FFI Forsvarets forskningsinstitutt

22/00544

FFI-RAPPORT

# Trender innen IKT

## – relatert til militærmakt

Ole Ingar Bentstuen

# Trender innen IKT
## – relatert til militærmakt

Ole Ingar Bentstuen

Forsvarets forskningsinstitutt (FFI) 20. juni 2022

**Emneord**
Teknologiske trender
Trendanalyser
IKT

**FFI-rapport**
22/00544

**Prosjektnummer**
1501

**Elektronisk ISBN**
978-82-464-3416-2

**Engelsk tittel**
Trends related to ICT

**Godkjennere**
Ronny Windvik, *forskningssjef*
Espen Skjelland, *forskningsdirektør*

*Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur*.

# Sammendrag

IKT blir stadig viktigere for å understøtte Forsvarets operasjoner, og utviklingen innen IKT fremover vil derfor også påvirke Forsvarets operasjoner. Det er derfor nødvendig å forstå fremtidig utvikling av IKT.

Rapporten oppsummerer en analyse av både kommersielle og statlige studier av trender innen informasjons- og kommunikasjonsteknologi. Rapporter trekker ut de store linjene i hva som er felles disse trendanalysene og forsøker å knytte dem til hvordan Forsvaret må forholde seg til teknologitrendene fremover. Analysen er gjennomført som en litteraturstudie. Utvalget av litteratur dekker både dokumenter hos våre viktigste samarbeidspartnere og fra de store kommersielle analyseselskapene.

Rapportens konklusjon er at utviklingen innenfor enkeltteknologier nå spiller en mindre rolle enn tidligere når det gjelder anvendelse av IKT. Studien har ikke identifisert at utviklingen innen én enkelt teknologi vil ha stor innvirkning på Forsvaret innenfor en tidsperiode på fem til ti år. Det er derimot en tydelig trend at utviklingen at ny funksjonalitet oppstår ved å sette sammen nye og eksisterende enkeltteknologier for å dekke et behov. IKT kan dermed muliggjøre helt nye måter å operere på eller skape helt nye trusler mot Forsvaret, uten at disse nye mulighetene eller truslene relateres til én enkelt teknologiutvikling.

De kommersielle trendstudiene er veldig tydelige på at det er stadig viktigere å styre IKT-utviklingen. Bedrifter må ta strategiske veivalg basert på et mulighetsrom gitt av nåværende og fremtidig teknologiske muligheter samt samfunnsutviklingen generelt. Deretter må teknologi utvikles eller fremskaffes for å støtte opp den valgte strategien. Det er viktig med god teknologi-forståelse hos ledende personell for å kunne ta de riktige strategiske valgene. Dette er over-førbart til militær kontekst, noe som også trendstudiene fra Nato og allierte nasjoner peker på. Det er en stor endring i hvordan konflikter mellom nasjoner vil arte seg i fremtiden. Forsvaret må forstå både hvordan fremtidens konflikter vil arte seg og hvilke muligheter IKT kan gi til å løse morgendagens utfordringer. Forsvaret må velge en strategiske tilnærming til hvordan konflikter skal håndteres fremover og deretter utvikle og fremskaffe IKT som understøtter den valgte strategiske tilnærmingen.

# Summary

Information and communications technology (ICT) is becoming more and more important in support of military operations, and the future development of ICT will affect military operations. To be able to understand future military operations, we therefore have to understand the future development of ICT.

This report summarizes an analysis of both commercial and governmental studies of relevant ICT trend reports. The report identifies the common features from the trend reports and tries to identify how the Norwegian Armed Forces should respond to these trends in the future. The selection of literature covers both literature from selected allied nations and from the major commercial trend analysis companies.

The conclusion of this report is that the development in individual ICT technologies now plays a smaller role than previously. There is a clear trend that application of technology should be governed by the interaction between technology and organization instead of just applying new technology to existing processes and business. Assembling and applying different technologies in new ways is what leads to progress. Thereby lies the possibility that new ways to combine both existing and emerging technologies can both present new opportunities and new threats for the armed forces.

The commercial trend studies are very clear that it is increasingly important to control development of how technology is applied in an organization. Organizations must make strategic choices based on a space of opportunity given by current and future technological development as well as societal development in general. Technology that supports the chosen strategy must be developed or procured subsequently. In order to make the right strategic choises, senior personnel need to understand technology trends. This is transferable to a military context, which is also identified in the trend studies from NATO and allied nations. Conflicts in the future will change character. The Armed Forces must understand both the nature of future conflicts and what opportunities technology can provide to solve tomorrow's challenges. The Armed Forces must choose strategic approaches to future conflicts, then develop and procure ICT that supports the chosen strategic approaches.

# Innhold

# Innledning

FFI-prosjekt «Forsvarets bruk av det digitale og det elektromagnetiske rom» har som mål å støtte Forsvarsdepartementet og Forsvaret i å behandle informasjons- og kommunikasjonsteknologi (IKT), cyberoperasjoner og elektronisk krigføring i forbindelse med forsvarsanalyser, langtidsplanlegging og militære operasjoner.

En av deloppgavene i prosjektet er å beskrive teknologiske trender[1] innenfor IKT, cyberoperasjoner og elektronisk krigføring i en femårsperiode og hvilke konsekvenser disse trendene har for Forsvaret. Trendanalyser bidrar til bedre forståelse på flere plan. Det kan være teknologiutvikling og -trender som vil påvirke Forsvaret direkte gjennom nye trusler eller at eksisterende prosesser og taktikk må endres, og trender kan gi Forsvaret nye operative muligheter i fremtiden. I gjennomføring av analysen har det dessverre vist seg at det er vanskelig å knytte konkrete enkeltteknologier opp mot konkrete operative konsekvenser for Forsvaret.

Formålet med denne rapporten er å tolke både militære og kommersielle trendrapporter med fokus på hva teknologiutviklingen innen IKT har å si for Forsvaret fremover. Rapporten trekker ut de store linjene i hva som er felles for de studerte trendanalysene og forsøker å knytte disse til hvordan Forsvaret må forholde seg til teknologitrendene fremover. Rapporten vil også forklare hvorfor siste del av deloppgaven, det vil si kople teknologitrender til operative konsekvenser, ikke lar seg besvare på en god måte.[2]

## 1.1 Metode

Analysen er gjennomført som en litteraturstudie. Utvalget av kilder er gjort etter flere kriterier. Vi har søkt etter dokumenter hos våre viktigste samarbeidspartnere som omhandler både teknologitrender og strategier for hvordan de respektive landene skal utnytte IKT-teknologi fremover. Her spiller særlig Nato en viktig rolle i sin tilnærming til og fokus på Emerging and Disruptive Technologies (EDT). Vi har deretter gått gjennom primærkildene som disse dokumentene har benyttet i sitt arbeid og gjort en vurdering om vi skal bruke de i vårt arbeid.

Vi har analysert et utvalg av trendrapporter fra de store, kjente kommersielle selskapene,[3] for eksempel Gartner sin årsrapport som er mye brukt i Forsvaret. Vi har identifisert om slike rapporter har konklusjoner som er overførbare til militære operasjoner eller problemstillinger.

I forsøket på å kople spesifikke teknologitrender opp mot konkrete operative konsekvenser utarbeidet prosjektet et sett med høynivå beskrivelser av teknologiutviklingen. Disse

[1] Når vi bruker ordene teknologi og trender videre i denne rapporten begrenser vi oss til informasjons- og kommunikasjonsteknologi hvis noe annet ikke er spesifisert.
[2] Det er gjennomført aktiviteter i prosjektet som delvis besvarer andre halvdel av deloppgaven for utvalgte teknologier i én bestemt situasjon. Se. Siedler, Ragnhild E. mfl. (2022) «(U) Det Blå IKT-spillet – en beskrivelse av muligheter ved ny IKT under begrenset angrep», FFI-rapport 22/00897, KONFIDENSIELT.
[3] Det ble utgitt nye versjoner av de omtalte kommersielle trendrapportene under ferdigstillelse av denne rapporten. De nye versjonene endrer ikke vesentlig på noen av konklusjonene i denne rapporten.

beskrivelsene omhandler ikke enkeltteknologier, men beskriver muligheter gitt kombinasjoner av enkeltteknologier.

Denne rapporten beskriver ikke enkeltteknologier i detalj, til det henvises leseren til våre primærkilder. Innsatsen har vært på å forstå teknologitrendene, hva som endrer seg og hvordan teknologiutviklingen blir beskrevet i de forskjellige kildene.

## 1.2 Avgrensninger

Prosjektet har studert teknologiutvikling som Forsvaret må ta hensyn til innenfor en periode på fem år til ti år. Det vil si teknologiendringer som Forsvaret må ta hensyn til innenfor tidsperioden, selv om teknologien i seg selv ikke er moden innen fem år. Det er likevel teknologitrender som blir mye omtalt i dag som ikke blir behandlet i denne rapporten, for eksempel kvanteteknologi.[4]

Rapporten fokuserer på trender innen IKT. Prosjektet studerer også elektronisk krigføring (EK) og cyberoperasjoner. Hovedtrekkene fra analyse av IKT-trender vil i stor grad også være gyldige for EK og cyberoperasjoner. Den teknologiske utviklingen innen EK bygger stort sett på de samme enkeltteknologiene som for IKT. Trender innen IKT vil i stor grad styre det teknologiske mulighetsrommet innen cyberoperasjoner.

Prosjektet vil også gi ut en egen rapport som beskriver operative muligheter innen EK. Rapporten vil beskrive både muligheter gitt dagens tilgjengelige teknologier og muligheter basert på teknologiutvikling i nær fremtid.

## 1.3 Rapportens oppbygging

For å få frem de viktigste poengene er det lagt vekt på å lage denne rapporten kort.

Kapittel 2 beskriver de trendanalysene vi har brukt som kilder i dette arbeidet. I kapittel 3 diskuterer vi både de store trekkene fra trendanalysene og hvilke konsekvenser trendene kan få for Forsvaret. I kapittel 4 forsøker vi å beskrive dagens teknologiutvikling på et overordnet nivå slik at personell uten teknisk kompetanse kan få litt bedre grep på muligheter gitt teknologiutviklingen. Til slutt konkluderer og diskuterer vi funnene i kapittel 5.

[4] Kvanteteknologi og kryptografi er et felt som sikkerhetsmyndigheter må ta hensyn til allerede i dag, men vi er av den oppfatning at relevante fagmiljøer har kontroll på denne teknologiutviklingen. Kvanteteknologi relatert til kryptografi og tilsvarende teknologiutvikling er derfor ikke med i rapporten.

# 2 De store trendene

Det er to forskjellige kategorier av trender som er av interesse for denne rapporten. Den første går på effekten av den teknologiske utviklingen innen IKT. Den andre går på den sosio-teknologiske utviklingen og inkluderer trender utenfor våre teknologiområder. De sosio-teknologiske trendene vil påvirke hvordan Forsvaret må ta i bruk eksisterende og kommende IKT for å møte fremtidige utfordringer.

Vi bruker kilder som setter teknologiutviklingen inn i en militær kontekst eller en kontekst som er overførbar til militær anvendelse. Kapittelet forsøker ikke å gjengi alt som står i de forskjellige kildene, men oppsummerer det viktigste for vår analyse. For mer detaljerte beskrivelser henvises leseren til de refererte dokumentene.

## 2.1 Nato

Nato har et stort fokus på hvordan teknologiutviklingen vil styre utviklingen av forsvars- og sikkerhetspolitikk i fremtiden. Nato bruker begrepet *emerging and disruptive technologies* (EDT-er) og har analysert hvordan EDT-ene vil eller kan påvirke alliansens sikkerhet og fremtidige operasjoner. Initiativet følger i hovedsak en *bottom-up*-tilnærming hvor det er teknologiutviklingen som setter rammer for endringer. EDT-ene har vært tema på de siste toppmøtene[5] i Nato.

### 2.1.1 Nato Emerging and Disruptive Technologies

Nato Science and Technology Organization (STO) sammen med Nato Chief Scientist har identifisert åtte EDT-er[6] som på norsk omtales som banebrytende teknologier.

- *Disruptive technologies*
  - Data(vitenskap) (Stordata og avanserte analyser)
  - Kunstig intelligens (AI)
  - Autonomi
  - Verdensrommet (Space)
  - Hypersonisk
- *Emerging technologies*
  - Kvanteteknologier
  - Bioteknologi
  - Nye materialer

[5] Nato (2021): «Emerging and disruptive technologies», hentet fra https://www.nato.int/cps/en/natohq/topics_184303.htm
[6] Nato STO (2020): «Science & Technology Trends 2020-2040 – Exploring the S&T Edge», hentet fra https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

Av disse åtte teknologiene treffer minst fire direkte på fokusområde til denne rapporten: Datavitenskap, AI, autonomi og kvanteteknologi. I tillegg vil space, hypersonisk og bioteknologi sterkt påvirke eller bli påvirket av utviklingen innen IKT.

Forskjellen på brytningsteknologier (disruptive) og kommende (emerging) teknologier er tidshorisonten. Brytningsteknologier begynner allerede å utnyttes i nye militære kapabiliteter, og dette vil bli mer utbredt de neste 5 til 10 årene. Kommende teknologier forventes ikke å gi banebrytende effekter på militære operasjoner før tidligst om 10 til 20 år. Disse blir da ikke videre omtalt i denne rapporten.[7]

Det er viktig å merke seg at EDT-rapporten sier at det mest interessante ikke er de åtte EDT-ene, men forskjellige kombinasjoner av disse trendene. De lister spesielt:

- Data, AI og autonomi
- Data, AI og bioteknologi
- Data, AI og materialer
- Data og kvanteteknologi
- Space og kvanteteknologi
- Space, hypersonisk og nye materialer

Ut ifra de åtte teknologitrendene springer det dermed ut en rekke forskjellige anvendelser av teknologiene. Det er hvordan vi setter sammen de forskjellige teknologikomponentene som forventes å få størst effekt på alliansen.

EDT-rapporten lister i tillegg en del kontekstavhengige trender. Den peker på viktigheten av at utviklingen innen vitenskap og teknologi endrer både samfunn, organisasjoner og individer. Det er også mulig at teknologier blir tatt i bruk på en helt annen måte enn forutsatt eller forventet. EDT-rapporten diskuterer spesifikt både arktiske områder og operasjonsmiljøer dannet av IKT, cyberkapasiteter og elektronisk krigføring, altså det digitale og elektromagnetiske rom. Disse operasjonsmiljøene blir særlig påvirket av teknologiutviklingen innen IKT, og det kan være store forskjeller på hvordan ulike nasjoner tar i bruk ny teknologi. Dette kan være en utfordring i seg selv.

### 2.1.2 Nato Advisory group on EDT

Nato har satt sammen en ekspertgruppe bestående av fremtredende sivile teknologer[8] og innovatører for å støtte Nato i å forstå konsekvensene av den teknologiske utviklingen. Ekspertgruppen skal gi ut årlige rapporter innen EDT. Årsrapporten fra 2020[9] beskriver trender[10] i fem hovedkategorier med tilhørende underkategorier:

[7] Jf. kapittel 1.1 for avgrensning av prosjektet.
[8] Norsk representant er Silvija Seres.
[9] Nato (2020): «Nato advisory group on emerging and disruptive technologies – annual report 2020», hentet fra https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf
[10] Merk at disse trendene er på et annet abstraksjonsnivå enn EDTene i forrige delkapittel.

- Vitenskaps- og teknologiområder
    - Maskinlæring og AI
    - Kvanteteknologi
    - Datasikkerhet
    - *Computing enabled hardware*
    - Biologiske og syntetiske materialer
- Den sosio-tekniske konteksten
    - Cyber-fysiske systemer
- Kampen om ressurser
    - Inkluderer konkurranse om kompetanse som en strategisk utfordring
- Det nye teateret for EDT-aktiviteter: Verdensrommet
- Nødvendige organisatoriske egenskaper
    - Viktigheten av at organisasjonen evner å håndtere EDT

Det er altså bare én av de fem kategoriene som konkret handler om teknologi. De fire andre omhandler sosiale effekter av teknologiutviklingen eller faktorer som vil påvirke anvendelsen av og behovet for ny teknologi. Det er flere interessante trekk ved disse kategoriene, særlig kategori tre og fem.

Det har lenge vært offentlige diskusjoner om kampen om ressurser og da særlig rundt sjeldne mineraler[11]. Ekspertgruppen mener at denne kampen om ressurser fremover også vil inkludere data og kompetanse. Anvendelse av stordataanalyser av forskjellig art, også utenfor militær bruk, krever tilgang til store mengder data. Nasjoner har forskjellige tilnærminger til tilgang til data, for eksempel på grunn av ulike syn på personvern, og dette kan skape store forskjeller i anvendelse av denne type teknologi.

Mange av teknologitrendene utnytter meget komplekse og sammensatte teknologier, og tilgang på kompetanse kan derfor bli en mangelvare på verdensbasis. Nasjoner bør utvikle strategier for hvordan de skal kunne skaffe og beholde kompetanse innen de aktuelle områdene.

Årsrapporten fra 2020 tar frem ett viktig krav for at NATO skal kunne utnytte og forstå konsekvenser av den teknologiske utviklingen:

> *What matters in the technological adaptation as well as technological innovation is how well new and improved technologies are incorporated into effective and intelligent concepts of fighting: it is not the technological sophistication that matters, rather it is the larger framework.*

Dette sitatet indikerer at det ikke er nok å integrere ny teknologi inn i eksisterende operasjons-måter, men at teknologibruken og operasjonsmåter må utvikles i et samspill. Taktikk og operative prosesser må utvikles i takt med teknologiutviklingen og de teknologiske mulighetene.

[11] https://www.aftenposten.no/norge/i/3p6P9/17-sjeldne-mineraler-skaper-storpolitisk-troebbel

Tilsvarende fremhever ekspertgruppen nødvendigheten av å endre organisasjoner for å kunne ta ut effekten av teknologiutviklingen.

## 2.2 Nato Allied Command Transformation (ACT)

Nato Warfighting Capstone Concept (NWCC) er et Nato ACT-program som analyserer hvordan Nato bør se ut i 2040 for å møte morgendagens trusler. De fleste dokumentene er graderte, men det finnes noe offentlig dokumentasjon[12], som vi har tatt utgangspunkt i her.

NWCC er opptatt av hvordan morgendagens trusler mot alliansen vil arte seg. Det er fokus på at en konflikt i fremtiden vil involvere mange domener, inkludert cyberspace og det kognitive domenet. For å møte disse truslene må alliansen kunne bygge situasjonsbilder og utøve kommando og kontroll (K2) på tvers av domener.

I forbindelse med utviklingen av NWCC ble det arrangert et symposium i Nederland sommeren 2020. Rapporten[13] fra symposiet trekker frem mange interessante momenter. Den gjør særlig et nummer ut av samspillet mellom mennesket og teknologien hvor det er kulturelle forskjeller på vesten og andre regioner. Dette kan medføre at teknologi blir tatt i bruk forskjellig i ulike nasjoner. Den fokuserer også på *cross-domain* i to betydninger. Den første er koplingen mellom de forskjellige krigføringsdomenene, det er ikke lenger nok kun å ta hensyn til de tradisjonelle krigføringsdomene (land, sjø og luft). Neste konflikt vil også involvere rom (space), cyber-domenet og det elektromagnetiske rom. Den andre betydningen av cross-domain er nødvendigheten av samvirke mellom militærmakt og sivilsamfunnet.

Rapporten diskuterer videre blant annet konsekvensen av cross-domain. K2 i fremtiden vil bli vanskeligere grunnet kompleksiteten med antall aktører og operasjonsmiljøer, og det er viktig å få på plass ny teknologi som håndterer denne kompleksiteten. Fremtidens K2-systemer må ha flere egenskaper enn dagens systemer. De må evne å fungere på tvers av de tradisjonelle krig-føringsdomenene samt dekke både det digitale og elektromagnetiske rom. Fremtidens K2-systemer må også samvirke med eller håndtere ikke-militære organisasjoner og ressurser, og de må kunne håndtere konflikter under terskelen til væpnet konflikt.

## 2.3 Kommersielle trendanalyser

Det er flere selskaper som utgir årlige trendrapporter, hvor Gartner sin rapport er blant de mest kjente. Rapportene har forskjellig fokus, for eksempel i vektingen mellom teknologi og sosiale konsekvenser av teknologiutviklingen eller mellom fokus på bedrifter og samfunnsmessige forhold. Gartner er den rapporten i vårt utvalg som mest fokuserer på teknologiske aspekter, og får følgelig mest omtale her.

[12] https://www.act.nato.int/nwcc
[13] HCSS Security (2020): «The NATO Warfighting Capstone Concept: Key Insights from the Global Expert Symposium Summer 2020».

### 2.3.1 Gartner Top Strategic Technology Trends for 2021

Gartner sin årlige rapport beskriver de viktigste teknologitrendene og har normalt mye vekting mot utviklingen innen IKT. Naturlig nok fokuserer årsrapporten for 2021[14] på effekten av Covid-19-pandemien. Det er likevel en del effekter vi kan trekke ut fra Gartner sin liste.

Gartner lister ni trender delt inn i tre kategorier:

1) People centricity
    - Internet of Behaviour
    - Total Experience
    - Privacy-enhancing computation
2) Location independence
    - Distributed Cloud
    - Anywhere operations
    - Cybersecurity mesh
3) Resilient delivery
    - Intelligent composable business
    - AI engineering
    - Hyper automation

De tre kategoriene er relevante for Forsvaret på forskjellige måter. Den første kategorien omhandler i stor grad sosiale aspekter ved bruk av teknologi. Selv om pandemien har endret mye på hvordan vi samhandler, er det fortsatt mennesker som er i fokus. Denne kategorien omhandler også bruk av teknologi som medfører endret oppførsel i befolkningen, og til å forstå oppførsel hos mennesker. Den andre kategorien identifiserer endringer som ble tvunget frem av pandemien hvor frakopling fra fysisk tilhørighet er en sentral faktor. Den tredje kategorien omhandler teknologitrender for å levere robuste tjenester under skiftende omstendigheter.

Det er særlig to trekk i Gartner sin rapport som det er verdt å legge merke til:

- Samspillet mellom teknologi og organisasjon
- Fraværet av konkrete teknologier i trendbeskrivelsene

Gartner hevder at de bedriftene og organisasjonene som har gjort det bra under pandemien, er de som har evnet å endre både sin organisasjon og sin bruk av teknologi. Utnyttelse av teknologi er ikke lenger et teknologisk anliggende. Argumentasjonen er at det er et samspill mellom organisasjon og teknologi, det er ikke tilstrekkelig å utvikle kun én av disse uten å tenke på den andre faktoren samtidig. Dette aspektet er ikke nytt, men det har blitt særlig synlig og merkbart under pandemien.

Ingen av de ni trendene fra Gartner omtaler én spesifikk teknologi; alle omhandler anvendelse av teknologi. Dette er en meget merkbar dreining som begynte med Gartner-rapporten fra

[14] Gartner (2021): «Gartner Top Strategic Technology Trends for 2021».

2019[15] og som ble forsterket i 2020[16] og 2021. Dagens trender er ikke lenger avhengig av én spesifikk teknologiutvikling. Trendene består av hvordan samfunnet utnytter et sett med teknologier for å dekke behov.

### 2.3.2 Deloitte Insights Tech Trends 2021

Deloitte fokuserer også på Covid-19 i sin årsrapport for 2021[17] og har et fokus på *resiliens* – evnen til å tilpasse seg og vokse når eksterne faktorer endrer seg. Deloitte sin rapport er først og fremst rettet mot bedrifter og hvordan både teknologitrender og andre trender setter krav til riktige og gode strategiske beslutninger for bedrifter. De velger hvert år ut et sett med trender de fokuserer på, og i rapporten for 2021 er fokusområdene samspillet mellom strategi og teknologi, *data* og samspillet mellom mennesker og teknologi.

Deloitte diskuterer samspillet mellom strategi (for bedriften) og teknologi. Det pågår et markant skifte i dette samspillet, og de bruker begrepet *Tech-enabled strategy*. Bedriftsstrategien må bygge på muligheter gitt av teknologiutviklingen. Følgende sitat karakteriserer dette synet:

> *40% of CEOs said their CIO or tech leader will be the key driver of business strategy — more than the CFO, COO, and CMO combined.*[18]

En viktig presisering er at det er ikke teknologien i seg selv som skal styre bedriftens strategi, men at teknologiutviklingen og -trender muliggjør forskjellige strategier. Når én strategi er valgt må dette følges opp med implementering i både organisasjon og med teknologi.

Oversatt til militær kontekst kan dette leses som at teknologiutviklingen gir et mulighetsrom for både hvilke oppgaver Forsvaret kan løse i fremtiden og hvordan disse oppgavene kan løses. Teknologiutviklingen og andre trender medfører nye trusler og muliggjør nye operasjons-konsepter. Disse må analyseres for at Forsvaret kan vurdere og beslutte hvordan de fremtidige utfordringene skal løse konseptuelt. og deretter velge teknologier som understøtter konseptene.

### 2.3.3 Future Today Institute 2021 Tech Trends Report

Future Today Institute (FTI) gir ut årlige rapporter som beskriver viktige trender basert på teknologiutviklingen.

FTI sin rapport for 2021[19] nevner spesifikt 11 forskjellige trender, hvorav minst åtte er av interesse for vårt prosjekt da de primært er drevet av IKT. Hver av de elleve trendene er beskrevet på samme måte, med *Key insight*, eksempler på bruk, hvilke konsekvenser trenden har, hvem som er viktige aktører og til slutt hvordan en bedrift bør forholde seg til trenden.

[15] Gartner (2019): «Top 10 Strategic Technology Trends for 2019».
[16] Gartner (2020): «Top 10 Strategic Technology Trends for 2020».
[17] Deloitte (2021): «Deloitte Tech Trends for 2021».
[18] Forkortelser: Chief Execute Officer, Chief Information Officer, Chief Financial Officer, Chief Operating Officer, Chief Marketing Officer.
[19] Future Today Institute (2021): «2021 Tech Trends report».

Selv om overskriftene på trendene varierer, fra *Artificial intelligence* til *Health*, *Medical and Wearables*, så er innholdet fokusert på anvendelsen og konsekvenser av trendene og mindre på selve teknologien.

Rapporten fokuserer mye på hvilke strategiske valg en bedrift må gjøre for å kunne utnytte teknologitrendene. Følgende sitat oppsummerer dette:

> *Now, more than ever, your organization should examine the potential near and long-term impact of tech trends. You must factor the trends in this report into your strategic thinking for the coming year, and adjust your planning, operations and business models accordingly.*

Dette sitatet likner på konklusjonen i rapporten fra Deloitte, selv om de bruker forskjellige ord. Mulige fremtidige strategier formes av teknologitrender, og en bedrift må velge en retning innenfor dette mulighetsrommet.

## 2.4 FFI-rapporter

FFI har flere fagmiljøer som arbeider med relaterte temaer. Vi har et eget forskningsmiljø som studerer trender i stort og hvordan trender vil påvirke Forsvaret fremover, og vi har flere dedikerte fagmiljøer innen enkeltteknologier som generelt må holde seg oppdatert innen sine fagfelt.

I perioden 2013 til 2019 gjennomførte FFI en serie med prosjekter som analyserte effekten av globale trender på militære operasjoner. Hovedrapporten[20] fra studien i 2019 diskuterer effekten av en rekke forskjellige typer trender inkludert teknologitrender. Rapporten omhandler i stor grad hvordan globale trender vil påvirke internasjonale relasjoner og den liberale verdens-ordenen. Rapporten diskuterer effekten av teknologiutviklingen og en av konklusjonene er at ny teknologi, som cyberdomenet, kan bidra til raskere eskalering av konflikter. Utviklingen innen IKT bidrar også til at teknologi blir spredt mye raskere mellom nasjoner, og bidrar til at nasjoner med høyere økonomisk vekst, for eksempel utviklingsland, kan oppnå høyere moder-niseringsnivå. Det å være på teknologiske etterskudd vil få enda større konsekvenser i fremtiden.

FFIs prosjektmiljø TEKNO[21] studerer den teknologiske utviklingen generelt og hvilke konsekvenser utviklingen har for Forsvaret. Rapporten «Emerging Technology Trends for Defence and Security»[22] lister 17 teknologitrender som vil påvirke Forsvaret fremover.[23] Den listen er generell og inneholder dermed mye som ikke er relatert til IKT. Hovedkonklusjonen fra

[20] Beadle, Alexander William mfl. (2019): «Globale trender mot 2040 – et oppdatert fremtidsbilde», FFI-rapport 19/00045.
[21] https://www.ffi.no/forskning/prosjekter/teknologiske-trender.
[22] Andås, Harald (2020): «Emerging technology trends for defence and security», FFI-rapport 20/01050.
[23] Teknologitrendene er delt inn i tre tidshorisonter: 2020–2026, 2028–2032 og 2035–2040+.

rapporten er at teknologiutviklingen kan endre både hvordan krigføring arter seg og maktbalansen mellom stater.

TEKNO-miljøet har også studert hvordan ikke-statlige aktører kan utnytte kommende teknologier, dokumentert i en rapport[24] fra 2021. Rapporten diskuterer hvordan ikke-statlige aktører kan benytte teknologiutviklingen til å skape et skadepotensiale mot samfunns- og statssikkerhet som slike grupper ikke har i dag. Hovedkonklusjonen i rapporten er at Forsvaret vil få helt nye utfordringer med å håndtere eventuelle trusler fra slike aktører og grupperinger i fremtiden.

Andre utvalgte prosjektmiljøer på FFI har nylig gitt ut en rapport som beskriver hvordan Forsvaret kan utnytte noen muligheter gitt av utviklingen innen IKT.[25] Rapporter tar for seg fire teknologiområder og gir fire eksempler på hvordan Forsvaret kan utnytte de omtalte teknologiområdene. De fire teknologiene er automatisert analyse, skyteknologi, femte generasjons kommersiell mobiltelefon (5G) og langtrekkende høyhastighetskommunikasjon. Alle de omtalte eksemplene på operativ bruk av teknologiutviklingen, som dekker både totalforsvaret og rene militære operasjoner, benytter flere av de omtalte teknologiområdene. Det illustrerer at én-til-én kopling mellom teknologiutvikling og anvendelse er mindre relevant enn tidligere.

På oppdrag fra NSM analyserte FFI i 2017 relevante sikkerhetsutfordringer i fremtidens EKOM-tjenester.[26] Rapporten diskuterer spesifikt temaene virtualisering, 5G, kunstig intelligens og autonomi, komplekse verdikjeder og tillitsskapende teknologier. Utviklingen innen virtualisering og nye systemer for management av kommunikasjonsinfrastruktur, som blir innført i forbindelse med 5G, medfører store endringer i hvordan sikkerhetsfunksjonalitet kan implementeres i moderne kommunikasjonsnettverk. Rapporten diskuterer også den økte kompleksiteten i moderne kommunikasjonsnettverk og hvilke konsekvenser det har på organisasjon og krav til kompetanse fremover.

## 2.5 Storbritannia

Storbritannia har i de senere årene hatt stor oppmerksomhet på hvilke konsekvenser utviklingen innen forskning og teknologi vil få på sitt forsvar. Dette gir utslag i for eksempel øremerking av £4,1 milliarder ekstra til forskning under forsvarsbudsjettet for perioden 2021–2024.[27] Det er tre dokumenter fra Storbritannia som er av spesiell interesse.

- UK MoD: defence technology framework 2019[28]
- Science and Technology Strategy, høst 2020[29]

[24] Mayer Michael, Mats Rjaanes Harald Erik Andås Truls H. Tønnessen (2021): «Ikke-statlige aktører og fremvoksende teknologi mot 2050 - utviklingstrekk og konsekvenser for militære operasjoner», FFI-rapport 21/01026.
[25] Voldhaug, Jan Erik mfl. (2021): «Hvordan kan ny IKT gjøre Forsvaret bedre?», FFI-rapport 21/01819.
[26] Bentstuen, Ole Ingar, Bodil Hvesser Farsund, Lasse Øverlier og Geir Køien (2017): «Sikkerhetsutfordringer i fremtidens EKOM-tjenester», FFI-rapport 17/17047.
[27] House of Commons library (2021): «Integrated Review 2021: Emerging defence technologies», mars 2021.
[28] UK MOD Defence Science and Technology (2019): «The Defence Technology Framework», september 2019.
[29] UK MOD (2020a): «Science and Technology Strategy 2020», v1.2, oktober 2020.

- UK MoD: Intergrated Operating Concept, høst 2020[30] og høst 2021[31]

Et særtrekk fra Storbritannia er at arbeidet med teknologitrender og dens betydning for det britiske forsvaret er forankret høyt i både forsvaret og i forsvarsdepartementet (MoD). Det er en top-down tilnærming hvor teknologitrendenes betydning på for militære kapabiliteter på lang sikt er med på å styre utviklingen og utformingen av forsvaret.

### 2.5.1 UK MoD: Defence Technology Framework

Dette dokumentet fra 2019 beskriver viktigheten av å forstå teknologiutviklingen og dens strategiske betydning. Dokumentet lister fire viktige steg i denne prosessen.

- Forstå utfordringer, implikasjoner, trusler og valgmulighet gitt av teknologiutviklingen.
- Utvikle politikk og strategier for å realisere strategiske ambisjoner.
- Optimalisere egen tilnærming til hvordan teknologi skal utnyttes.
- Prioritere investeringer i kapabiliteter innen vitenskap og teknologi som gir best effekt på kort og lang sikt. Dokumentet er nøye på å beskrive at slike kapabiliteter inkluderer mennesker, kunnskap og infrastruktur i statlige organer, eksterne leverandører og internasjonale partnere.

Dokumentet skiller så mellom teknologifamilier og anvendelsesområder. Teknologifamiliene er teknologiutvikling som har de største mulighetene til, enten alene eller i kombinasjon, å kunne avgjøre fremtidige konflikter. Dokumentet lister sju teknologifamilier:

- avanserte materialer
- kunstig intelligens, maskinlæring og datavitenskap
- autonome systemer og *robotics*
- energi; energilagring, -konvertering og -transport
- sensorer
- avansert elektronikk og prosessering
- effektorteknologier.

Deretter lister dokumentet ni forskjellige anvendelsesområder: *space*, *platforms*, *comprehensive intelligence*, *surveillance and reconnaissance*, *modernised logistics and support*, *enhanced cyber and electronic warfare*, *next generation weapon systems*, *resilient communications*, *human enhancement* og *next-generation command and control*. For hvert anvendelsesområde er det knytning til hvilke teknologifamilier som bidrar til anvendelsen. For eksempel bygger resilient communications på teknologifamiliene avanserte materialer, kunstig intelligens, energi, sensorer og avansert elektronikk og prosessering. Det er verdt å merke seg at alle de ni anvendelsesområdene hviler på minst fem av de sju teknologifamiliene. Områdene space og platforms hviler på alle de sju teknologifamiliene.

[30] UK MOD (2020b): «Introducing the Integrated Operating Concept», september 2020.
[31] UK MOD (2021): «Integrated Operating Concept», august 2021.

Inndelingen i teknologifamilier og anvendelsesområder er en bevissthet rundt at det ikke lenger er enkeltteknologier i seg selv om har størst konsekvenser for den strategiske utviklingen av militære styrker. Den store operative nytten oppnås når flere teknologier sammen bidrar til nye operative kapabiliteter.

### 2.5.2 Science and Technology Strategy

Dette dokumentet ble gitt ut av *Chief Scientific Advisor to the UK MoD* i oktober 2020 og beskriver hvordan forskning og teknologi vil forme det britiske forsvaret fremover. Dokumentet fremhever at fremtidige målbilder må beskrive hva Forsvaret ønsker å oppnå av kapabiliteter. Teknologi må deretter utvikles og settes sammen for å oppnå disse kapabilitetene. Dette til forskjell fra tidligere tider hvor ny forskning og teknologi stort sett ble brukt for å løse eksisterende utfordringer og problemer. Det er viktigere å forstå hvordan teknologiutviklingen former fremtiden enn å bruke teknologiutviklingen til å løse et eksisterende problem.

Dokumentet lister spesielt fem områder som er viktige i tiden fremover:

- Pervasive, full spectrum, multi domain Intelligence, Surveillance and Reconnaissance
- Multi-domain Command & Control, Communications and Computers (C4)
- Secure and sustain advantage in the sub-threshold[32]
- Asymmetric hard power
- Freedom of Access and Manoeuvre

Dokumentet skiller mellom fremtider formet av teknologiutvikling og konkret utvikling av teknologi. Strategier må etableres basert på mulige fremtidsbilder basert på forskning og utvikling. Når strategier er laget må det utvikles konkret teknologi eller sammensetting av teknologi for å realisere strategiene.

Dokumentet gjør også et stort poeng ut av at teknologiledelse må være en integrert del av ledelsen av forsvaret. Ledere må forstå teknologi og konsekvenser av teknologiutviklingen, det er ikke lenger nok å overlate dette til noen langt ned i organisasjonen. Dette er forøvrig også en av konklusjonene til Svendsen-utvalget.[33]

### 2.5.3 Intergrated Operating Concept

Integrated Operating Concept er et britisk strategidokument som peker på en ny tilnærming til hvordan militære styrker skal anvendes i en fremtid preget av stormaktrivalisering og -konkurranse og hurtig utvikling i anvendelse av militærmakt.

Dokumentet skisserer strategiske målbilder basert på hvordan potensielle fiender kan true Storbritannia på lang sikt. Dokumentet legger mye vekt på Russland og Kina og hvordan disse

[32] Konflikter under terskelen til væpnet konflikt.
[33] Svendsen-utvalget (2020): «Økt evne til å kombinere menneske og teknologi – Veier mot et høyteknologisk forsvar», 24. juni 2020.

nasjonene jobber aktivt under terskelen for væpnet konflikt. Trusselen mot Storbritannia er ikke lenger kun bruk av militærmakt, og det er en utydelig grense mellom fred og krig.

Noen momenter i dokumentet er særlig relevant for utviklingen innen IKT, cyberkapasiteter og elektronisk krigføring. Det er ikke slik at disse teknologiene hver for seg og alene utgjør en trussel mot Storbritannia, det er mer hvordan teknologiutviklingen innen disse områdene utnyttes i en større kontekst av andre nasjoner mot Storbritannia.

Siden trusselbildet er sammensatt og ikke lenger kun er begrenset til militære virkemidler, er det meget sannsynlig at neste store konflikt ikke løses (kun) med militærmakt. Dokumentet gjør et stort poeng ut av at *warfighting* er et subsett av operasjoner. Det vil være mange militære operasjoner i fremtiden som ikke inkluderer bruk av væpnet makt. Det betyr at militære operasjoner i fremtiden må være integrert mellom alle fem krigføringsdomener (luft, land, sjø, cyber og space) og integrert nasjonalt ved at militærmakt fungerer i et samspill med resten av samfunnet, inkludert industri, akademia og sivile samfunnsfunksjoner.

Dokumentet diskuterer mange aspekter som faller utenfor målsettingen med vår rapport. Det som er av interesse er at dokumentet analyserer hva fremtidige operasjonskonsepter vil få av konsekvenser ned på fysiske komponenter. Dokumentet lister ti forutsetninger for implementering av fremtidens forsvar, hvorav disse sju er av direkte interesse for oss:

- rely more heavily on low-observable and stealth technologies
- depend increasingly on electronic warfare and passive deception measures to gain and maintain information advantage
- include a mix of crewed, uncrewed and autonomous platforms
- be integrated into an even more sophisticated networks of systems through a combat cloud that makes best use of the mass of data
- have an open systems architecture that enables the rapid incorporation of new capability, and rapid integration into the network
- employ non-line-of-sight fires to exploit the advantages we gain from information advantage
- emphasise the non-lethal disabling of enemy capabilities, thereby increasing the range of political and strategic options.

Disse sju punktene viser at fremtidens operasjonskonsepter i Storbritannia er sterkt avhengig av nye kapabiliteter innen IKT, cyberkapasiteter og elektronisk krigføring. Dokumentet nevner også at det vil være en vanskelig vei fremover for å få til dette. Det vil kreve store ressurser, mye risiko med aksept for feil og mye eksperimentering med teknologi, militære styrker og nye konsepter.

Det er også åpenbart fra dokumentet at teknologi ikke kan utvikles i et vakuum eller ta utgangspunkt i dagens militære operasjonskonsepter. Teknologi og fremtidige operasjonskonsepter må utvikles i et samspill.

## 2.6 USA

USA har svært mange forskjellige organisasjoner og etater, og det kan derfor være vanskelig å skaffe oversikt over styrende dokumenter.

Det er flere styrende dokumenter, som *National security strategy*[34] og *executive order*[35] om kritisk infrastruktur som bekrefter viktigheten av IKT for USAs sikkerhet. Ut fra disse styrende dokumentene er det igjen utarbeidet andre dokumenter som spesifiserer og svarer på de styrende dokumentene. Vi nevner to av disse her; *National Defence Strategy*[36] og *US DoD 5G strategy implementation plan*[37].

National Defence Strategy er forsvarsministerens sitt svar på National security strategy, og er relativt kortfattet. Dokumentet lister åtte områder som det amerikanske forsvaret må modernisere for å møte USAs sikkerhetsutfordringer. Ett av disse områdene er *Command, control, communications, computers and intelligence, surveillance and reconnaissance* (C4ISR). Andre områder er for eksempel *Nuclear forces* og *Space and cyberspace as warfighting domains*. Dette viser tydelig hvilken plass moderne IKT har på strategisk nivå.

*US DoD 5G strategy implementation plan* er en plan for hvordan det amerikanske forsvaret skal utnytte 5G i fremtidige operasjoner. Dokumentet slår fast at USA er helt avhengig av å utnytte 5G-teknologi på en god måte for å møte fremtidens utfordringer. Dokumentet lister fire forskjellige utgangspunkt for anvendelse av 5G, fra samarbeid med nasjonal industri til at det amerikanske forsvaret utnytter 5G-infrastrukturer i ikke-vennligsinnede land. Dokumentet er interessant for Norge og Forsvaret fordi det åpner for at USA kan sette krav til norsk 5G-infrastruktur – hvordan det amerikanske forsvaret vil utnytte norsk 5G-infrastruktur er avhengig av hvordan vi i Norge har bygget vår infrastruktur.

### 2.6.1 Forskning og teknologi i Forsvarsdepartementet

Forsvarsdepartementet i USA (DoD) har et eget kontor for *Research and Engineering* ledet av en egen viseforsvarsminister – en Chief Technology Officer (CTO).[38] De har laget en prioritert liste over teknologiområder som departementet skal prioritere:

- Kunstig intelligens
- Bioteknologi
- Autonomi
- Cybersikkerhet
- Direktive energivåpen

[34] White House (2017): «National security strategy of the United States of America», Washington, DC, USA, desember 2017.
[35] White House (2019): «Securing the Information and Communications Technology and Service Supply Chain», Executive Office of the President, Executive Order 13873, 15. mai 2019.
[36] US DoD (2018): «Summary of the 2018 National Defence Strategy of the United States of America».
[37] US DoD (2020): «Department of Defense 5G Strategy Implementation Plan», desember 2020.
[38] https://www.cto.mil/

- Fully Networked Command, Control and Communications (FNC3)
- Mikroelektronikk
- Kvantevitenskap
- Hypersonisk
- Space
- 5G

Områdene autonomi, cybersikkerhet, FNC3 og 5G går direkte på områdene vi omtaler i denne rapporten. Det er verdt å nevne at IKT også inngår i alle de andre områdene, ofte som en integrator eller muliggjører av annen teknologi.

Beskrivelsen av 5G er av interesse, departementet tildelte 600 millioner USD til fem testfasiliteter i 2021. Det er ingen av fasilitetene som kun studerer 5G, men de ser på 5G som en muliggjører for ny funksjonalitet. Fokus i de fem fasilitetene er utvidet virkelighet, *smart warehousing* (logistikk og kjøretøy), distribuert kommando og kontroll, og dynamisk spektrumutnyttelse. Dette er nok et eksempel på at 5G kun er en muliggjører for innovasjon, det er først når en setter 5G i system sammen med annen teknologi og organisasjonsutvikling at fremskritt skjer.

### 2.6.2 Forsvarsgrenene

Både US Marine Corps (USMC) og US Army har gjennomført strategiarbeider de siste årene hvor de har analysert hvordan trender, både for teknologi og i samfunnet for øvrig, vil påvirke hvordan konflikter vil arte seg i fremtiden. De har deretter analysert hvordan de skal operere i fremtiden og hvilke kapabiliteter de trenger for disse operasjonene. Disse analysene har resultert i nye strategiske retninger for både USMC og US Army.

US Army Futures Command prioriterer seks områder for utviklingen av hæren i USA.[39] I denne listen er *mobile*, *expeditionary networks* listet på samme nivå som *long range fires* og *next-generation combat vehicle*, som godt illustrerer behovet for robust IKT i morgendagens kampsituasjoner. Long range fires må tilby ildkapasiteter som kan trenge gjennom forsvaret til avanserte motparter og ha god presisjon på mye lengre avstander enn i dag. Det er også nødvendig med nye artillerisystemer med lengre rekkevidde enn dagens systemer. Next-generation combat vehicle er en erkjennelse at dagens kampvogner ikke dekker fremtidens behov, og må få økt mobilitet, ildkraft og beskyttelsesevne. Mobile Expeditionary Network er en moderniseringsstrategi for IKT-systemer som skal gi US Army en mulighet til å «slåss i natt»[40], med fokus på morgendagens teknologiske løsninger. Utviklingen skal fokusere på fire aspekter. Nettverket[41] skal være enhetlig og tilby kommunikasjonstjenester uavhengig av operativ kontekst og situasjon. Nettverket skal ha fokus på interoperabilitet både mot andre forsvarsgrener og mot allierte. Nettverket skal støtte kommandoplassers behov for mobilitet og

[39] US Army (2019): «2019 Army Modernization Strategy: Investing in the future».
[40] *Fight tonight* er et begrep som brukes i flere dokumenter fra US Army.
[41] Bruken av ordet *Network* i beskrivelsen av Mobile Expeditionary Network ser ut til å bety distribuerte IKT-systemer med applikasjoner for å understøtte operasjoner i US Army, altså mer enn et rent kommunikasjonsnettverk.

overlevelsesevne og nettverket skal tilby et felles operasjonsmiljø på tvers av alle nivåene i organisasjonen.

USMC har også analysert hvordan fremtidige konflikter vil arte seg, og hvilke egenskaper eller kapabiliteter USMC må ha for å vinne neste konflikt. En av konklusjonene fra denne studien er at USMC ikke lenger skal ha stridsvogner, men satser på kapabiliteter med høy mobilitet, lav signatur og som har evne til å virke i områder kontrollert av en fiende. Studien beskriver ikke spesielle krav til IKT utover at de trenger C4IS[42] som fungerer under sterk påvirkning fra både offensive cyberoperasjoner og elektronisk krigføring fra en motstander, og som har de samme egenskapene som kampavdelingene innen signatur og mobilitet.

Vi har ikke funnet store arbeider eller rapporter om teknologitrender generelt, de amerikanske rapportene fokuserer mer på hvordan morgendagens operasjoner både blir formet av og avhenger av moderne IKT.

# 3 Vurdering av trender

I dette kapitlet gjør vi en sammenfattet vurdering av dokumentene som er omtalt i kapittel 2. Første trekker vi ut det som er felles fra trendstudiene før vi diskutere hvilke konsekvenser disse trendene kan ha på Forsvaret.

## 3.1 Analyse

Det har skjedd en merkbar dreining over de siste 3–4 årene på hvordan teknologitrender blir beskrevet i forskjellige trendstudier, og det er veldig få studier som i dag lister konkrete enkelt-teknologier. Stort sett alle trender som blir nevnt består av en sammensetting av flere teknologier. Det er også teknologier og bruksområder som blir mindre omtalt i 2020–2021 enn for kun kort tid siden, for eksempel *blockchain*.

De forskjellige studiene bruker til dels forskjellige navn og begreper i sine beskrivelser. Det er likevel mange likhetstrekk mellom studiene da det stort sett er den samme underliggende tekno-logiutviklingen som går igjen i alle studiene. Dette gjelder blant annet 5G med medfølgende teknologier, stordata og tilgang på IKT-tjenester uavhengig av fysisk lokasjon.

Stort sett alle trendstudiene fokuserer på hvilke effekter teknologiutviklingen vil ha i fremtiden. Hvordan vi tar og ønsker å ta i bruk ny teknologi er viktigere enn selve teknologien. Dette er en indikasjon på at det ikke lenger er tilgang på ny teknologi som er den dominerende faktoren for

[42] Command, Control, Communications and Computer Information Systems.

hvordan vi tar i bruk teknologi. Nå er det mer vår egen evne til å se muligheter og deretter ta beslutninger om er den primære begrensende faktor.

Det vil derfor i mange situasjoner være de kommersielle mulighetene som bestemmer hvordan samfunnet tar i bruk i teknologi og hvilke teknologier som blir tilgjengelig for samfunnet. Dette betyr at det finnes teknologiske muligheter som ikke blir realisert eller som realiseres på et senere tidspunkt for Forsvaret. Hvis Forsvarets behov for ny teknologisk funksjonalitet ikke er sammenfallende med de kommersielle behovene, må Forsvaret inngå samarbeid med både andre aktører i Norge og med allierte for å fronte felles behov for ny teknologi som industrien kan ta frem. Relevant industri er ikke bare de kommersielle aktørene som Telenor, Telia og Ice, men også utstyrsleverandører av IKT-systemer og enkeltkomponenter innen IKT.

Trendanalysene som fokuserer på bedriftsmarkedet, er også samstemte om behovet for god teknologiledelse. Teknologiutviklingen åpner opp et stort mulighetsrom for hvordan både samfunnet og bedrifter kan utnytte teknologier fremover. Bedrifter trenger en god forståelse for dette mulighetsrommet for å etablere gode strategier. Deretter må bedrifter implementere nye løsninger, i hele PTO-perspektivet, som følger valgt strategi.

Trendstudier som fokuserer på militære konsekvenser ser ut til å ha noe mer fokus på konkrete teknologier enn de kommersielle trendstudiene. Det finnes fortsatt teknologiutviklinger som kan ha direkte omveltende konsekvenser på Forsvaret i fremtiden, og ofte blir kvanteteknologier og hypersoniske våpen trukket frem som eksempler på dette. Vi ser derimot ikke mange slike eksempler innen IKT-området innenfor en tidshorisont på 5 til 10 år. Det er likevel verdt å merke seg at IKT inngår som en komponent i mange, om ikke alle, av de andre teknologi-områdene som blir nevnt i disse trendstudiene.

I tillegg er det mye diskusjon om hvordan fremtidige militære operasjoner vil arte seg. Noen faktorer går igjen i diskusjonene: Neste konflikt vil ikke være begrenset til militærmakt alene og neste konflikt vil heller ikke være begrenset til de tradisjonelle militære krigføringsdomenene land, sjø og luft, men også inkludere space og cyberdomenet. Disse faktorene vil påvirke både hvordan Forsvaret bør operere i fremtiden og hvordan Forsvaret og samfunnet sammen skal løse konflikter og andre oppdukkende hendelser i fremtiden. Det vil være nødvendig for Forsvaret og alliansen å diskutere og definere hvordan fremtidige operasjoner vil arte seg for å finne retningen på fremtidige IKT-anskaffelser i Forsvaret.

Vi mener det er klare paralleller mellom diskusjonene om hvordan bedrifter og Forsvaret skal tilnærme seg teknologiutviklingen. Teknologiutviklingen, sammen med andre sikkerhets-politiske og samfunnsmessige faktorer former fremtidige operasjoner. Forsvaret må identifisere hvilke muligheter som ligger i teknologiutviklingen for deretter å etablere konsepter for sine operasjoner i fremtiden. Først når dette er gjort vil det være mulig å etablere en optimal sammensetting av IKT-løsninger. Dette er et arbeid som må utføres av alle avdelinger i Forsvaret.

## 3.2 Konsekvenser for Forsvaret

Teknologiutviklingen og -trender vil treffe Forsvaret på flere forskjellige måter. Ny teknologi kan erstatte gammel teknologi én-til-én. Ny teknologi kan gjøre at Forsvaret kan løse en oppgave på en annen måte enn i dag. Til slutt kan nye teknologier og trender medføre at Forsvaret får nye eller andre utfordringer de må løse. Det finnes antagelig flere avarter av disse alternativene.

Det enkleste å forholde seg til er at ny teknologi erstatter gammel teknologi én-til-én. Ny teknologi gjør at vi kan gjøre akkurat det samme som før, men antagelig litt bedre, litt fortere eller til en lavere kostnad.

Ny teknologi kan også tillate Forsvaret å løse en oppgave på en annen måte enn før, eller løse oppgaver Forsvaret tidligere ikke har vært i stand til å løse. Denne muligheten er antagelig vanskeligst å forholde seg til på en metodisk, analytisk måte. Slik utnyttelse av teknologiutviklingen vil kreve ny taktikk, endret kompetanse og/eller andre operasjonskonsepter enn i dag. Evaluering av ny teknologi for å løse eksisterende eller nye utfordringer på en annen måte krever at personell klarer å løsrive seg fra eksisterende tankesett om hvordan Forsvaret skal løse en oppgave.

Ny teknologi eller nye trender endrer situasjoner Forsvaret kan komme ut for, det vil si hvilke oppgaver Forsvaret skal eller må løse – trusselbildet endrer seg. Eksempel er fremveksten av cyberoperasjoner, påvirkning og andre effekter i det digitale rom som utfordrer norsk sikkerhet. Autonome plattformer og hypersoniske våpen er også eksempler på teknologiutvikling som vil skape nye trusselbilder og dermed utfordringer for det norske forsvaret.

Nye muligheter og trusler, som de nevnte eksemplene autonome plattformer og hypersoniske våpen, vil mest sannsynlig kreve nye eller endrete egenskaper til den IKT-en som Forsvaret anskaffer. Autonome plattformer utfordrer dagens løsninger for kryptografi[43] og hypersoniske våpen vil kreve robuste kommunikasjonsløsninger med mye lenger rekkevidde enn dagens løsninger.

For å kunne utnytte teknologiutviklingen optimalt må Forsvaret håndtere alle de tre alternativene over gjennom først å forstå konsekvenser av teknologiutviklingen, så diskutere strategiske og taktiske tilnærminger til hvordan Forsvaret skal møte nye utfordringer, og til slutt stake ut en kurs for hvordan Forsvaret tar i bruk ny teknologi.

Alle de kommersielle trendstudiene er enige i at det er behov for god teknologikompetanse høyt oppe i organisasjoner. Dette er etter vår vurdering også gyldig for Forsvaret. For å kunne gjøre strategiske valg må Forsvarets ledere være gode på å forstå teknologitrendene og evne å se hvordan disse påvirker Forsvarets operasjoner og handlemåter.

[43] Martin Strand og Jan Henrik Wiik (2019): «Kryptografisk sikring av autonome og ubemannede enheter – eksisterende forskning», FFI-rapport 19/02042.

Merk at denne studien ikke har analysert hvor Forsvaret er i dag med tanke på konsekvensene over. Forsvaret har gjort mange grep de siste årene for å forbedre prosessene rundt utviklingen av IKT, for eksempel gjennom programmer som MAST[44] og Mime[45], og opprettelsen av en IKT-avdeling i Forsvarsstaben (FST J6).

# 4 Anvendelsesområder

Som beskrevet i kapittel 3 er det ikke lenger en én-til-én kopling mellom en teknologi og anvendelse av teknologien. Selv om essensen i de forskjellige trendstudiene er den samme, er det store forskjeller i hvilke ord og begreper som brukes. De forskjellige trendstudiene har også ulike utgangspunkt for sine analyser. Det kan derfor være vanskelig å forstå konsekvenser og muligheter gitt teknologiutviklingen. Det mangler en enhetlig beskrivelse tilpasset Forsvaret.

Vi[46] har derfor, på tilsvarende måte som strategidokumentene fra Storbritannia, gjort et forsøk på å definere fem anvendelsesområder basert på den pågående teknologiutviklingen innen IKT. Formålet er å løfte beskrivelsen av teknologiutviklingen til et nivå som gjør at beslutningstakere bedre kan diskutere hva Forsvaret ønsker å oppnå på lang sikt. For hvert område lister vi også noen av de underliggende teknologiene som området bygger på. Inndelingen her har en top-down tilnærming og forsøker å beskrive en helhet i mulighetsrommet basert på teknologi-utviklingen innen IKT.[47]

## 4.1 Prosessautomatisering

Fremskritt spesielt innen AI og stordata gjør det nå mulig i større grad enn før å digitalisere og automatisere også avansert analyse, og med det flere prosesser som tidligere kun kunne utføres av mennesker. Disse teknologiene vil hjelpe mennesker til å unytte informasjonen som ligger i store datamengder, og dermed muliggjøre bedre beslutninger. Et eksempel er automatiserte prosesser som kan være bedre enn mennesker til medisinsk diagnose basert på analyse av bilder.

Innen dette området er det et stort spenn av muligheter, fra analyse til det å ta beslutninger. Det siste utfordrer både ansvars- og myndighetsprinsippene i militære operasjoner og krever ekstrem høy tillit til IKT-systemene. Det er mest sannsynlig at prosessautomatisering først vil gjøre seg

[44] Militær anvendelse av skyteknologier.
[45] Program som tar frem kampnær IKT.
[46] Takk til Bjørn Jervel Hansen og Bodil Hvesser Farsund for arbeidet med å definere innholdet i dette kapitlet.
[47] Noen fremtidige muligheter er omtalt i FFI-rapporten «Hvordan kan ny IKT gjøre Forsvaret bedre?». Den rapporten tar en mer bottom-up tilnærming og dekker dermed ikke hele utfallsrommet.

gjeldende innen analyse av til dels store datamengder, for eksempler innen bildeanalyse. Deretter vil det komme systemer for automatisert beslutningsstøtte før vi eventuelt, om lang tid, får systemer som også kan gjennomføre beslutninger på egen hånd.

Dette området vil bli sterkt påvirket av jus, særlig med tanke på personvern. Tilgang på data og myndighetenes mulighet til både samle inn og analysere data vil være forskjellige fra nasjon til nasjon.

Prosessautomatisering ser også ut til å ha stor nytte innen elektronisk krigføring, både på sensorsiden og koordinering av offensive tiltak.[48] Innen cyberoperasjoner kan prosessautomatisering bidra på både defensive og offensiv side.[49]

Eksempler på underliggende teknologier er skytjenester, kunstig intelligens, stordata og 5G.

## 4.2 Empowered Edge

Den sivile utviklingen innen mikroprosessorer gir god tilgang på kraftige, små, fleksible enheter som kan brukes på taktisk nivå. Stor prosesseringskraft er tilgjengelig i små enheter da teknologiutviklingen både reduserer størrelse, vekt og effektbehov, samtidig som batteriteknologi har blitt bedre. Tilgang til både data og prosesseringskraft gjennom skytjenester og kapable nettverk har forsterket denne trenden.

Dette kan gi flere fordeler til Forsvaret. Et opplagt bruksområde er stadig kraftigere prosesseringskapasitet ute i taktiske avdelinger, noe som kan redusere behovet for reachback til hovedkvarterer og andre sentrale lokasjoner for avansert prosessering og analyse. Informasjon og dataverktøy som er nødvendige for å gjennomføre en operasjon, vil være tilgjengelig lokalt og kan skiftes ut fortløpende for hvert nye oppdrag. Dette gir også muligheter for avanserte analyse- og beslutningsstøttesystemer på taktisk nivå. Utviklingen tillater også å plassere ut veldig små enheter, for eksempel små, billige og gode sensorer med prosesseringskapasitet, i et geografisk område for informasjonsinnsamling og -analyse.

Empowered edge vil også gi nye muligheter innen elektronisk krigføring og noen typer cyberoperasjoner. Lokal prosessering i forbindelse med sensorsystemer vil øke kapasiteten til både EK og defensive cyberoperasjoner på taktisk nivå.

Eksempler på underliggende teknologier er tingenes internett (IoT), skytjenester, 5G og virtualisering.

[48] Se for eksempel Sharma, Purabi & Sarma, Kandarpa & Mastorakis, Nikos (2020): «Artificial Intelligence Aided Electronic Warfare Systems – Recent Trends and Evolving Applications»
[49] https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity

## 4.3 Autonome enheter

Autonomi er et stort forskningsfelt i mange nasjoner, også i Norge. Én definisjon på autonomi er maskiner som opererer på egenhånd.[50] Området dekker mange bruksområder og modenhetsnivåer, fra mobile plattformer, som kjøretøy, som kan følge en forhåndsdefinert rute, til våpen og annet utstyr som kan ta beslutninger på egen hånd. Mengden av ting som gjøres autonome øker stadig, og de mest etablerte løsningene er allerede i militær bruk. Ubemannede flygende enheter (kalt droner eller UAV-er) er et eksempel på det siste, selv om disse ikke er autonome i seg selv har de autonome funksjoner som støtter mennesker i å operere disse plattformene. Merk at det finnes våpensystemer i dag som ikke vil fungere uten en eller annen form for autonomi, for eksempel langtrekkende missiler og nærforsvarsvåpen for å skyte ned innkommende missiler.

Det er viktig å huske at autonomi ikke kun dreier seg om autonome våpensystemer. Det er mange eksempler på bruk av autonomi på andre områder. Både i det fysiske domenet og i det digitale eller elektromagnetiske rom eksisterer det sensorsystemer som kan automatisere sine analyser og omkonfigurere sine sensorer etter skiftende behov. Autonome kjøretøy og andre mobile plattformer er også meget velegnete verktøy i situasjoner hvor Forsvaret ikke ønsker å utsette personell for unødvendig fare.

Innenfor IKT-området er det mye forskning og utvikling innen bruk av autonomi for å styre og konfigurere infrastrukturer. Dette kan være plassering av en kommunikasjons-UAV som dekker et operasjonsområde eller automatisert konfigurasjon av kommersielle 5G-nett.

Eksempler på underliggende teknologier er kunstig intelligens, prosessorkapasitet og 5G.

## 4.4 Utvidet virkelighet

Utvidet virkelighet tilbyr tilgang til informasjon direkte til brukerne samtidig som brukeren «ser» den virkelige verden. Dette kan være informasjon i briller, siktemidler eller tilsvarende som tillater brukerne å interaktere med den digitale og den fysiske verdenen samtidig.

Teknologiene bak utvidet virkelighet har vært under utvikling lenge (siden 1990-tallet), men har så langt ikke funnet sitt endelige gjennombrudd i ordinær bruk utover muligens i spillindustrien. Utviklingen har imidlertid pågått jevnt og trutt, og det forventes at teknologiene i løpet av de neste fem årene er modne for mer utstrakt bruk, også militært.

Fordelene med utvidet virkelighet spenner seg fra bedre informasjonsdeling og situasjonsforståelse til trening og øving. Utvidet virkelighet har et stort potensiale innen trening og øving, utover dagens bruk av simulatorer. Utvidet virkelighet tillater også samhandling over lange avstander, for eksempel for å endre hvordan Forsvaret gjennomfører fellestaktisk planlegging.

[50] https://www.ffi.no/forskning/tema/autonomi.

Eksempler på underliggende teknologier er prosesseringskapasitet, 5G og miniatyrisering.

### 4.5 Alltid online

Tilkopling til Internett ses av mange på som en grunnleggende nødvendighet i dagens samfunn, og det er mye utvikling innen kommunikasjonstjenester som bidrar til et slikt mål. Muligheten til å være «online» med god kvalitet på tjenesten vil bli oppnåelig nesten uansett hvor på kloden en bruker er.

5G, felles styringssystemer for kommunikasjonsinfrastrukturer[51] og massive satellittsystemer er de viktigste teknologiske fremskrittene for denne evnen. Til sammen vil disse teknologiene kunne gi tilpassede kommunikasjonstjenester så og si uavhengig av lokasjon. Utviklingen bidrar til at det blir mye enklere dynamisk å sette sammen forskjellige kommunikasjonsteknologier tilpasset et gitt behov. Brukerne kan dermed få de samme tjenestene uavhengig av hvilke teknologiske løsninger som leveres til brukeren.

Samme teknologiutvikling kan også forbedre Forsvarets egen infrastruktur samt samspillet mellom Forsvarets infrastruktur, kommersielle infrastrukturer og infrastrukturer hos andre statlige etater eller hos allierte nasjoner. Tilgang på kommunikasjonstjenester til Forsvarets enheter kan bli bedre, uavhengig av lokasjon og hvilken teknologi hver enhet har tilgang på.

Utviklingen tilsier at Forsvaret enklere kan integrere alle de forskjellige teknologiløsningene Forsvaret har for kommunikasjon. I tillegg vil det bli enklere å utnytte tjenester levert av andre aktører samt knytte Forsvaret kommunikasjonsnettverk sammen med alliertes nettverk og med sivile beredskapsaktører. Dette kan skje samtidig som Forsvaret opprettholder sine særegne krav innen sikkerhet og robusthet.

# 5 Oppsummering

Prosjektet har gått gjennom mange forskjellige kilder som beskriver teknologiutviklingen innen IKT. Vår konklusjon er at utviklingen innen én enkelt teknologi ikke alene vil få store følger for Forsvaret innenfor en tidshorisont på 5 til 10 år. Anvendelsen av teknologi er mer styrt av behov for funksjonalitet og ikke hva som teknisk blir tilgjengelig. Innovasjon er vel så mye drevet av å sette sammen teknologier på nye måter som å ta frem ny enkeltteknologi. Dette betyr også at teknologier kan bli tatt i bruk på andre måter enn de opprinnelig var tiltenkt.

Enkeltteknologier blir så å si ikke lenger omtalt i de kommersielle trendstudiene. Det er vår egen evne til å se muligheter, og deretter ta beslutninger om fremtiden, som er den primære

[51] Bentstuen, Ole Ingar (2019): «Trender som påvirker Forsvarets kommunikasjonsinfrastruktur», FFI-fakta 2019.

begrensende faktor i utnyttelse av teknologi. Dette i motsetning til tidligere da det i større grad var enkeltteknologier som begrenset vårt mulighetsrom.

En konsekvens av dette er at det ofte vil være de kommersielle mulighetene som bestemmer hvordan samfunnet tar i bruk i teknologi og hvilke teknologier som blir tilgjengelige for samfunnet. I dette ligger det også at det finnes teknologiske muligheter som ikke blir realisert eller som blir realisert på et senere tidspunkt da de mangler kommersielle muligheter. Forsvaret må samarbeide med andre aktører, både nasjonalt og internasjonalt, for å, om mulig, få IKT-industrien til ta frem teknologiløsninger som også dekker Forsvarets behov.

De kommersielle trendstudiene har et stort fokus på at organisasjoner og teknologi må utvikles sammen for å kunne nå strategiske mål. Organisasjoner må evne å forstå et mulighetsrom gitt av teknologiutvikling og deretter forme organisasjonen og anvendelse av teknologi opp mot organisasjonens strategiske mål.

Disse trendene er overførbare til Forsvaret, noe som også blir beskrevet i trendstudiene fra Storbritannia og Nato. Det fremtidige mulighetsrommet gitt av teknologiutviklingen må forstås for å kunne ta gode beslutninger om IKT fremover. Det vil være gap mellom det Forsvaret har behov for av IKT i fremtiden og den teknologien som i utgangspunktet leveres av industrien. Dette gapet må dekkes av forskning og utvikling spesifikt for Forsvaret, helst i samarbeid med akademia og industrien. Det vil derfor fortsatt være nødvendig med forskning og utvikling innenfor både enkeltteknologier og hvordan teknologiutviklingen kan utnyttes.

Det er en pedagogisk utfordring å beskrive dette fremtidige mulighetsrommet. Kapittel 4 i denne rapporten er et forsøk på å løfte beskrivelse av teknologiske muligheter til et nivå som skal hjelpe beslutningstakere til å forstå dette mulighetsrommet.

Et samfunns utnyttelse av teknologiutviklingen blir også styrt av andre forhold, som kultur og legale prinsipper. Dette er for eksempel synlig innen anvendelse av stordata og automatisert analyse. Forskjellige nasjoner har forskjellig tilnærming til tilgang til store datamengder, for eksempel innen syn på personvern, og dette kan skape store forskjeller mellom nasjoner i anvendelse av denne type teknologi. Dette betyr at det ikke lenger er gitt at det eksisterer en symmetri mellom muligheter og trusler på tvers av nasjoner da nasjoner vil ta i bruk teknologier på forskjellige måter.

Særlig Storbritannia har stort fokus på hvordan utviklingen innen vitenskap og teknologi vil påvirke nasjonens sikkerhet fremover. Natos diskusjoner rundt EDT-er skisserer også en slik retning, men ikke like utfyllende som den britiske. Utviklingen av en nasjons sikkerhet i fremtiden avhenger av å forstå mulighetsrommet gitt av teknologiutviklingen. Nasjoner må så gjøre valg innenfor dette mulighetsrommet og deretter iverksette tiltak i hele spennet fra forskning til organisasjonsutvikling for å nå disse målene.

De militære trendstudiene vi har analysert er alle opptatt av at fremtidens operasjonsmiljø og trusler vil forandre seg fremover. Krigens art og hvordan konflikter vil arte seg om 20 år vil sette andre krav til IKT-systemer enn dagens operasjoner. Samvirke mellom Forsvaret, sivile

etater og kommersiell industri blir trukket frem som et viktig område som fremtidige IKT-systemer må understøtte. Fremtidens IKT-systemer må fungere på tvers av alle krigførings-domener, inkludert det digitale og elektromagnetiske rom, og fremtidige IKT-systemer må også få nye egenskaper slik at de fungerer bedre i miljøer utfordret av en fiende.

# Referanser


Aftenposten (2015): «17 sjeldne mineraler skaper storpolitisk trøbbel», hentet fra https://www.aftenposten.no/norge/i/3p6P9/17-sjeldne-mineraler-skaper-storpolitisk-troebbel.

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

Beadle, Alexander William mfl. (2019): «Globale trender mot 2040 – et oppdatert fremtidsbilde», FFI-rapport 19-00045, juli 2019.

Bentstuen, Ole Ingar (2019): «Trender som påvirker Forsvarets kommunikasjonsinfrastruktur», FFI-fakta 2019.

Bentstuen, Ole Ingar, Bodil H. Farsund, Lasse Øverlier og Geir Køien (2017): «Sikkerhetsutfordringer i fremtidens EKOM-tjenester», FFI-rapport 17/17047, februar 2018

Deloitte (2021): «Deloitte Tech Trends for 2021».

Future Today Institute (2021): «2021 Tech Trends report».

Gartner (2019): «Top 10 Strategic Technology Trends for 2019», hentet fra https://www.gartner.com/en/doc/3891569-top-10-strategic-technology-trends-for-2019

Gartner (2021): «Gartner Top Strategic Technology Trends for 2021», hentet fra: https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021/

HCSS Security (2020): «The NATO Warfighting Capstone Concept: Key Insights from the Global Expert Symposium Summer 2020».

House of Commons library (2021): «Integrated Review 2021: Emerging defence technologies», mars 2021.

Martin Strand og Jan Henrik Wiik (2019): «Kryptografisk sikring av autonome og ubemannede enheter – eksisterende forskning», FFI-rapport 19/02042.

Mayer Michael, Mats Rjaanes Harald Erik Andås, Truls H. Tønnessen (2021). «Ikke-statlige aktører og fremvoksende teknologi mot 2050 – utviklingstrekk og konsekvenser for militære operasjoner», FFI-rapport 21/01026.

Nato (2020): «Nato advisory group on emerging and disruptive technologies – annual report 2020», hentet fra https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf

Nato (2021): «Emerging and disruptive technologies», hentet fra https://www.nato.int/cps/en/natohq/topics_184303.htm

Nato ACT: «Nato Warfighting Capstone Concept», https://www.act.nato.int/nwcc

Nato STO (2020): «Science & Technology Trends 2020-2040 – Exploring the S&T Edge», hentet fra https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

Sharma, Purabi & Sarma, Kandarpa & Mastorakis, Nikos (2020): «Artificial Intelligence Aided Electronic Warfare Systems – Recent Trends and Evolving Applications», IEEE Access. 8. 1-1. 10.1109/ACCESS.2020.3044453.

Svendsen-utvalget (2020): «Økt evne til å kombinere menneske og teknologi – Veier mot et høyteknologisk forsvar», 24. juni 2020.

Siedler, Ragnhild E. mfl. (2022) «(U) Det Blå IKT-spillet – en beskrivelse av muligheter ved ny IKT under begrenset angrep», FFI-rapport 22/00897, KONFIDENSIELT.

Voldhaug, Jan Erik mfl. (2021): «Hvordan kan ny IKT gjøre Forsvaret bedre?», FFI-rapport 21/01819, november 2021.

White House (2017): «National security strategy of the United States of America», Washington, DC, USA, desember 2017.

White House (2019): «Securing the Information and Communications Technology and Service Supply Chain», Executive Office of the President, Executive Order 13873, 15. mai 2019.

UK MOD (2019): «The Defence Technology Framework», september 2019.

UK MOD (2020a): «Science and Technology Strategy 2020, v1.2», oktober 2020.

UK MOD (2020b): «Introducing the Integrated Operating Concept», september 2020.

UK MOD (2021): «Integrated Operating Concept», august 2021.

US Army (2019): «2019 Army Modernization Strategy: Investing in the future», hentet fra https://www.army.mil/standto/archive/2019/10/17/

US DoD (2018): «Summary of the 2018 National Defence Strategy of the United States of America».

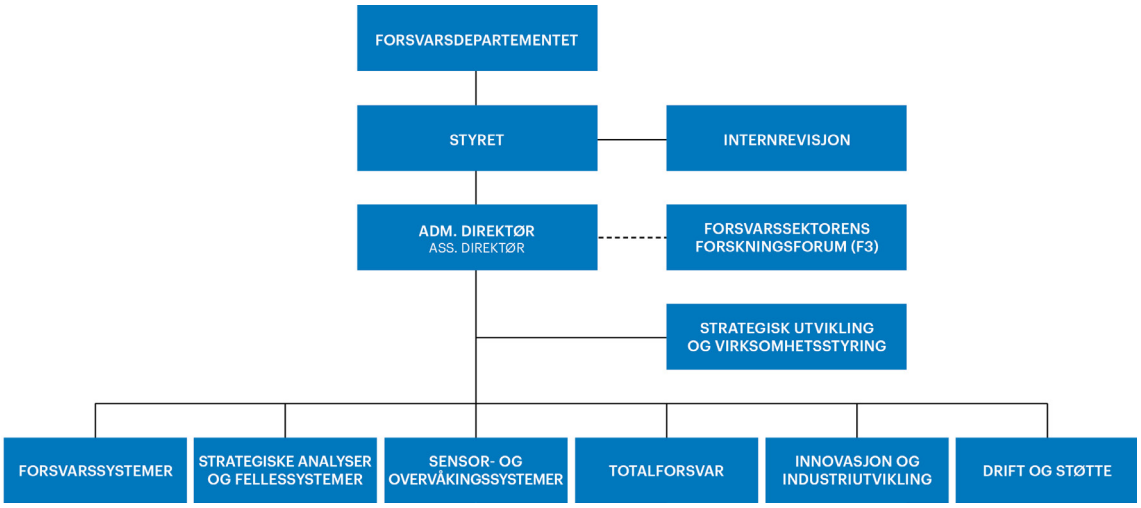
US DoD (2020): «Department of Defense 5G Strategy Implementation Plan», desember 2020.

## 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