviseres og tilpasses den aktuelle, konkrete situasjon. Digitale verktøy for å lette redningsinnsatsen bør ikke improviseres. Slike verktøy må utvikles eller anskaffes i forkant av redningshendelser og de som skal bruke verktøyene må ha*

[92] Forsvarsdepartementet (2020c).
[93] Mykkeltveit, Anders mfl. (2021).
[94] Samferdselsdepartementet (2017): Mer båndbredde for bedre mobile tjenester. Pressemelding nr. 212/17.
[95] Direktoratet for samfunnssikkerhet og beredskap (2020b): KVU for fremtidig løsning.

god kompetanse på disse.».[96] Med løsningen skissert her kan formaliserte beskrivelser for en rekke ulike scenarioer og med ulike deltakende totalforsvarsaktører lages på forhånd, og passende nettverk og informasjonssystemer kan etableres raskt og automatisk ved behov.

Dersom operasjonen foregår i et område med dårlig dekning eller de offentlige basestasjonene i området er ute av drift, kan det suppleres med egne, mobile basestasjoner. De transportable basestasjonene koples enten direkte mot fast infrastruktur (for eksempel optisk fiber), der dette er tilgjengelig, eller man benytter satellittkommunikasjon mellom basestasjonene og resten av nettverket. Med slike mobile basestasjoner og langtrekkende høyhastighets radiokommunikasjon kan man også sikre dekning i de tilfeller hvor eksisterende offentlig infrastruktur bryter sammen, som man eksempelvis så i forbindelse med brannen i Lærdal i 2014.[97]



Figur 3.3 Bruk av 5G-skivedeling for å lage oppdragsspesifikke nettverk.

I figur 3.2 illustrerte vi hvordan Forsvaret kan utnytte skivedeling i 5G-nettverk for å skille Forsvarets interne datatrafikk under en operasjon fra andre brukeres datatrafikk i det samme mobilnettet. Det kan opprettes kontrollert tilgang til det oppdragsspesifikke nettverket fra Forsvarets nettverksskive. Figur 3.3 viser et eksempel hvor det er opprettet et oppdragsspesifikt nettverk for en totalforsvarsoperasjon indikert med en blå ellipse. Denne operasjonen inkluderer DSB og Forsvarets operative hovedkvarter (FOH), og det benyttes skytjenester fra et sentralt datasenter. For mobilkommunikasjon benyttes her kun offentlige mobilnett. Forsvarets egne tjenester (illustrert med grønn ellipse) er adskilt fra totalforsvarsoperasjonen. I figuren er

[96] Hovedredningssentralen (2021).
[97] Direktoratet for samfunnssikkerhet og beredskap (2014): Brannene i Lærdal, Flatanger og på Frøya vinteren 2014. Rapport.

Forsvares nettverksskive også koplet mot en satellittlink for å kommunisere med en fregatt. I dette eksemplet deltar altså FOH i to parallelle operasjoner, men fordi disse operasjonene benytter to separate nettverk kan den forsvarsinterne datatrafikken holdes adskilt fra datatrafikken til total-forsvarsaktørene.

Forsvaret trenger dermed ikke å slippe sivile aktører inn i sine nettverk, eller kople egne nettverk sammen med sivile aktørers nettverk. Da de oppdragsspesifikke nettverkene er basert på moderne prinsipper for virtualisering, kan de i prinsippet enkelt gjøres tilgjengelig i Forsvarets hoved-kvarter, uten at det må gjøres fysiske koplinger eller at det må installeres maskin- eller program-vare. Ved behov kan informasjon likevel slippes inn på Forsvarets nettverk gjennom såkalte diodeløsninger[98]. På sikt kan kanskje løsninger for sikker informasjonsutveksling gjøre det mulig å overføre informasjon også den andre veien, men i dag er muligheten svært begrenset.[99] [100]

3.3 Mobilitet og hurtighet i militære operasjoner

Forsvarets operative evne er under kontinuerlig utvikling, og det samme er faktorer og utfordringer som påvirker den utenfra. Langtrekkende presisjonsvåpen er i dag et av de viktigste forholdene som påvirker den videre utviklingen av Forsvaret.[101] Fremveksten av hypersoniske våpen medfører nye trusler mot norsk sikkerhet[102] og vil trolig forsterke denne utviklingen. Utviklingen av ny teknologi fører også til at operasjonstempoet øker.[103]

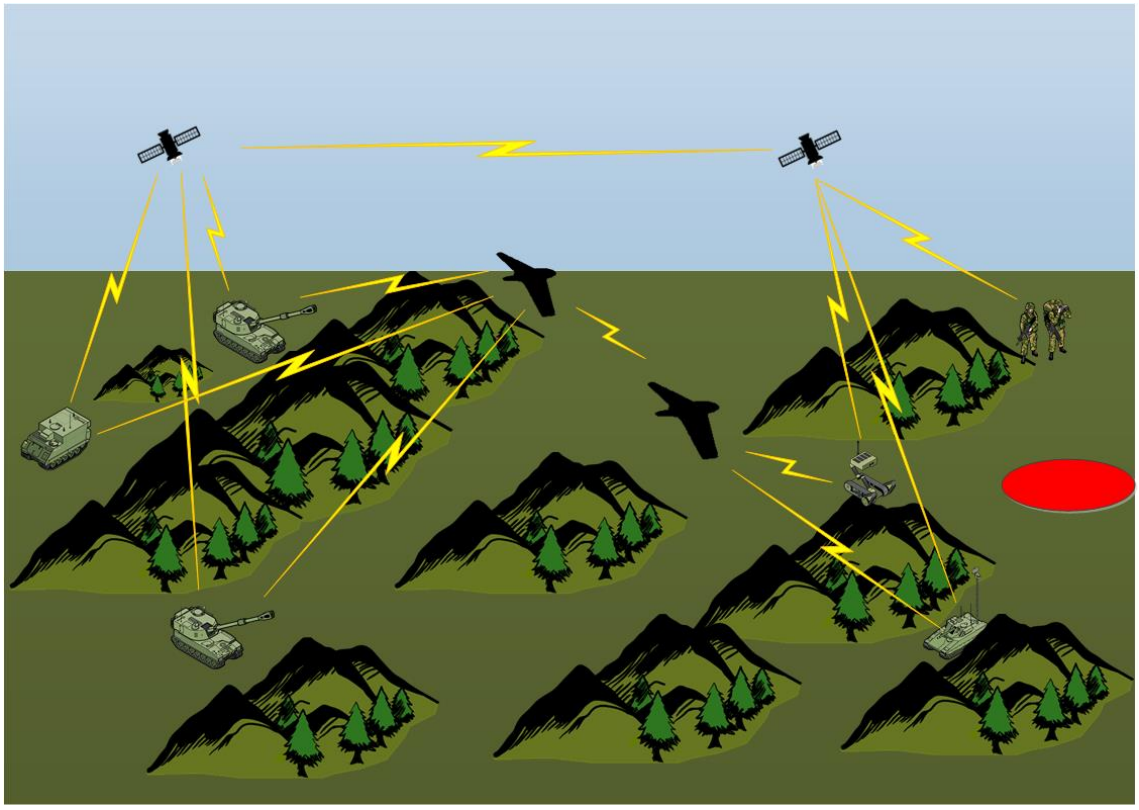
Tiltak som kan redusere sårbarheten for trusler fra langtrekkende presisjonsvåpen, er spredning og mobilitet, samt minst mulig bruk av fast infrastruktur.[104] For å opprettholde samvirke mellom spredte enheter som er i bevegelse, i et operasjonsmiljø preget av elektronisk krigføring, trengs det robuste kommunikasjonsløsninger. For å opprettholde operativ evne i tråd med operasjons-konseptet må disse kommunikasjonsløsningene også tilby tilstrekkelig overføringshastighet slik at for eksempel sensor og skytter ikke trenger å være i nærheten av hverandre når det overføres store datamengder mellom disse. Dette er noen av grunnene til at høyhastighetskommunikasjon mellom enheter i bevegelse er et operativt effektmål i virksomhetsprogrammet Mime.[105] [106]

I dag er høyhastighetskommunikasjon tilgjengelig bare til store plattformer, som for eksempel fregatter og dedikerte kommunikasjonsnoder, og faste installasjoner. Mindre enheter, som mindre kjøretøy og soldater, kommuniserer ved hjelp av radioer med begrenset overføringshastighet. Slike radioer har typisk en maksimal rekkevidde på noen titalls kilometer og er i varierende grad sårbare for elektronisk krigføring. Begrensninger på rekkevidde og overføringshastighet fører til

[98] En diode er i denne sammenhengen en mekanisme som koples mellom to datanettverk, og som bare tillater over-føring av data én vei. Man kan dermed sende data fra et ugradert nettverk inn på et gradert nettverk, mens det er umulig å sende data den andre veien.
[99] Nordbotten, Nils Agne mfl. (2015): Information sharing across security domains, FFI-rapport 15/00456.
[100] Haakseth, Raymond mfl. (2017): Cross-domain communication using an XMPP chat guard, FFI-rapport 17/01491.
[101] Forsvarsdepartementet (2020a).
[102] Ibid.
[103] Forsvarets forskningsinstitutt (2021): Utsyn, Forskings- og utviklingsplan 2021–2024, del 1.
[104] United States Marine Corps (2020): Force Design 2030.
[105] Program Mime skal modernisere IKT-systemene for taktisk ledelse i Forsvaret i perioden frem til 2030.
[106] Forsvaret (2020): Effektrealiseringsplan, Program Mime.

at noen enheter enten må være mindre mobile eller tvinges til å operere nærmere hverandre enn ønskelig. Kommandoplasser må ofte følges av dedikerte kommunikasjonsnoder. Slike kommunikasjonsnoder krever fysisk beskyttelse og kan begrense mobiliteten til kommando-plassene.

Som beskrevet i kapittel 2.4, blir kommunikasjon ved hjelp av satellitt og UAV-relé langt mer tilgjengelig, med mindre og billigere terminaler, større kapasitet og økt robusthet i løsninger.



Figur 3.4 Langtrekkende ild. Ulike enheter/sensorer på ulike steder formidler informasjon om mål (rød sirkel) ved hjelp av satellitter og UAV-er. Linjene mellom de ulike enhetene symboliserer kommunikasjon.

3.3.1 Langtrekkende ild

I en militær operasjon vil det kunne være behov for å beskyte mål på stor avstand. For å få tilstrekkelig informasjon om slike mål vil det være behov for å ha ulike typer enheter eller sensorer nærme målet. Det kan imidlertid være utfordrende både å få plassert enheter og sensorer i nær-heten av målet og å få overført informasjonen tilbake til beslutningstaker og våpen når avstanden fra beslutningstaker og våpen til sensorer og fremskutte enheter øker. Ved å benytte høykapasitets satellittkommunikasjon eller UAV-relé, kan man i prinsippet kommunisere uavhengig av avstand mellom sensorer/observatører og mottakere av informasjon, og også uavhengig av om noen av

disse er stasjonære eller i bevegelse. I prinsippet kan både beslutningstakere og våpenplattformer være virkårlig spredt, begrenset kun av rekkevidden til våpen og andre operative hensyn.

Figur 3.4 illustrerer en mulig situasjon der informasjon om mål (rød sirkel) formidles fra bemannede kjøretøy, en ubemannet bakkefarkost (UGV) eller fra soldatpatruljer via satellitter og UAV-reléer. Terminalene som sender disse dataene er små i størrelse, størrelsesorden 20x20 cm og 4 kg. I tilfeller der den samme satellitten eller UAV-en ikke er synlig både for senderen og den som skal motta informasjonen kan Forsvaret benytte flere satellitter og/eller UAV-er som kommuniserer seg imellom. I en UAV-basert løsning kan det være en fordel å benytte en UAV i litt større høyde og lengre unna målet som et relé for andre UAV-er som er nærmere.

Det er, som beskrevet i kapittel 2.4, fullt mulig å lage robuste systemer som består av flere komponenter (satellitter og/eller UAV-er), hvor tap av, eller feil i, noen få komponenter ikke påvirker ytelsen. Ved å benytte direktive og ikke-statiske kommunikasjonslinker[107] på høye frekvenser kan man lage løsninger med god beskyttelse mot elektronisk krigføring.

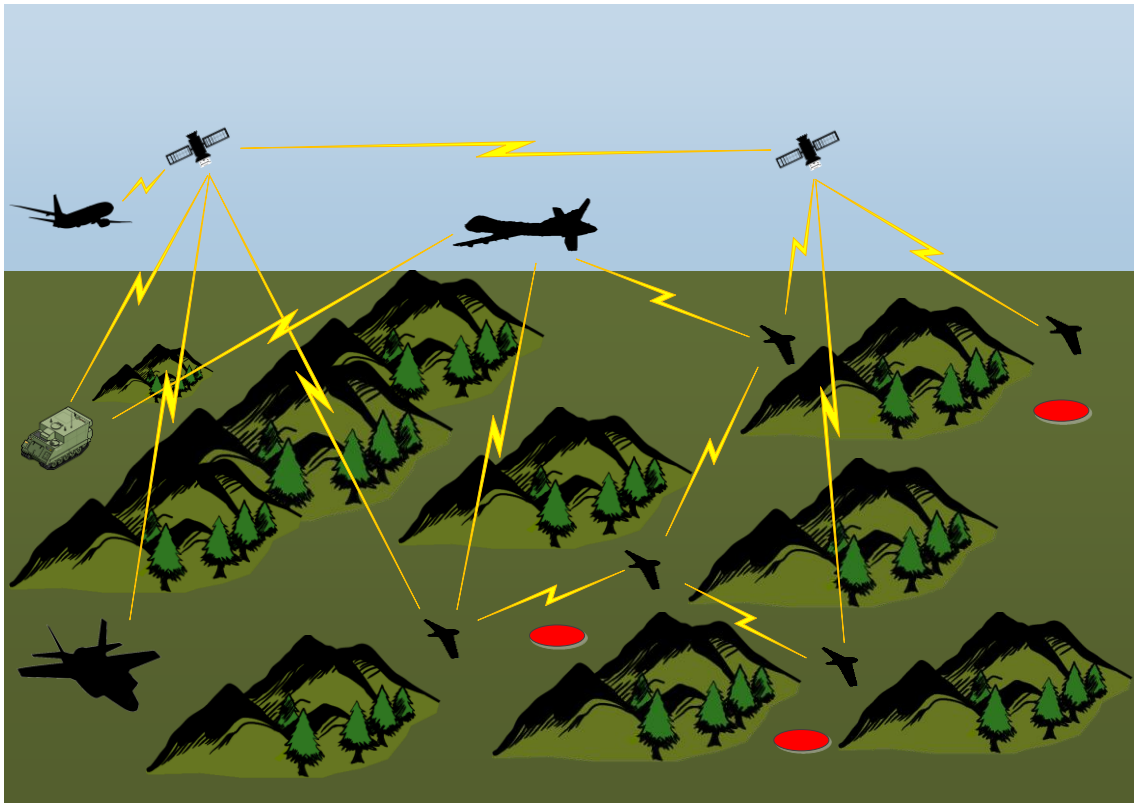
3.3.2 Rekognosering

For å få detaljert situasjonsforståelse over et større område og identifisere uønsket aktivitet eller mulige militære mål kreves det ofte detaljerte observasjoner fra kort avstand. I tilfeller hvor området av interesse er stort, er det vanskelig å dekke dette med bakkebaserte sensorer. I stedet kan man bruke et større antall mindre UAV-er, for eksempel billige fixed-wing UAV-er. Som beskrevet i kapittel 2.4, er det en trend å bruke billigere UAV-er også i militære sammenhenger. Disse kan med fordel kombineres med mindre kommunikasjonsterminaler som bruker høye frekvenser mot enten satellitt eller UAV.

I figur 3.5 ser vi at satellitter og én UAV i stor høyde sørger for kommunikasjon mellom lavtflygende UAV-er. Posisjonering av den enkelte UAV er derfor ikke begrenset av rekkevidden til kommunikasjonssystemene samtidig som de kan fly lavt for å unngå å bli oppdaget og for å kunne utføre rekognoseringen. Kommunikasjonsløsningen brukes også til å samarbeide med andre luftplattformer (F-35 kampfly og P-8 maritimt patruljefly er illustrert) og for å overføre informasjon til en mobil kommandovogn. Som i eksempelet med langtrekkende ild, er robusthet viktig. Robusthet mot elektronisk krigføring ivaretas ved bruk av elektronisk styrte svært direktive antenner som bruker høye frekvenser eller optisk kommunikasjon.

Bruken vi beskriver her er basert på et scenario beskrevet av RAND,[108] men en viktig forskjell at over terreng må UAV-er fly lavt både på grunn av begrenset deteksjonsevne på sensorene og for å unngå luftvern. Lav flyhøyde begrenser frisikt, og dermed muligheten for å kommunisere, mellom UAV-er, mellom UAV-er og andre flyvende plattformer og mellom UAV-er og bakkebasert infrastruktur.

[107] Med kommunikasjonslink menes her radiokommunikasjon eller optisk kommunikasjon. En direktiv kommunikasjonslink sender signalet bare i en ønsket (smal) retning. En ikke-statisk kommunikasjonslink forandrer retningen over tid, for eksempel til satellitt som er i bevegelse i forhold til overflaten.
[108] Hamilton, Thomas mfl. (2019).



Figur 3.5 Lavtflygende UAV-er brukes til rekognosering. UAV-er kommuniserer med hverandre og leverer informasjon til kommandovogn, kampfly og maritimt patruljefly ved hjelp av andre UAV-er eller satellitter. Røde sirkler indikerer områder av interesse.

3.4 Utnyttelse av sensordata

I planlegging og gjennomføring av militære operasjoner er Forsvaret avhengige av god forståelse av omgivelser og status på egne og fiendtlige styrker. Denne forståelsen bygges på ulike informasjonskilder som etterretningsrapporter og de mange sensorene som Forsvaret har til rådighet. Forsvarets sensorer inkluderer alt fra den enkelte soldats observasjoner til radarer og avanserte systemer som Natos Allied Ground Surveillance (AGS), og de ulike sensorene leverer data i ulike formater, herunder dokumenter, bilder, videoer, radar- og sonarmålinger.

Det er forventet at situasjonsforståelsen til beslutningstakere i Forsvaret kan bedres ved at data fra mange kilder sammenstilles i større grad enn i dag.[109] Økt sammenstilling av data vil imidlertid føre til at disse systemene må kunne håndtere større mengder data enn i dag, noe som forsterkes av at nye kapabiliteter som F-35 kampfly, Nato AGS og nye overvåkningsfly er ventet å kunne bidra med store mengder sensordata.

[109] Forsvarsdepartementet (2016).

Forsvaret ønsker å øke sin evne til å håndtere økt informasjonsvolum og i større grad utnytte automatiserte beslutningsstøttesystemer for sammenstilling og analyse av data fra flere kilder.[110] I det følgende vil vi beskrive to eksempler der vi mener at bruk av ny IKT kan bedre Forsvarets utnyttelse av data, basert på utviklingen innen automatisert analyse av informasjon som beskrevet i kapittel 2.1.

3.4.1 Avansert bildeprosessering – bedre utnyttelse av radardata

AGS er en fellesressurs i Nato som består av fem UAV-er av typen Global Hawk som opererer ut fra sin hovedbase i Italia. AGS vil kunne dekke store områder på kort tid og forventes å samle inn enorme mengder informasjon som skal lagres sentralt av Nato.[111]

UAV-ene er utstyrt med radarene SAR (Syntetisk apertur-radar) og (*ground*) MTI (*Moving Target Indicator*), og data fra disse sensorene overføres til bakkestasjonen i Italia for prosessering. AGS-systemet består også av et antall bakkestasjoner som kan plasseres der det er behov, og som gjør det mulig å hente ned og tolke data andre steder enn ved hovedbasen.[112] Ved behov kan Forsvaret motta AGS-informasjon fra en av disse bakkestasjonene.

SAR-bilder er et viktig produkt fra AGS. SAR er en bildedannende radar, men tolking av disse bildene for å trekke ut den essensielle informasjonen er i dag en tidkrevende, manuell prosess som krever personell med høy kompetanse.[113] Den manuelle prosessen gjør at det kan ta lang tid å identifisere relevante objekter i SAR-bildene, og at informasjonen i SAR-bildet ikke kommer til beslutningstakere i tide til å støtte viktige beslutninger. Dette kan for eksempel være tilfelle i situasjoner der fiendtlige styrker manøvrerer i høyt tempo for å gjøre det vanskelig for motstanderen å holde oversikt over styrkene deres.

Ved hjelp av maskinlæring kan man trene opp modeller som kan brukes til automatisert analyse av SAR-bilder på tilsvarende måte som man i dag støtter medisinsk personell med diagnose på bakgrunn av bilder.[114] Dette vil kunne øke kapasiteten til behandling av SAR-bilder, både ved AGS' hovedbase og ved de utplasserte bakkestasjonene, noe som kan utnyttes til å få raskere analysesvar. Dette kan også gjøre at man kan behandle en større mengder SAR-bilder og dermed potensielt bidra til en høyere kvalitet på analyseproduktene.

Automatisert analyse av SAR-bilder vil med andre ord kunne gjøre viktig informasjon tilgjengelig for beslutningstakere i Forsvaret hurtigere og dermed potensielt øke nytten av informasjonen.

[110] Ibid.
[111] NATO (2021): Allied Ground Surveillance (AGS).
[112] Ibid.
[113] Bhamidipati, Sai mfl. (2020): Generation of SAR Images Using Deep Learning. SN Computer Science. Vol. 1. No. 6. Springer.
[114] Ibid.

3.4.2 Automatisert tekstprosessering – tolking av skriftlig informasjon

Rapporter i tekstformat er også en viktig kilde til informasjon for militære beslutningstakere. Dette kan for eksempel være situasjonsrapporter fra egne styrker, observasjoner rapportert av eget personell og etterretningsrapporter om fiendens mulige handlemåter. For å dra nytte av informasjonen i slike skriftlige rapporter, må de imidlertid leses av beslutningstaker eller dennes stab, og dette er tidkrevende.

Når informasjonen som trekkes ut av slike rapporter skal deles videre i dag, skjer dette i hovedsak i form av nye rapporter. For å kunne utnyttes i neste ledd må de da igjen leses manuelt, og tiden det tar å nyttiggjøre seg av informasjonen som ble pakket inn i en rapport i første omgang går ytterligere opp. En effekt av dette er at beslutningstakere risikerer å gå glipp av viktig informasjon fordi man ikke har rukket å frembringe informasjonen i tide til at den kan tas i betraktning i beslutningsprosessen.

Denne utfordringen kan bøtes på med automatisert tekstprosessering som kan bistå med å trekke ut viktig informasjon fra rapportene og omdanne dette til en strukturert form. Ved å omdanne den ustrukturerte teksten til en strukturert form, kan man legge til rette for automatisert deling og gjenbruk av data.[115] Dette vil kunne øke mengden data som kan overbringes til beslutningstakere i tide til å kunne tas i betraktning når avgjørelser skal tas.

4 Vurderinger – hva bør Forsvaret gjøre?

I dette kapittelet vurderer vi mulige gevinster og utfordringer, herunder risikoer og kostnader, ved de fire tilnærmingene som er beskrevet i kapittel 3. Ut fra de identifiserte gevinstene og utfordringene, utledes anbefalinger til Forsvaret. Vi understreker at denne rapporten har fokusert på teknologi og teknologiske muligheter og at rapporten kun har studert utvalgte teknologiområder og mulig bruk av disse i Forsvaret. Anbefalingene i rapporten bør leses i denne konteksten.

4.1 Effektiv og sikker IKT-infrastruktur

I kapittel 3.1 presenterte vi hvordan skyteknologi og 5G kan benyttes for å gjøre IKT-infrastrukturen Forsvaret bruker under sine operasjoner effektiv og sikker. Her diskuterer vi mulige gevinster og utfordringer og gir anbefalinger.

[115] Halvorsen, Jonas og Bjørn Jervell Hansen (2020): Exploring data reuse using a big data infrastructure. FFI-rapport 20/02840.

4.1.1 Mulige gevinster

Til sammen kan bruk av skyteknologi, langtrekkende kommunikasjonsløsninger og 5G i infrastrukturen gi Forsvaret større fleksibilitet i hvordan IKT kan benyttes i operasjoner, og dermed i Forsvarets operasjonsmønster.

Med skyteknologi kan applikasjoner gjøres tilgjengelige uavhengig av hvor brukeren er, og samtidig løpende tilpasses de operative behovene. Både 5G og satellittkommunikasjon gir gevinst gjennom å muliggjøre høye overføringshastigheter, og dermed god samhandling. 5G har god dekning på land, mens satellittkommunikasjon kan tilby dekning «overalt». 5G gir mulighet for sikrere og mer robust kommunikasjon enn tidligere generasjoner mobilteknologi.

Å ta i bruk skyteknologi og 5G i IKT-infrastrukturen til Forsvaret vil kunne påvirke det økonomiske bildet. Bruk av offentlig sky vil dreie kostnader fra investeringer i maskinvare mot løpende driftskostnader,[116] mens bruk av privat sky kan bidra til besparelser gjennom mer effektiv utnyttelse av maskinvare og gi mulighet for sentralisert styring og kontroll av IKT-infrastrukturen. Sentralisert styring og kontroll kan i tillegg gi økonomiske gevinster i form av redusert behov for personell, spesielt personell i felt. 5G er en kommersiell teknologi som kan gi billigere løsninger enn spesialiserte militære løsninger siden utstyr masseproduseres for et stort marked.

4.1.2 Utfordringer

Skyteknologi fra store leverandører har ofte god sikkerhet, men Forsvaret har en del krav til sikkerhet for graderte informasjonssystemer som er utfordrende å møte ved bruk av skytjenester.[117] Nasjonal sikkerhetsmyndighet (NSM) undersøker for tiden muligheter nye teknologier som skytjenester gir offentlig sektor med fokus på å finne sikre anvendelser.[118] Vi har i kapittel 3.1 foreslått å benytte private skyer[119] både ute i de mobile enhetene og i den stasjonære infrastrukturen. Dette kan gjøre det enklere å benytte skyteknologien, samtidig som det vil kunne gjøre løsningene dyrere enn offentlige skyer siden maskinvaren er reservert for én bruker, nemlig Forsvaret.

For å dra full nytte av skyteknologien må Forsvarets applikasjoner være utformet på en slik måte at de kan fungere optimalt som skytjenester. Dette kalles cloud native (se kapittel 2.2.1) og innebærer at applikasjonene raskt og automatisk kan tilpasses varierende etterspørsel og belastning. Det vil sannsynligvis være enkelt å utvikle nye applikasjoner slik at disse er forberedt for bruk som skytjenester da denne teknologien begynner å bli moden, mens det kan være mer omfattende å skrive om eksisterende applikasjoner slik at de blir cloud native. Vi anbefaler likevel at Forsvaret tar i bruk cloud native så mye som mulig, da det uansett gir gevinster i form av automatisk tilpasning til belastning, bedre utnyttelse av maskinvare og at det blir enklere å legge

[116] Lund, Ketil mfl. (2021).
[117] Ibid.
[118] Nasjonal sikkerhetsmyndighet (2020): Muligheter for en moderne IT-plattform». Dokument-id VIRT-1902-NO.
[119] Se kapittel 2.2.1.

til ny funksjonalitet i applikasjonene. Nato har allerede i flere år jobbet mot dette gjennom prosjektet IT Modernization.[120]

I kapittel 3.1 beskrev vi hvordan skyteknologi kan gjøre tjenester tilgjengelig for brukerne uavhengig av hvor de befinner seg. Dette forutsetter at Forsvaret lykkes i å kontrollere hvor dataene befinner seg og at dataene er replikert så de ikke går tapt om maskinvare på én lokasjon skulle bli ødelagt. Kapittel 3.1 beskriver også hvordan edge computing kan benyttes sammen med 5G-nettene til å sikre at tjenester kjøres fra lokale datasentre for å bedre robusthet. Dette er muligheter som teknologien åpner for, men som vi diskuterte avslutningsvis i kapittel 2.3.2, er det behov for et stort nok marked for at en gitt type tjenester skal bli gjort tilgjengelig.

Innføringen av skyteknologi vil føre til større behov for løsninger for styring og kontroll av infrastrukturen. Dette vil medføre kostnader i anskaffelse, tilpasning og drift. Løsningene er omfattende, kompliserte og i kontinuerlig utvikling. Personellet som skal drifte og videreutvikle IKT-løsningene sentralt, vil derfor typisk ha behov for spisskompetanse og kan dermed være vanskeligere å få tak i og beholde.

4.1.3 Anbefalinger

Vi mener at skyteknologi kan spille en viktig rolle i Forsvaret[121], også i militære operasjoner, men at Forsvaret ikke kun kan benytte seg av offentlig sky. Det må i tillegg etableres løsninger med egne datasentre som leverer skytjenester nærmere brukerne.

Vi anbefaler at Forsvaret iverksetter systematisk testing av skyteknologi i felt. Det er sentralt å finne løsninger som både fungerer autonomt når det er nødvendig, og som også fungerer sømløst sammen med sentrale skytjenester når det er mulig. Det må undersøkes om kommersielt tilgjengelige løsninger fra de større leverandørene kan benyttes, eller om det er behov for mer spesialiserte løsninger. Det må også undersøkes om systemer for styring og kontroll er fleksible nok til raskt og effektivt å kunne endre på hvilke applikasjoner som skal kjøres hvor.

For å få til en overgang til skytjenester må Forsvaret utforme en strategi for hvordan Forsvaret skal utnytte slike tjenester. Denne strategien må forankres i alle deler av forsvarssektoren, og må formidles tydelig til relevante eksterne aktører, som teleoperatører og leverandører av skytjenester og applikasjoner. For å forenkle fremtidig overgang til bruk av skytjenester og -teknologi, anbefaler vi at nye applikasjoner som skal benyttes i Forsvaret, gjøres cloud native[122].

Når det gjelder å bruke 5G i kombinasjon med nettverksskiver er ikke teknologien i dag helt moden. EU-prosjektene 5G-VINNI og FUDGE-5G er viktige arenaer for utforsking av 5G, men for at Forsvaret skal klare å utnytte mulighetene 5G gir trengs det også tydelige føringer fra toppen

[120] NCI Agency (2017): NATO signs milestone contract for IT modernization.
[121] Dette er også Forsvarets eget syn, og programmet MAST (Militær anvendelse av skytjenester) er opprettet for å starte arbeidet med å ta i bruk skytjenester i Forsvaret.
[122] Cloud native innebærer at applikasjoner består av en rekke selvstendige mikrotjenester som samarbeider. Dette gjør at applikasjoner raskt og automatisk kan tilpasses varierende bruksmønster og belastning.

av organisasjonen på at dette skal satses på, kanskje etter modell fra USAs 5G-strategi[123] og tilhørende implementeringsplan[124]. For å få realisert 5G og edge computing bør Forsvaret undersøke om det finnes behov i privat og offentlig sektor som sammen med Forsvarets behov kan skape et velfungerende marked for dette i Norge. Ett eksempel på slike behov er fremtidig Nødnett som er ventet realisert i mobilnettene.[125] Forsvaret kan også undersøke om kommunene eller helsesektoren har interesse av å oppnå bedre robusthet gjennom utnyttelse av edge computing.

4.2 Samvirke i totalforsvaret

I kapittel 3.2 viste vi hvordan 5G og skyteknologi kan benyttes for å møte en del av samvirkeutfordringene i totalforsvaret. Den skisserte løsningen bygger på at alle aktørene som er med i et totalforsvarsoppdrag samles i et oppdragsspesifikt nettverk. Her diskuterer vi mulige gevinster og utfordringer og gir anbefalinger.

4.2.1 Mulige gevinster

Ved en hendelse kan et komplett nettverk med nødvendige informasjonssystemer for alle involverte aktører opprettes svært raskt, ettersom prosedyrer, ansvar og alle nødvendige IKT-tjenester og nettverkssammenkoplinger er forberedt på forhånd. Dette har flere viktige fordeler. For det første kan samarbeidet på høyere nivå mellom aktørene (dvs. utenfor selve innsatsstedet) komme raskere i gang med operasjonen, fordi evnen til samvirke er på plass svært raskt. For det andre vil det å ha et felles, dedikert nettverk der all informasjon relatert til hendelsen kan gjøres tilgjengelig, legge til rette for god situasjonsforståelse hos alle deltakende aktører.

Informasjonen knyttet til operasjonen vil også være godt beskyttet fordi nettverket er lukket og kun tilgjengelig for aktørene. For Forsvarets del er det også fordelaktig at nettverket kan holdes adskilt fra deres operative nettverk, ettersom disse er høyt gradert, og derfor i svært liten grad kan koples sammen med andre nettverk.

Ved bruk av offentlige mobilnett samt egne mobile basestasjoner kombinert med satellittkommunikasjon sikres høy tilgjengelighet for det oppdragsspesifikke nettverket. Dette forsterkes av at man til en viss grad vil kunne bruke vanlige mobiltelefoner, i stedet for dedikerte terminaler som i dagens Nødnett, noe som kan redusere behovet for å anskaffe terminaler.

Bruk av offentlige basestasjoner bidrar også til at oppgaver knyttet til vedlikehold av infrastrukturen enklere kan overlates til en kommersiell aktør.[126] Dette kan bidra til å redusere driftskostnadene for infrastrukturen, samtidig som det å basere seg på bruk av eksisterende kommersiell infrastruktur kan gi svært god kapasitet og dekning.

[123] United States Department of Defense (2020): Department of Defense (DoD) 5G Strategy (U).
[124] United States Department of Defense (2020): Department of Defense 5G Strategy Implementation Plan.
[125] Samferdselsdepartementet (2017).
[126] I dagens Nødnett er det Justis- og beredskapsdepartementet som har dette ansvaret.

4.2.2 Utfordringer

Bruk av oppdragsspesifikke, lukkede nettverk som skissert i kapittel 3.2, er delvis basert på teknologi som per i dag ikke er i utstrakt bruk. Dette medfører noen usikkerheter og mulige utfordringer. Skivedeling i 5G-nettet er per i dag ikke tilgjengelig, og man er avhengig av at de store teleoperatørene ser et kommersielt grunnlag for å tilby slike tjenester til eksterne kunder. Myndighetene må tidlig signalisere overfor teleoperatørene at slik funksjonalitet er ønskelig i fremtiden (se også kapittel 2.3) for å motivere operatørene til å tilby slik funksjonalitet. Det er også et alternativ at offentlig sektor går inn og bidrar finansielt for at operatørene skal satse. Det er svært usikkert hva kostnadsnivået vil være for en slik finansiering, men sannsynligvis er det snakk om en investering av et slik omfang at den bør vurderes gjort på tvers av ulike sektorer.

Som nevnt tidligere bør det legges opp til å ha et sett av forhåndsdefinerte oppsett, tilpasset ulike oppdrag. Alle oppdrag er imidlertid unike, så nøyaktig hvilke aktører som skal delta i en operasjon er vanskelig å forutse. Det må derfor sikres at løsningene er tilstrekkelig fleksible til at et oppdragsspesifikt nettverk basert på et forhåndsdefinert oppsett kan endres underveis i operasjonen.

Et viktig prinsipp ved det foreslåtte konseptet er at alle aktørene så langt som mulig har tilgang til sine applikasjoner inne fra det oppdragsspesifikke nettverket. Dette innebærer at de enkelte verktøyene enten kjører på et datasenter som er direkte knyttet til det oppdragsspesifikke nettverket, eller at det opprettes en sikker forbindelse fra dette nettverket og tilbake til aktørens eget organisasjonsinterne nettverk.[127] I begge tilfeller vil det settes krav til aktørenes informasjonssystemer, herunder at informasjonssystemene kun deler informasjon som er relevant for den konkrete situasjonen. Digitaliseringsdirektoratet har etablert en rekke nasjonale fellesløsninger som kan være nyttige i denne sammenhengen.[128] Det vil være kostnader forbundet med valg og utvikling av løsninger for å kople sammen de ulike systemene, men fordi alt utstyr i de oppdragsspesifikke nettverkene er virtuelt, vil investeringskostnadene trolig være lave eller moderate. Det må også avklares om det kan være juridiske utfordringer knyttet til sammenkopling av ulike informasjonssystemer, eksempelvis relatert til personvern.

For Forsvarets del må de oppdragsspesifikke nettverkene kunne gjøres tilgjengelige hos FOH, i relevante taktiske kommandoer (eksempelvis i HVs territorielle operasjonssenter) og andre steder som er sentrale i totalforsvarssammenheng. Fordi nettverkene er virtuelle kan de i prinsippet benytte eksisterende fysisk infrastruktur. Ettersom det meste av tjenester i nettverkene vil bli levert som skytjenester, så vil det i liten grad være behov for å installere fysisk maskinvare. Vi har ikke studert i hvilken grad Forsvarets nåværende IKT-løsninger vil kunne støtte slike virtuelle nettverk. For Forsvarets del kan det dermed være investeringskostnader forbundet med dette. I kapittel 4.2.3 viser vi til at dette er investeringer som kanskje må gjøres uansett, ettersom det skjer fundamentale endringer i måten nettverksutstyr fungerer.

Det må gjøres avklaringer innen totalforsvaret rundt roller, ansvar og myndighet for å få til en løsning som skissert her. De tekniske løsningene kan antakelig i stor grad håndteres av en

[127] Dette forutsetter at det organisasjonsinterne nettverket er ugradert.
[128] Digitaliseringsdirektoratet (2021): Fellesløsninger.

kommersiell aktør, men det må avklares hvem som skal stå som ansvarlig, både for de forhåndsdefinerte oppsettene, og for nettverkene som opprettes i forbindelse med operasjoner. Dette inkluderer å sikre at alle nødvendige IKT-tjenester er tilgjengelige, at konfigurasjonsbeskrivelsene er korrekte og at riktig konfigurasjon blir benyttet når et nettverk skal opprettes. Videre må det avklares ansvarsfordeling når ulike aktørers informasjonssystemer knyttes opp mot et oppdragsspesifikt nettverk, hvem som er eier av dataene som lagres der, og hvem som er ansvarlig for at alle deltakende aktører holder et tilstrekkelig nivå på datasikkerheten.

4.2.3 Anbefalinger

Oppdragsspesifikke nettverk som beskrevet i kapittel 3.2, baserer seg på at datamaskiner kjører nettverksfunksjoner som programvare fremfor den tradisjonelle tilnærmingen der man benytter spesialtilpasset maskinvare for å realisere rutere, svitsjer og brannmurer. Dette innebærer også at endringer i nettverket kan gjøres uten noen form for fysiske omkoplinger. Hele tankegangen rundt nettverk endres, og uavhengig av løsningen foreslått i kapittel 3.2 bør Forsvaret utrede hva dette innebærer av muligheter og utfordringer for Forsvaret. Ettersom Forsvaret benytter en rekke sikkerhetsgraderte informasjonssystemer er det ikke sikkert at alle sivile løsninger kan brukes uendret i en militær sammenheng. Forsvaret bør derfor kartlegge hvordan slik nettverksteknologi kan utnyttes innenfor sikkerhetslovens rammer. Fordi det kan være behov for tilpasninger bør man også sørge for tilstrekkelig tilgang på personell med kompetanse innen nettverksvirtualisering, som også har en tilstrekkelig forståelse av Forsvarets behov og utfordringer. Dette kan skje gjennom utdanning av eget personell, eller ved samarbeid med en kommersiell aktør.

Forsvaret er en sentral aktør innenfor totalforsvaret, som blant annet redningsaksjonen i Gjerdrum viste, og det er helt nødvendig med effektiv kommunikasjon med de andre nød- og beredskapsaktørene. Mye tyder på at neste generasjons Nødnett vil bli basert på bruk av kommersielle mobilnett,[129] og det er derfor naturlig at også Forsvaret og forsvarssektoren ser på muligheten for bruk av kommersiell mobilteknologi for å dekke en del av sine kommunikasjonsbehov.[130] I tillegg tilsier gjeldende konsept for utvikling av IKT til bruk på taktisk nivå i Forsvaret, at Forsvaret skal satse på en såkalt hybrid løsning, det vil si en kombinasjon av militære og sivile løsninger.[131] Forsvaret bør derfor undersøke interessen blant de øvrige totalforsvarsaktørene for et samarbeid om å bidra til å realisere et slikt konsept.

For å sikre dekning for de oppdragsspesifikke nettverkene, også der hvor offentlig infrastruktur mangler eller er ødelagt, vil det være hensiktsmessig å fremskaffe mobile 5G basestasjoner samt løsninger for å knytte disse til den øvrige kommunikasjonsinfrastrukturen. For dette vil kommersiell satellittkommunikasjon kunne være et realistisk alternativ, se kapittel 2.4. Gitt at Forsvaret går for en hybrid løsning som nevnt over, bør man ta initiativ til et samarbeid med resten av totalforsvaret rundt fremskaffelse av slike mobile basestasjoner.

[129] Mykkeltveit, Anders mfl. (2021).
[130] Ibid.
[131] Forsvarsdepartementet (2018): Konseptuell løsning for P8043 – Taktisk ledelsessystem for landdomenet. BEGRENSET.

4.3 Mobilitet og hurtighet i militære operasjoner

I kapittel 3.3 presenterte vi hvordan satellitter og UAV-reléer kan legge til rette for økt mobilitet og hurtighet i militære operasjoner. Her diskuterer vi mulige gevinster og utfordringer og gir anbefalinger.

4.3.1 Mulige gevinster

Utviklingen innen satellittkommunikasjon, UAV og billigere og mindre terminaler kan gi høyhastighetskommunikasjon til små kjøretøy og enheter i bevegelse, i prinsippet uavhengig av hvor de befinner seg. Når enheter ikke trenger å stoppe for å etablere kommunikasjon blir de mindre sårbare for lokalisering og dermed også mot beskytning. Selv om de kan lokaliseres vil det kunne ha mindre betydning for beskytning når enhetene konstant flytter på seg.

Tilsvarende gir tilgjengelig kommunikasjon under bevegelse større fleksibilitet under utførelse av militære operasjoner. Forskjellige enheters plassering og bevegelser er ikke begrenset av kommunikasjonssystemer og kan gjøres ut fra rent operative vurderinger, og det er ikke behov for å vente på etablering av kommunikasjonsløsninger.

Dersom Forsvaret velger en løsning som beskrevet i kapittel 3.3, medfører dette at ulike kampavdelinger i større grad får egne sambandsressurser, og behovet for dedikerte sambandsavdelinger, som for eksempel Sambandsbataljonen i Hæren, vil bli mindre. Dette kan gi kostnadsreduksjoner, alternativt frigi personell som kan løse andre oppgaver. Ved å benytte satellittkommunikasjon fremfor løsninger som i større grad baserer seg på distribuert bakkebasert infrastruktur, kan man også redusere det totale behovet for driftspersonell.

Fremveksten av billigere, små terminaler for satellittkommunikasjon på høye frekvenser, muliggjør også at Forsvaret kan redusere omfanget på sin bruk av kostbare satellittkommunikasjonssystemer på lavere frekvenser.

4.3.2 Utfordringer

Valg av optimal kombinasjon av forskjellige typer kommunikasjonssystemer er ikke trivielt. Et stort antall sivile og militære kommunikasjonsløsninger blir tilgjengelige, samtidig som det også blir billigere å bygge egne systemer.

Realisering av gevinstene i kapittel 4.3.1 vil kreve endringer innen både operasjonskonsepter og styrkestruktur, noe som kan være vanskelig å gjennomføre. Økonomiske gevinster som kommer av redusert bruk av nye kommunikasjonsløsninger kan bli begrenset eller forsinket av manglende endringsvilje i organisasjonen og av hensyn til samvirke med allierte.

Satellittkommunikasjonssystemer har, som andre kommunikasjonssystemer, forskjellige typer sårbarheter. Spesielt ved militær bruk av løsninger som er utviklet for sivil bruk, må en ha god forståelse av de ulike løsningenes egenskaper og velge riktig kombinasjon av løsninger tilpasset

behov og trusler. Økt bruk av satellittkommunikasjonsløsninger vil muligens kreve økning i høykvalifisert personell innen drift og forvaltning, selv om det totale antallet personell går ned, se kapittel 4.3.1.

Siden Forsvaret blir mer avhengig av systemer plassert i verdensrommet øker det behovet for å ha oversikt over hendelser i rommet, såkalt s*pace situational awareness* eller SSA. Behovet for SSA er tilstede allerede i dag på grunn av samfunnets og Forsvarets avhengighet av satellittnavigasjon og Forsvarets bruk av rombaserte sensorer. Å etablere og vedlikeholde god situasjonsforståelse i rommet kan være kostbart, men kan være et velegnet område for samarbeid med allierte. I tillegg finnes det allerede sivile tilbydere av slike tjenester.

4.3.3 Anbefalinger

Forsvaret bør utføre en evaluering av egenskaper og testing av ytelse av eksisterende og kommende relevante sivile løsninger for satellittkommunikasjon samt militære løsninger fra allierte. Satellitter i lavbanesystemer kan for eksempel ha ubrukt kapasitet når de flyr over Norge, som ikke uten videre kan benyttes av andre.

Parallelt bør Forsvaret gjøre en detaljert analyse av mulige kombinasjoner av løsninger, som dekker Forsvarets brukerbehov og eventuelle andre krav. Ved analyse av brukerbehov er det viktig å utelukke krav som er til stede på grunn av begrensinger i kommunikasjonsløsninger som brukes i dag.

For å dekke eventuelle behov som ikke kan dekkes av sivile eller allierte løsninger, bør Forsvaret vurdere å fremskaffe en satellittkonstellasjon med lavbanesatellitter. En slik løsning kan for eksempel gi robust samband til utvalgte brukere eller spesifikke plattformer. En tidligere studie gjennomført av FFI viser at en slik konstellasjon med 30 satellitter kan gi svært god dekning.[132] Kostnader vil være sterkt avhengig av ambisjonsnivå, men antas å kunne være under 1 milliard kroner.

Vi anbefaler også at Forsvaret utreder å anskaffe et mindre antall UAV-er i som kan benyttes til kommunikasjonsformål. Beregninger gjort av FFI viser at Forsvaret med et relativt lavt antall UAV-er (10–20) med evne til å fly i noen tusens meters høyde kan oppnå svært god dekning.[133] Slike UAV-er bør kunne benytte forskjellige radioløsninger, med ulik robusthet mot elektronisk krigføring.

Vi anbefaler at Forsvaret utreder anskaffelse av et stort antall terminaler for satellittkommunikasjon til bruk på kjøretøyer og andre mindre enheter. Forsvaret bør vurdere terminaler til bruk med både eksisterende geostasjonære satellittsystemer og med kommende systemer i andre baner.

[132] Bråten, Lars Erling, Abdikerim Yusuf og Andreas Nordmo Skauen (2018): Nanosatellites in low earth orbits for satellite communications. FFI-rapport 17/16210.
[133] Skeie, Bjørn (2020): UAV-dekning i Nord-Norge. FFI-eksternnotat 20/01436. BEGRENSET.

4.4 Utnyttelse av sensordata

Kapittel 3.4 beskriver eksempler på hvordan avansert bildeprosessering og automatisert tekstprosessering kan bidra til å øke Forsvarets evne til å utnytte sensordata og dermed forbedre sin situasjonsforståelse. I det følgende diskuterer vi mulige gevinster og utfordringer og gir anbefalinger.

4.4.1 Mulige gevinster

Gevinsten for Forsvaret ligger først og fremst i å kunne øke automatiseringen av dataprosessering og dermed kunne lage et bedre informasjonsgrunnlag for beslutninger under operasjoner. Eksemplet med AGS (kapittel 3.4.1) illustrerer at automatisering kan øke hastigheten i produksjon av informasjonsgrunnlag, ettersom automatisert prosessering av data tar mindre tid enn manuell behandling. Denne tidsgevinsten kan høstes på to måter: Enten kan beslutningsgrunnlaget komme de rette personene i hende raskere enn det ellers ville gjort, eller så kan tiden man tidligere brukte på manuell behandling utnyttes til å lage et mer solid beslutningsgrunnlag fordi grunnlaget kan baseres på en større mengde informasjon.

Eksempelet med tekstprosessering (kapittel 3.4.2) illustrerer en annen potensiell gevinst. Ved å trekke informasjon ut fra tekst og lagre den på en strukturert form, kan man øke gjenbrukbarheten av informasjonen gjennom at den er enklere å dele med andre. Strukturert lagring av informasjon gjør det også lettere for en organisasjon å vite hvilken informasjon man faktisk besitter, og legger til rette for at informasjonen lettere kan kombineres med annen informasjon slik at man automatisk kan avdekke sammenhenger på tvers av tekstdokumenter. Begge disse aspektene bidrar til å øke kvaliteten på informasjonsgrunnlaget til en beslutningstaker.

Det ligger også en potensiell økonomisk gevinst her hvis man kan redusere behovet for personell til for eksempel bildeanalyse gjennom automatisert analyse. Det er imidlertid mer trolig at man heller vil benytte dette til å utnytte det eksisterende personellet mer effektivt slik at de for eksempel kan utføre analyseoppgaver som ikke så enkelt lar seg automatisere.

4.4.2 Utfordringer

Automatiske analyser av potensielt store mengder informasjon krever omfattende prosesserings- og lagringskapasitet. Slike løsninger omfatter både maskinvare og programvare, og finnes i stor grad som hyllevare på markedet i dag. Ulike komponenter må imidlertid settes sammen til systemer i henhold til de konkrete problemene som skal løses. Man kan i liten grad sette opp eller anskaffe generelle systemer som kan dekke alle slike oppgaver.[134]

Kompetanse er den viktigste innsatsfaktoren for å sette sammen slike komponenter og dermed realisere gode systemer. Det kreves at man kjenner både domenet der oppgaven skal løses (for eksempel taktisk nivå i det militære domenet), problemstillingen som ønskes løst (for eksempel automatisk klassifikasjon av SAR-bilder) og teknologiene som ligger til grunn for løsningene man

[134] Stolpe, Audun mfl. (2019).

har til rådighet for å løse problemstillingen (for eksempel datamaskiner tilpasset taktisk bruk og maskinlæringsalgoritmer som skal utføre klassifiseringen).

Det er vanskelig å finne kompetansemiljøer som behersker alle disse tre momentene. Forsvaret har for eksempel god kompetanse på det militære domenet og tilhørende problemstillinger, men mangler ofte nødvendig kompetanse på teknologi. Denne kompetansen finnes generelt i det sivile markedet. Viktige spørsmål for Forsvaret er derfor hvordan Forsvaret skal skaffe seg tilgang til nødvendig kompetanse, hvilke oppgaver Forsvaret skal løse selv, og hvilke oppgaver som skal overlates til leverandører?

Ved å sette sammen komponenter selv, kan Forsvaret ta i bruk de mange mulighetene som åpen kildekode gir, men dette krever at Forsvaret bygger opp kompetansen til det personellet som skal utvikle, vedlikeholde og drifte løsningene. Militær operativ virksomhet har ofte såpass spesialiserte krav til løsninger at man kanskje ikke vil få de innsparingene man kunne ønske ved å kjøpe standardløsninger.[135] Man må også ta med i beregningen at man vil risikere at mindre direkte styring av løsningen kan føre til at ønskede endringer og forbedringer tar lenger tid å få implementert fordi det er lenger avstand fra bruker til leverandør enn om man håndterte dette i egen organisasjon. Man risikerer også å låse seg til én leverandør (*vendor lock-in*) slik at det kan bli kostbart dersom man ønsker å bytte.

Det er verdt å merke seg at flere store norske virksomheter de siste årene har valgt å ansette egne team for å kunne håndtere mer av utviklingen av komplekse, virksomhetskritiske løsninger selv, heller enn å la dette bli gjort av eksterne leverandører. Eksempler på dette er at NAV ønsker tettere kontroll på sin komplekse IT-portefølje, at Meteorologisk institutt selv håndterer IT relatert til kjernevirksomheten samt Digitaliseringsdirektoratets videre utvikling av Altinn.[136] [137] [138]

En annen utfordring er at resultatene fra automatisert prosessering kan være vanskelig etterprøvbare. Dette gjelder spesielt innenfor gruppen av metoder der man trener opp algoritmer kun ved hjelp av dataeksempler og uten menneskelig rettledning, såkalt dyp læring. Det beste botemiddelet mot dette er så langt kompetanse. Man må sørge for at systemene som utnytter slik teknologi betjenes av personell som kjenner teknologiene godt nok til å kunne betrakte resultatene med sunn skepsis. Det arbeides samtidig med å utvikle algoritmer som selv kan forklare hvordan resultatene er blitt til og på den måten kan bistå beslutningstakere til å vurdere hvordan resultatene fra automatisert prosessering skal behandles.[139] Dette arbeidet er imidlertid foreløpig på forskningsnivå, og vi forventer ikke at dette har nådd tilstrekkelig modenhet for allmenn bruk før om 5–10 år.

[135] Military Embedded Systems (2020): Managing the military's big data challenge.
[136] Digi.no (2016): Nav bygger helt ny IT-avdeling.
[137] Seip, Åsmund Arup (2020): Sourcingstrategier for IKT i offentlig sektor. Fafo-rapport 2020:17.
[138] Digi.no (2021): Altinn skal aldri mer gå ut på dato. Men først må inntil tusen tjenester skrives om.
[139] Tjoa, Erico og Cuntai Guan (2020): A survey on explainable artificial intelligence (XAI): Toward medical XAI. IEEE Transactions on Neural Networks and Learning Systems. PP. 10.1109/TNNLS.2020.3027314.

4.4.3 Anbefalinger

Med tanke på de enorme datamengdene som forventes å være tilgjengelig for Forsvarets beslutningstakere i fremtiden, mener vi det er overveiende sannsynlig at Forsvaret vil komme til å benytte ulike kunstig intelligente systemer, for eksempel til bilde- og tekstprosessering som beskrevet i kapittel 3.4.

Vi anbefaler at Forsvaret gjennomfører en pilotstudie for å øke forståelsen av hvilke teknologier for automatisert analyse av informasjon som egner seg til operativ bruk, hvordan prosessene som blir støttet av teknologien bør utformes for å utnytte disse best mulig, og hvilken kompetanse som trengs for å utvikle, tilpasse og utnytte den nødvendige teknologien. Pilotstudien bør gjennomføres som et samarbeid mellom en egnet operativ avdeling, en forskningsinstitusjon eller universitet med kompetanse på den nødvendige teknologien og FMA som vil være ansvarlige for å gjennomføre eventuelle anskaffelser og forvaltning av materiell.

Vi mener at evnen til å utnytte store datamengder vil bli virksomhetskritisk for Forsvaret, og anbefaler derfor at Forsvaret utarbeider en plan for hvordan man skal oppnå tilstrekkelig tilgang på kompetanse innen dette området til å utvikle og videreutvikle løsninger i nødvendig tempo, også i krise og krig. Som nevnt i kapittel 4.4.2, så har flere store norske virksomheter kommet til at komplekse, virksomhetskritiske løsninger best utvikles internt, og Forsvaret må gjøre en tilsvarende vurdering innenfor dette området.

Forsvaret vil ha behov for kompetanse, også selv om man kun skal benytte systemer som er utviklet av andre aktører. Tolking av resultater fordrer nemlig ofte en god kjennskap til hvordan systemene virker og hvilke styrker og svakheter teknologiene har. Det kan være krevende for forsvarssektoren å rekruttere nødvendig kompetanse i et konkurranseutsatt marked, og vi anbefaler at Forsvaret vurderer å inngå et samarbeid om kompetanseutvikling med utvalgte aktører både for å utdanne og videreutdanne egnet eget personell.

5 Oppsummering og anbefalinger

Målet med studien har vært å peke på muligheter og gi råd til Forsvarets ledelse om utnyttelse av IKT, og dermed bidra til at Forsvaret løser oppgavene sine bedre og mer effektivt. Studien har undersøkt hvordan utvalgte teknologiområder kan bidra til å gjøre Forsvaret bedre og gir eksempler på gevinster Forsvaret kan oppnå ved å ta i bruk ny IKT.

Studien søkte å besvare tre spørsmål: i) Hvordan kan utvalgte teknologiområder bidra til å gjøre Forsvaret bedre?, ii) Hvilke gevinster kan Forsvaret oppnå ved å ta i bruk ny IKT? og iii) Hva kan/bør Forsvaret gjøre på kort sikt for å kunne høste disse gevinstene? For å svare på spørsmålene beskrives først utviklingen innen fire utvalgte teknologiområder innen IKT og hvilke muligheter denne utviklingen medfører. Deretter skisseres fire mulige tilnærminger for hvordan disse mulighetene kan komme Forsvaret til gode, samt mulige gevinster og utfordringer, herunder risikoer og kostnader, for Forsvaret. De viktigste anbefalingene til Forsvaret er oppsummert i dette kapittelet.

Alle de fire tilnærmingene som er beskrevet i rapporten, utnytter flere underliggende teknologier. Vår klare vurdering er at å lage gode løsninger for Forsvaret, i større grad vil handle om å sette sammen teknologier på riktig måte enn å velge enkeltteknologier. Enkeltteknologier alene vil i liten grad generere store gevinster for Forsvaret.

Vi ser også at det ikke kun er manglende teknologisk utvikling som begrenser utnyttelse av teknologi i Forsvaret. Andre faktorer som merkantile og juridiske forhold (for eksempel personvern) og ikke minst Forsvarets vilje og evne til å ta i bruk nye løsninger, er avgjørende.

Vi anbefaler (se også kapittel 4):

1. Forsvaret bør utforme en strategi for hvordan Forsvaret skal utnytte skytjenester, for å få til en kosteffektiv og sikker overgang til bruk av skytjenester i operativ bruk.

2. Forsvaret bør teste operativ bruk av skytjenester for å identifisere løsninger som dekker Forsvarets behov. Det må særlig undersøkes hvor kommersielt tilgjengelige løsninger fra de større leverandørene kan benyttes, og hvor det er behov for mer spesialiserte løsninger.

3. Forsvaret bør øke sin tilgang på kompetanse innen området nettverksvirtualisering, for å sikre at man har tilstrekkelig forståelse av problemområdet, herunder hvilke muligheter som eksisterer innenfor sikkerhetslovens rammer.

4. Forsvaret bør i størst mulig grad sørge for at applikasjoner de bruker er optimaliset for å kjøre i skyen (ofte kalt cloud native).

5. Forsvaret bør ta i bruk 5G, også i operativ bruk, og utarbeide tydelige føringer for bruk av 5G, for eksempel i form av en egen strategi.

6. Forsvaret bør undersøke om det finnes behov i privat og offentlig sektor som sammen med Forsvarets behov kan skape et velfungerende marked for 5G og distribuert sky med små lokale datasentre i Norge.

7. Forsvaret bør vurdere mulig bruk av neste generasjons Nødnett, eller tilsvarende løsninger basert på kommersielle mobilnett, både til kommunikasjon på tvers av totalforsvarsaktører og internt i Forsvaret. Forsvaret bør derfor undersøke interessen blant øvrige totalforsvarsaktører for et samarbeid om å realisere et slikt konsept.

8. Forsvaret bør fremskaffe mobile 5G basestasjoner samt løsninger for å knytte disse til sin øvrige IKT-infrastruktur. Forsvaret bør ta initiativ til et samarbeid med resten av totalforsvaret rundt fremskaffelse av slike mobile basestasjoner. (Betinger at anbefaling 5 følges).

9. Forsvaret bør evaluere egenskaper og ytelse ved relevante sivile og militære løsninger for satellittkommunikasjon. Parallelt bør Forsvaret analysere mulige kombinasjoner av løsninger, som samlet dekker Forsvarets krav.

10. Forsvaret bør utrede å fremskaffe en liten satellittkonstellasjon, for å dekke behov som ikke kan dekkes av sivile eller allierte løsninger, for eksempel robust samband til utvalgte brukere eller spesifikke plattformer.

11. Forsvaret bør utrede fremskaffelse av et stort antall terminaler for satellittkommunikasjon til bruk på kjøretøyer og andre mindre enheter.

12. Forsvaret bør utrede å fremskaffe et mindre antall UAV-er som kan brukes til kommunikasjonsformål. Slike UAV-er bør kunne benytte forskjellige radio- og satellittkommunikasjonsløsninger, med ulik robusthet mot elektronisk krigføring.

13. Forsvaret bør gjennomføre en pilotstudie for å øke forståelsen av hvilke typer teknologier for automatisert analyse av informasjon, for eksempel til bilde- og tekstprosessering, som egner seg til operativ bruk. Studien bør også finne svar på hvordan prosesser i Forsvaret bør utformes for å utnytte systemene best mulig samt hvilken kompetanse som trengs for å utvikle, tilpasse og utnytte systemene.

14. Forsvaret bør øke sin tilgang på kompetanse innen kunstig intelligente systemer for automatisert analyse av informasjon for å sikre tilstrekkelig evne til å utvikle, oppdatere og utnytte systemene også i krise og krig. Vi anbefaler at Forsvaret vurderer å inngå et kompetanseutviklingssamarbeid med utvalgte aktører for å utdanne og videreutdanne egnet eget personell.

Vi understreker igjen at rapporten har fokusert på teknologi og teknologiske muligheter og at rapporten kun har studert utvalgte teknologiområder og mulig bruk av disse i Forsvaret. Anbefalingene i rapporten bør leses i denne konteksten. Anbefalingene i rapporten bør vurderes av

Forsvarets ledelse, sammenstilles med økonomiske rammer, prioriteringer og ambisjonsnivå, og deretter eventuelt konkretiseres og omgjøres til planer.

Forkortelser

3G	Tredje generasjons mobilteknologi
3GPP	3rd Generation Partnership Project
4G	Fjerde generasjons mobilteknologi
5G	Femte generasjons mobilteknologi
AGS	Allied Ground Surveillance
AI	Artificial Intelligence (kunstig intelligens)
AIS	Automatic Identification System
API	Application Programming Interface
AR	Augmented Reality (utvidet virkelighet)
ASBM	Arctic Satellite Broadband Mission
BACN	Battlefield Airborne Communications Node
DSB	Direktoratet for samfunnssikkerhet og beredskap
FD	Forsvarsdepartementet
FFI	Forsvarets forskningsinstitutt
FMA	Forsvarsmateriell
FOH	Forsvarets operative hovedkvarter
GPS	Global Positioning System
GSM	Global System for Mobile Communications (andre generasjons mobilteknologi)
HV	Heimevernet
IaC	Infrastructure as Code
IKT	Informasjons- og kommunikasjonsteknologi
ITU	International Telecommunication Union
MIMO	Multiple-input and multiple-output
MTI	Moving Target Indicator
NKOM	Nasjonal kommunikasjonsmyndighet
NR	5G New Radio
SAR	Syntetisk apertur-radar
SSA	Space Situational Awareness
UAV	Unmanned Aerial Vehicle
UGV	Unmanned Ground Vehicle
USD	Amerikanske dollar

VPN	Virtual Private Network

Referanser

5G Americas (2018): New Services and Applications with 5G Ultra-reliable and low latency communications. 5G Americas whitepaper, November 2018.

Airforce Technology (2020): Project Blackjack: DARPA's LEO satellites take off. Hentet fra: https://www.airforce-technology.com/features/project-blackjack-darpas-leo-satellites-take-off/. Lest 1. juni 2021.

Andås, Harald (2020): Emerging technology trends for defence and security. FFI-rapport 20/01050.

Arnfinnsson, Brynjar, Elisabeth Elman og Sondre Hansen Eriksen (2020): Hvor mye bruker forsvarssektoren på IKT? FFI-rapport 20/00806. BEGRENSET.

Bhamidipati, Sai, Chinmaya Srivatsa, Chethan Gowda og Srikanth Vadada (2020): Generation of SAR Images Using Deep Learning. SN Computer Science. Vol. 1. No. 6. Springer.

Birutis, Agnius og Anders Mykkeltveit (2020): 5G New Radio – oversikt og foreløpige målinger, FFI-eksternnotat 20/02198.

Bråten, Lars Erling, Abdikerim Yusuf og Andreas Nordmo Skauen (2018): Nanosatellites in low earth orbits for satellite communications. FFI-rapport 17/16210.

Business Insider (2019): DeepMind is teaching Google's self-driving cars to get smarter and spot pedestrians better. Hentet fra: https://www.businessinsider.com/deepmind-is-teaching-googles-self-driving-cars-to-get-smarter-2019-7?r=US&IR=T. Lest 15. april 2021.

Business Insider (2021): Drone technology uses and applications for commercial, industrial and military drones in 2021 and the future. Hentet fra: https://www.businessinsider.com/drone-technology-uses-applications?r=US&IR=T. Lest 1. juni 2021.

Canalys (2020): Global cloud services market Q2 2020. Hentet fra: https://www.canalys.com/newsroom/worldwide-cloud-infrastructure-services-Q2-2020?time=1602835241. Lest 10. mars 2021.

Chowdhury, N. M. Mosharaf Kabir og Raouf Boutaba (2009): Network virtualization: state of the art and research challenges. IEEE Communications Magazine, vol. 47, no. 7, s. 20–26, July 2009.

Cloud Native Computing Foundation (2018): Cloud Native Computing Foundation ("CNCF") Charter. Hentet fra: https://github.com/cncf/foundation/blob/master/charter.md. Lest 10. mars 2021.

DataCenter Knowledge (2015): Understanding the Different Kinds of Infrastructure Convergence. Hentet fra:

https://www.datacenterknowledge.com/archives/2015/12/02/understanding-the-different-kinds-of-infrastructure-convergence. Lest 10. mars 2021.

Defensenews (2021): Weapons of the future: Trends in drone proliferation. Hentet fra: https://www.defensenews.com/opinion/commentary/2021/05/25/weapons-of-the-future-trends-in-drone-proliferation/. Lest 1. juni 2021.

Digi.no (2016): Nav bygger helt ny IT-avdeling. Hentet fra: https://www.digi.no/artikler/nav-bygger-helt-ny-it-avdeling/320700. Lest 3. august 2021.

Digi.no (2021): Altinn skal aldri mer gå ut på dato. Men først må inntil tusen tjenester skrives om. Hentet fra: https://www.digi.no/artikler/altinn-skal-aldri-mer-ga-ut-pa-dato-men-forst-ma-inntil-tusen-tjenester-skrives-om/508174. Lest 3. august 2021.

Digitaliseringsdirektoratet (2021): Fellesløsninger. Hentet fra: https://www.digdir.no/digitale-felleslosninger/felleslosninger/939. Lest 10. august 2021.

Direktoratet for samfunnssikkerhet og beredskap (2014): Brannene i Lærdal, Flatanger og på Frøya vinteren 2014. Rapport.

Direktoratet for samfunnssikkerhet og beredskap (2020a): Evaluering av Viking Sky-hendelsen. Rapport.

Direktoratet for samfunnssikkerhet og beredskap (2020b): KVU for fremtidig løsning. Hentet fra: https://www.nodnett.no/Nodnett/kvu-for-fremtidig-losning/. Lest 1. juni 2021.

Docker (2020): Docker. Hentet fra: https://www.docker.com/. Lest 10. mars 2021.

Endregard, Monica, Ann-Kristin Elstad, Ragnhild Endresen Siedler, Janne Tønsager, Kjersti Brattekås og Kristian Åtland (2019). Vurdering av Trident Juncture 2018. FFI-rapport 19/01791. BEGRENSET.

Esteva, Andre, Brett Kuprel, Roberto A. Novoa, Justin KO, Susan M. Swetter, Helen M. Blau og Sebastian Thrun (2017): Dermatologist-level classification of skin cancer with deep neural networks. Nature, vol. 542, no. 7639.

Farsund, Bodil Hvesser og Anne Marie Hegland (2020): 5G i Forsvaret – muligheter og sikkerhetsutfordringer. FFI-eksternnotat 20/01206.

Forsvaret (2018): Digitaliseringsstrategi for Forsvaret.

Forsvaret (2020): Effektrealiseringsplan, Program Mime.

Forsvaret (2021): Åpnet Forsvarets verktøykasse under redningsarbeidet i Gjerdrum. Hentet fra: https://www.forsvaret.no/aktuelt-og-presse/aktuelt/apnet-forsvarets-verktoykasse-under-redningsarbeidet-i-gjerdrum. Lest 10. august 2021.

Forsvarets forskningsinstitutt (2020): Teknologiske trender – Muligheter og utfordringer for fremtidens forsvar. FFI-fakta.

Forsvarets forskningsinstitutt (2021): Utsyn, Forskings- og utviklingsplan 2021-2024, del 1.

Forsvarsdepartementet (2016): Prop. 151 S (2015–2016) Kampkraft og bærekraft. Langtidsplan for forsvarssektoren.

Forsvarsdepartementet (2018): Konseptuell løsning for P8043 – Taktisk ledelsessystem for landdomenet. BEGRENSET.

Forsvarsdepartementet (2019): IKT-strategi for forsvarssektoren.

Forsvarsdepartementet (2020a): Prop. 14 S (2020–2021) Evne til forsvar – vilje til beredskap. Langtidsplan for forsvarssektoren.

Forsvarsdepartementet (2020b): Veileder for gevinstrealisering i forsvarssektoren.

Forsvarsdepartementet (2020c): Prop. 1 S (2020-2021).

Forsvarsdepartementet (2021): Framtidige anskaffelser til forsvarssektoren 2021–2028.

Forsvarsdepartementet og Justis- og beredskapsdepartementet (2018): Støtte og samarbeid: En beskrivelse av totalforsvaret i dag.

Gartner (2020): Gartner Top Strategic Technology Trends for 2021. Hentet fra: https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021/. Lest 10. mars 2021.

Haakseth, Raymond, Oddvar Brønstad, Øyvind Jonsson, Bengt Kristiansen og Nils Agne Nordbotten (2017): Cross-domain communication using an XMPP chat guard, FFI-rapport 17/01491.

Halvorsen, Jonas og Bjørn Jervell Hansen (2020): Exploring data reuse using a big data infrastructure. FFI-rapport 20/02840.

Hamilton, Thomas og David Ochmanek (2019): Operating Low-Cost Reusable Unmanned Aerial Vehicles in Contested Environments. RAND Corporation.

Harrison, Todd, Kaitlyn Johnson og Makena Young (2021): Defense against the dark arts in space – Protecting Space Systems from Counterspace Weapons. Center for Strategic & International Studies (CSIS) Report, February 2021.

Hovedredningssentralen (2021): EVALUERING - Redningsaksjonen og den akutte krise-håndteringen under kvikkleireskredet på Gjerdrum. Rapport til Justis- og beredskaps-departementet 1. juni 2021.

IBM (2019): Infrastructure as Code (IaC). Hentet fra: https://www.ibm.com/cloud/learn/infrastructure-as-code. Lest 15. november 2020.

ITU-R (2015): IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond. Recommendation ITU-R M.2083-0 (09/2015).

Jodalen, Vivianne, Martin Rytir, Vegard Arneson, Bjørn Skeie, Jostein Sander og Lars Erling Bråten (2019): Kommunikasjon i nordområdene – beskrivelse av utvalgte teknologier. FFI-rapport 19/00628. BEGRENSET.

Justis- og beredskapsdepartementet (2020) Meld. St. 5 (2020–2021). Samfunnssikkerhet i en usikker verden.

Kommunal- og moderniseringsdepartementet (2019): Digitaliseringsrundskrivet.

Kommunal- og moderniseringsdepartementet (2020): Nasjonal strategi for kunstig intelligens.

Kvalvik, Sverre, Helene Berg, Elisabeth Elman, Emil Graarud, Ola Krogh Halvorsen, Torbjørn Hanson, Brage Lien og Kristin Waage (2019): Hvordan skape økonomisk handlingsrom i den nye langtidsplanen? – potensial for forbedring og effektivisering 2021–2024. FFI-rapport 2019/01934.

Kystverket (2020): AIS Norge. Hentet fra: https://www.kystverket.no/navigasjonstjenester/ais/ais-artikkelside/. Lest 13. august 2021

Lund, Ketil, Frank T. Johnsen og Arild Bergh (2021): Bruk av skytjenester i Forsvaret – muligheter og utfordringer, FFI-rapport 21/00136.

Maucec, Mirjam Sepesy og Gregor Donaj (2019): Machine Translation and the Evaluation of Its Quality. Recent Trends in Computational Intelligence, 2019.

Military Embedded Systems (2020): Managing the military's big data challenge. Hentet fra: https://militaryembedded.com/ai/big-data/managing-the-militarys-big-data-challenge. Lest: 10. august 2021.

Managing the military's big data challenge - Military Embedded Systems

Mykkeltveit, Anders og Anne Pernielle Hveem (2021): Forsvarssektorens mulige tilnærminger til fremtidig løsning for nød- og beredskapskommunikasjon. FFI-rapport 21/00379. Unntatt offentlighet.

Nasjonal kommunikasjonsmyndighet (2021): Høring av lokale 5G-nett i 3,8-4,2 GHz-båndet. Høring. 9. juni 2021. Hentet fra: https://www.nkom.no/hoeringer/horing-av-lokale-5g-nett-i-3-8-4-2-ghz-bandet. Lest 9. juni 2021.

Nasjonal sikkerhetsmyndighet (2020): Muligheter for en moderne IT-plattform». Dokument-id VIRT-1902-NO. oppdatert september 2020. Hentet fra: https://nsm.no/getfile.php/136422-

1618226528/Demo/Dokumenter/20200921%20VIRT-1902-NO%20Moderne%20IT-plattform.pdf. Lest 10. juni 2021.

National Defense (2021): Federal AI Spending to Top $6 Billion. Hentet fra: https://www.nationaldefensemagazine.org/articles/2021/2/10/federal-ai-spending-to-top-$6-billion. Lest 15. april 2021.

Nato (2021): Allied Ground Surveillance (AGS). Hentet fra: https://www.nato.int/cps/en/natolive/topics_48892.htm. Lest 9. juni 2021.

Nato Science & Technology Board (2020): Science & Technology Trends 2020-2040. NATO UNCLASSIFIED.

NCI Agency (2017): NATO signs milestone contract for IT modernization. Hentet fra: https://www.ncia.nato.int/about-us/newsroom/nato-signs-milestone-contract-for-it-modernization.html. Lest 19. juli 2021.

Nordbotten, Nils Agne, Anne Marie Hegland, Bodil Hvesser Farsund, Federico Mancini, Frode Johan Lillevold og Raymond Haakseth (2015): Information sharing across security domains, FFI-rapport 15/00456.

Northrop Grumman (2021a): Battlefield Airborne Communications Node (BACN). Hentet fra: https://www.northropgrumman.com/what-we-do/air/battlefield-airborne-communications-node-bacn/. Lest 1. juni 2021.

Northrop Grumman (2021b): Global Hawk. Hentet fra: https://www.northropgrumman.com/what-we-do/air/global-hawk/. Lest 1. oktober 2021.

Samferdselsdepartementet (2017): Mer båndbredde for bedre mobile tjenester. pressemelding nr 212/17. Hentet fra: https://www.regjeringen.no/no/aktuelt/mer-bandbredde-for-bedre-mobile-tjenester/id2581485/. Lest 10. august 2021.

Schwab, Klaus (2015): The Fourth Industrial Revolution – What It Means and How to Respond. Foreign Affairs, Dec 2015.

Seip, Åsmund Arup (2020): Sourcingstrategier for IKT i offentlig sektor. Fafo-rapport 2020:17.

Sensei Enterprises (2018): Google Cloud's Defense In Depth Includes Physical Security. Hentet fra: https://senseient.com/ridethelightning/google-clouds-defense-in-depth-includes-physical-security/. Lest 10. mars 2021.

Skeie, Bjørn (2020): UAV-dekning i Nord-Norge. FFI-eksternnotat 20/01436. BEGRENSET.

Spacenews (2020): Amazon's Kuiper constellation gets FCC approval. Hentet fra: https://spacenews.com/amazons-kuiper-constellation-gets-fcc-approval/. Lest 1. juni 2021.

Spacenews (2021a): FCC approves Starlink license modification. Hentet fra: https://spacenews.com/fcc-approves-starlink-license-modification/. Lest 1. juni 2021.

Spacenews (2021b): DoD space agency to award multiple contracts for up to 150 satellites. Hentet fra: https://spacenews.com/dod-space-agency-to-award-multiple-contracts-for-up-to-150-satellites/. Lest 1. juni 2021.

Stolpe, Audun, Bjørn Jervell Hansen og Jonas Halvorsen (2019): Stordatasystemer og deres egenskaper. FFI-rapport 18/01676.

Svendsen-utvalget (2020): Økt evne til å kombinere menneske og teknologi. Veier mot et høyteknologisk forsvar.

Swarm (2021): Swarm. Hentet fra: https://swarm.space/our-technology/. Lest 1. juni 2021.

Tjoa, Erico og Cuntai Guan (2020): A survey on explainable artificial intelligence (XAI): Toward medical XAI. IEEE Transactions on Neural Networks and Learning Systems. PP. 10.1109/TNNLS.2020.3027314.

United States Department of Defense (2020): Department of Defense (DoD) 5G Strategy (U). Approved by Secretary of Defense, mai 2020, Hentet fra: https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf. Lest 10. august 2021.

United States Department of Defense (2020): Department of Defense 5G Strategy Implementation plan. Desember 2020. Hentet fra: https://www.cto.mil/wp-content/uploads/2020/12/DOD-5G-Strategy-Implementation-Plan.pdf. Lest 10. august 2021

United States Marine Corps (2020): Force Design 2030.

Webopedia (2020): Dynamic infrastructure. Hentet fra: https://www.webopedia.com/definitions/dynamic-infrastructure/. Lest 10. mars 2021.

Young, Tom, Devamanyu Hazarika, Soujanya Poria og Erik Cambria (2018): Recent trends in deep learning based natural language processing. IEEE Computational intelligence magazine, vol. 13, no. 3.

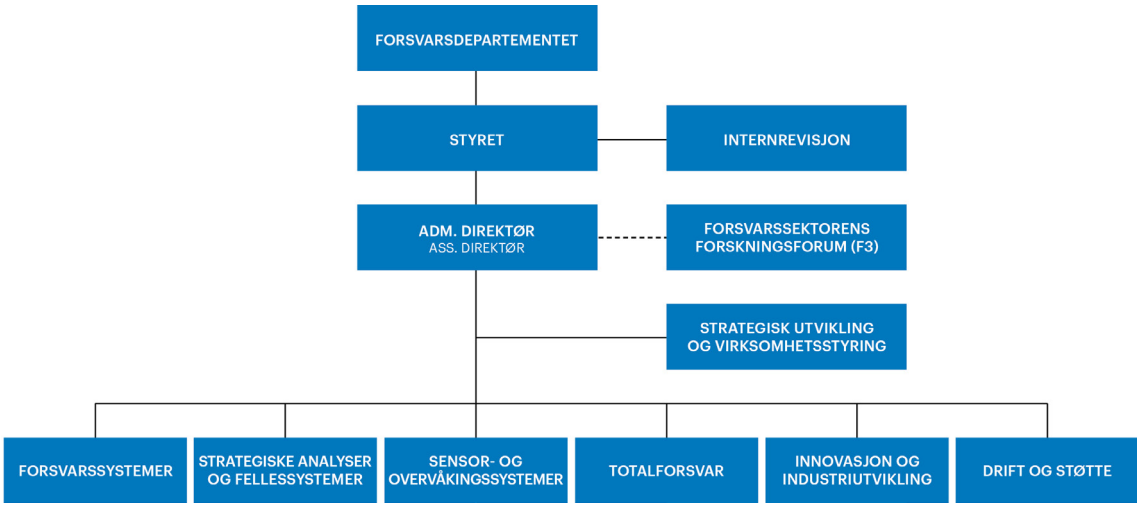
Zhang, Yunquan, Ting Cao, Shigang Li, Xinhui Tian, Liang Yuan, Haipeng Jia og Athanasios V. Vasilakos (2016): Parallel processing systems for big data: a survey. Proceedings of the IEEE, vol. 104, no. 11.

Om FFI
Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan. Med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs formål
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

FFIs visjon
FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs verdier
Skapende, drivende, vidsynt og ansvarlig.



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: post@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: post@ffi.no