FHS Krigsskolen

Bacheloroppgave

Mobil lavgradert enhet til bruk i Hæren

Av

Benjamin Sixten Nordén og Emil Øhre Skiaker

Levert som en del av kravet til graden:

BACHELOR I MILITÆRE STUDIER MED FORDYPNING I LEDELSE OG LANDMAKT

Antall ord: 14 752

Innlevert: MARS 2023

Godkjent for offentlig publisering

Forord

Denne oppgaven ble skrevet i perioden januar 2023 til mars 2023 som del av Bachelor i Ledelse og Landmakt ved Krigsskolen. Vi har gjennomført et teknologisk forskningsstudie som søker å utforske mulighetsrommet knyttet til C4IS, ny teknologi, samt integrasjon av sivilt materiell i militære systemer. Til hjelp i dette arbeidet har Team 5G ved Sindre Høyer Føllesdal og Håkon Eyde Kjuus vært til stor hjelp. Flere personer fra FMA har kommet med gode innspill under studiets varighet, spesielt retter vi en stor takk til systemarkitekt Johan Solli. Vi ønsker også å takke vår veileder orlogsmester Johnny Grøneng Aase ved Cyberingeniørskolen på Lillehammer for god veiledning gjennom bachelorperioden. Oppgaven kan leses av alle med interesse for teknologi og C4IS i Hæren og Forsvaret for øvrig.

Oslo, Krigsskolen, 31-03-2023

Sammendrag

Denne oppgaven omhandler C4IS i Hæren. Mer spesifikt handler den om hvordan Hæren kan ta i bruk sivil infrastruktur og teknologi på en hensiktsmessig og sikker måte. Virksomhetsprogrammet MIME i FMA skal modernisere IKT-systemer for taktisk ledelse, samt effektivisere prosessene for å implementere nye løsninger i Forsvaret. Team 5G har fått det omfattende ansvaret å utvikle konsepter og løsninger for militær anvendelse av 5G. På oppdrag fra Team 5G, har vi i denne avhandlingen søkt å besvare hvordan en 5G-kompatibel lavgradert mobil enhet kan implementeres taktisk nivå i Hæren. Oppgaven har et operativt og konseptuelt fokus, og vil ikke gå i dybden på teknisk virkemåte og spesifikasjoner utover det som er nødvendig for å forstå våre funn og konklusjoner. Metoden vi har benyttet oss av er DOTMLPFI, og vi drøfter vår problemstilling sett i lys av de ulike perspektivene Doktrine, Organisasjon, Trening, Materiell, Lederskap, Personell, Fasiliteter og Interoperabilitet. Vi har hatt til hensikt å besvare problemstillingen: *Hvordan kan en 5G-kompatibel mobil lavgradert enhet implementeres på taktisk nivå i Hæren?* For det første, bør enheten graderes BEGRENSET, for å ivareta informasjonssikkerheten, samtidig som at utveksling av informasjon kan gå begge veier. Vi har kommet fram til at en mobilenhet med 5G som bærer, tillater flyt av store datamengder, og slik bidrar til visjonen om et *Nettverksbasert Forsvar*. Videre bør en slik enhet ha et BMS, og vår anbefaling til applikasjon er Tactical Assault Kit. Formfaktoren og applikasjonen vil kunne gi avdelinger som hele- eller deler av tiden opererer til fots, et godt BMS, med muligheten til å overføre sensordata eller andre filer, samt strømme video direkte til kommandoplasser og beslutningstagere. Slik kan SA utveksles på en helt annen måte enn i dag. På kortere tid kan en få bedre situasjonsforståelse og derfor ta bedre avgjørelser, raskere. Dette kan trolig endre måten Hæren opererer, og 5G samt moderne mobilenheter, kan åpne for bruk av *Augmented Reality* for å heve kvalitet på trening, og kanskje også ytelse under skarpe operasjoner. Vår anbefaling er at en slik enhet er *modified-off-the-shelf*. Dette vil trolig medføre utfordringer knyttet til bl.a. elektromagnetisk kompatibilitet, juridiske forpliktelser og interoperabilitet. En implementering vil medføre både nye muligheter og potensielle fallgruver knyttet til bl.a. Oppdragsbasert ledelse og *Information Management.* Personellet som skal ta det nye materiellet i bruk er tilpasningsdyktige og mer teknologisk kompetente enn tidligere generasjoner, allerede før de mottar spesifikk utdanning. Elektronisk krigføring vil trolig alltid være en faktor i et moderne operasjonsmiljø, og 5G som bærer er ikke immun mot slik påvirkning. Likevel er teknologien lovende og under utvikling. En mobilenhet med TAK-programvare er allerede tatt i bruk av to av våre nærmeste allierte. Integrasjon i eksisterende

systemer er et allerede påbegynt arbeid, og fleksibiliteten i programvaren gir gode muligheter for tilpasninger i interoperabilitetsøyemed.

Innhold

Figurer:

Tabeller:

FEA – Funn – Eksisterende grunnlag – Anbefaling

Forkortelser:

2D – Todimensjonal

3D – Tredimensjonal

A2AD – Anti Access Area Denial

AIPN - All IP Network

AR – Augmented Reality

ATAK – Android Tactical Assault Kit/Android Team Awareness Kit

BMS – Battle Management System

C2 – Command and Control

C4IS - Command, Control, Communications and Computers Information Systems

CivTAK – ATAK sivil versjon

DCOTS – Commercial-off-the-shelf/Commercially available off-the-shelf

DOTMLPFI – Doktrine, organisasjon, trening, materiell, ledelse, personell, fasiliteter, interoperabilitet

EK – Elektronisk krigføring

FAF – Fremtidige anskaffelser til Forsvarssektoren

FDLO – Forsvarets doktrine for landoperasjoner

FFI – Forsvarets Forskningsinstitutt

FFOD – Forsvarets fellesoperative doktrine

FMA – Forsvarsmateriell

GPS – Global Positioning System

HF – High Frequency

HUD – Heads-Up-Display/Head-Up-Display

HV – Heimevernet

IKT – Informasjons- og kommunikasjonsteknologi

IMT – International Mobile Telecommunications

IoT – Internet of Things

ITU-R – International Telecommunication Union Radiocommunication Sector

JCIDS – Joint Capabilities Integration Development System

K2 – Kommando og kontroll

K2IS – Kommando og kontroll informasjonssystemer

LOS – Line of Sight

LTE – Long-Term Evolution

MIMO – Multiple-Input Multiple-Output

MOTS – Modified-off-the-shelf

MRR – Multirolleradio

NATO – North Atlantic Treaty Organization

NorBMS – Norwegian Battle Management System

NORCCIS – Norwegian Command and Control Information System

NSM – Nasjonal sikkerhetsmyndighet

OBL – Oppdragsbasert ledelse

OJT – On the Job Training

OODA – Observe – Orient – Decide - Act

SA – Situational Awareness

SHF – Super High Frequency

SNR – Signal to Noise Ratio

SOP – Standing Operating Procedures/Standard Operating Procedures

TAK – Tactical Assault Kit

TCP-IP – Transmission Control Protocol/Internet Protocol

TKI – Taktisk kommunikasjonsinfrastruktur

TTP – Taktikk, teknikker og prosedyrer

UHF – Ultra High Frequency

VHF – Very High Frequency

Win-TAK – TAK for Windows

1 Innledning

Få menneskelige aktiviteter har hatt like stor påvirkning på teknologisk utvikling som krig. Helt fra den mest primitive våpenteknologi til nåtidens sofistikerte presisjonsvåpen, har krig og teknologisk utvikling stått i et gjensidig avhengighetsforhold. Krigen er, og kommer trolig til å fortsette å være, en pådriver for utvikling og innovasjon, på samme måte som teknologi i stor grad legger premissene for morgendagens taktikk og operasjonskunst. Til alle tider har kommunikasjon og situasjonsforståelse vært en utfordring på slagmarken, og den troppeføreren med best forståelse for situasjonen, har hatt et betydelig fortrinn ovenfor sin motstander.

I lange tider handlet militærteknologisk utvikling hovedsakelig om å utvikle bedre og mer dødelige våpen enn sine motstandere, eller utvikling av funksjoner som direkte effektiviserte og understøttet måten man førte krig på. Slik er det også i dag, men i tillegg til utvikling og videreutvikling av ulike effektorer i det fysiske domenet, har rivende teknologisk utvikling påvirket operasjonsmiljøet på en rekke måter, bl.a. gjennom å åpne døren til nye domener. NATO anerkjente i 2016 Cyberspace som et eget operasjonsdomene, på lik linje med bl.a. land-, sjø-, og luftdomenet, og fastslo samtidig at et angrep i cyberdomenet kan være like skadelig for et moderne samfunn som et konvensjonelt angrep (NATO, 2016).

Spesielt innenfor informasjonsteknologi har en revolusjon funnet sted. Dette har påvirket militære styrker på mange måter. Mest relevant for denne oppgaven, vil det være å se informasjonsteknologi i sammenheng med Kommando og kontroll (K2). Dette begrepet kan ses på som synonymt med ledelse av operasjoner (Forsvarets Stabsskole, 2007, s. 128). Begrepet inneholder riktignok også alt som muliggjør ledelse av operasjoner: «K2 består av den organisasjonen, de prosessene, prosedyrene, systemene og det lederskapet som gjør militære sjefer i stand til å lede og kontrollere sine styrker.» (Forsvarets Stabsskole, 2007, s. 128). Gitt skalaen og kompleksiteten på dagens stridsfelt sier det seg selv at det er umulig å opprettholde kontroll, og ta beslutninger uten støtte fra informasjonsteknologi. Striden ledes ikke lenger fra hesteryggen eller fra nærmeste ås, men fra høyteknologiske kommandoplasser eller mobile plattformer. Her skal en rekke ulike systemer gi sjefer og staber på alle nivåer god nok SA (Situational Awareness), til å ta riktige beslutninger basert på et korrekt bilde av situasjonen. De samme systemene gjør det også mulig for ledere på lavere nivå å sitte på et mer komplett bilde av situasjon, egne og fienden i tid og rom. Hensikten er alltid å utøve hurtigere og bedre K2 enn fienden (Forsvarets Stabsskole, 2007,

s. 128). En har altså blitt helt avhengig av støtte fra høyteknologisk informasjonsteknologi, både i forberedelser til- og gjennomføring av moderne operasjoner (Forsvaret, 2019, s. 138). Følgelig bør K2-strukturer fasilitere for sikker, klar og rask formidling av ordre, situasjonsoppdateringer og annen viktig informasjon (NATO, 2022, s. 49). Kanskje finnes det verktøy som i nær fremtid kan gjøre K2 og utveksling av SA til en lettere oppgave for ledere i Hæren?

1.1 Bakgrunn

På fagkurs i regi av HSB/Sambandsskolen ble vi introdusert for militær anvendelse av 5G, og det pågående arbeidet med å bygge ut 5G-dekning i Norge. Fra før kjente vi til at 5G, eller femtegenerasjons mobilteknologi, ville kunne by på høyere hastigheter og større kapasitet enn tidligere generasjoner, for den gjennomsnittlige bruker. Det vi derimot ikke kjente til var hvilket potensiale 5G har for militær anvendelse. Et nettverk som baserer seg på landsdekkende sivil infrastruktur, men som lett kan bygges ut med mobile basestasjoner, som har rikelig kapasitet og hastighet for overføring av data i sanntid. Det vil også bli mulig for Forsvaret å få sin egen skjermede del (skivedeling) av det sivile 5G-nettet, samtidig som det er mindre sårbart mot Elektronisk krigføring enn eksisterende teknologi. Dette vil kunne utgjøre en liten revolusjon for K2IS i Forsvaret. MIME er et virksomhetsprogram i Forsvarsmateriell som skal «modernisere informasjons- og kommunikasjonssystemene for taktisk ledelse i Forsvaret» i tillegg til å effektivisere anskaffelse og implementering av det de kaller «kampnær IKT» (Forsvarsmateriell, 2020). En del av dette arbeidet går ut på å utforske muligheter knyttet til anvendelse av kommersielle produkter og teknologi som er «commercial-off-the-shelf» (hyllevare), i tråd med *Hybridkonseptet* (Forsvarsmateriell, 2022). «Det er ikke detaljert nøyaktig hvordan ulike teknologier skal benyttes av ulike typer brukere i ulike typer operasjoner; Team 5G skal derfor utforske og verifisere funksjonalitet i kommersiell 5[G]-teknologi for å finne ut hvor og på hvilken måte denne kan og bør benyttes i Forsvaret.» (Forsvarsmateriell, 2022). Et av mange spørsmål de ønsker svar på i den sammenheng er hvordan en 5G-kompatibel lavgradert mobil enhet eller mobiltelefon, kan og bør implementeres på taktisk nivå i Hæren, og hva dette vil kreve.

1.2 Problemstilling

Denne oppgaven skal besvare følgende problemstilling:

Hvordan kan en mobil lavgradert enhet med 5G som bærer implementeres på taktisk nivå i Hæren?

1.3 Avgrensninger og forutsetninger

Vi har valgt å avgrense oppgaven vår til å omhandle forsvarsgrenen i landdomenet, mer spesifikt Hæren i det norske Forsvaret. Dette valget har vi gjort på bakgrunn av at vi begge har avtjent verneplikt i Hæren, at utdanningen vår er rettet mot ledelse i landdomenet, og at vi begge er kommende sambandsoffiserer i Hæren. Problemstillingen vi har valgt kunne sannsynligvis vært gjenstand for et langt mer omfattende forskningsprosjekt enn en bacheloroppgave tillater. Det er svært mange perspektiver som må tas i betraktning når en utforsker muligheter og begrensninger rundt innføring av ny teknologi, og kanskje spesielt IKT. Vi ser det som hensiktsmessig å berøre et utvalg aspekter grundig, i stedet for å berøre veldig mange overfladisk. Som kadetter på operativ linje uten teknisk utdannelse, er det grenser for hvor dypt ned i det tekniske vi er i stand til å dykke. Oppgaven vil derfor utforske et utvalg problemer på et konseptuelt og generelt nivå, men samtidig holde det så konkret og håndfast som mulig. Av hensyn til dette har vi lagt forutsetninger til grunn og gjort avgrensninger som beskrevet i de neste to avsnittene.

Den mobile enheten vi ser for oss vil være en mobil enhet, dvs. en smarttelefon eller et nettbrett tilgjengelig på det åpne markedet (Commercial-off-the-shelf, eller Modified-off-the-shelf) med kompatibilitet for 5G stand-alone (5G SA). Utover dette vil vi ikke gå videre inn på hvilken produsent som bør levere enheten, hvilke tekniske spesifikasjoner enheten bør ha, eller hvilken modell enheten bør være. I skrivende stund er 5G SA ikke tilgjengelig i Norge, men vil trolig innen kort tid lanseres av kommersielle teleoperatører. Vi legger til grunn at dette vil bli tilgjengelig i fremtiden og vil ha landsdekkende dekning. I tillegg, forutsetter vi at Forsvaret blir tildelt en egen, skjermet del (*slice*, eller skivedel) av dette nettverket. Videre, forutsetter vi at Hæren vil ha tilgang på egne mobile basestasjoner som kan opprette *lokale* dekningsområder på noen få kilometer etter behov, men at en hovedsakelig baserer seg på å anvende kommersiell 5G-dekning. Enheten vil ha SIM-kort som støttes av militær *slice*. Avslutningsvis vil enheten være *lavgradert*, og med det mener

vi UGRADERT eller BEGRENSET. Hvilken gradering enheten bør ha vil vi drøfte på et senere punkt i oppgaven.

Vi har avgrenset oss til å se på hvordan mobilenheten kan implementeres på taktisk nivå i Hæren, dvs. patrulje/lag, tropp og kompani. Det er også nødvendig å se på samspillet mellom systemer på dette nivået og høyere nivå. Videre vil vi hovedsakelig undersøke hvordan *denne* enheten kan implementeres og bør fungere, og vi vil kun gi enkle beskrivelser av andre sambandssystemer for å ha noe å sammenligne med, og kunne diskutere fordeler og ulemper. Av applikasjoner/programvare enheten bør ha, kommer vi kun til å forholde oss til Tactical Assault Kit (TAK). Vi har gjennom prosjektperioden fått praktisk kjennskap til ATAK-CIV (sivil utgave). Funksjonalitet utover denne applikasjonen vil kun beskrives dersom det er relevant for det aktuelle drøftingsspørsmål. Metoden eller forskningsdesignet får sitt eget kapittel, men vi har valgt å diskutere ett til to spørsmål knyttet til hver kategori i metoden, grunnet tid til rådighet, ressurser tilgjengelig og for ikke å overstige den maksimale lengden på oppgaven.

1.4 Styrker og svakheter ved oppgaven

Å skulle vurdere reliabilitet og validitet ved metoden er utfordrende, da vi ikke har gjort forsøk og samlet inn data i så måte, men brukt egne observasjoner og teori som grunnlag for drøfting. For det andre besvarer vi i oppgaven hypotetiske spørsmål knyttet til anskaffelse av et produkt som det, så vidt vi vet, ikke foreligger noen planer om å gå til anskaffelse av. Vi har drøftet de ulike punktene i DOTMLPFI, og forsøkt å finne drøftingsspørsmål knyttet til hvert punkt som det sett med Hærens øyne vil være viktig å kunne besvare før en eventuell anskaffelsesprosess. For å ikke overstige grensen på oppgavens lengde, og for å vie alle kategoriene nok oppmerksomhet har vi begrenset oss til maksimalt to drøftingsspørsmål per kategori i DOTMPLFI. Dette er også fordi vi vurderer det som mer nyttig å gå i dybden på ett eller to spørsmål, i stedet for å besvare flere spørsmål overfladisk.

Kildegrunnlaget er mangfoldig, og spenner fra doktriner og andre kjente og pålitelige publikasjoner, til artikler funnet på internett. Kildekritikk har derfor vært viktig. Det er flere reglementer og førende dokumenter som kunne vært interessante for oss å anvende i oppgaven, men vi har valgt å begrense oss til ugraderte kilder, og skrive en UGRADERT oppgave. Dette har utelukket flere viktige publikasjoner som kunne ha bidratt til håndfasthet og faglig tyngde - dette ser vi på som en svakhet ved oppgaven.

Det forskes mye på hvordan Forsvaret og Hæren kan bruke 5G, men så vidt oss bekjent, har lite arbeid så langt vært gjort for å se på praktiske problemstillinger knyttet til implementering og anskaffelser, og hva doktrine, organisasjon, trening osv. har å si i dette arbeidet. Vi ser på det at vi ikke undersøker noe mange har gjort før oss, men at vi undersøker noe dagsaktuelt og fremtidsrettet, som en styrke ved oppgaven. DOTMLPFI som metode favner bredt, samtidig som den er et oversiktlig og forholdsvis enkelt analyseverktøy. Dette ser vi på som en styrke, at metoden er omfattende nok, men samtidig enkel å forholde seg til. Videre, ser vi på samarbeidet med Team 5G som en styrke for oppgaven, og at vi i forbindelse med Øvelse Jøssing fikk mulighet til å se fungerende prototyper av teknologien vi skriver om, tatt i bruk av militære styrker. Dette ga inspirasjon, økt forståelse og ikke minst noen nyttige observasjoner.

2. Metode

Dette kapittelet beskriver den metodiske fremgangsmåten vi har benyttet oss av i studien, hvordan oppgaven er strukturert, samt hvordan vi har samlet inn empiri til prosjektet.

2.1 Forskningsdesign DOTMLPFI (Doktrine, organisasjon, trening, materiell, ledelse, personell, fasiliteter, interoperabilitet)

Vi kommer til å benytte oss av forskningsmetoden DOTMLPFI, et analyseverktøy som bl.a. benyttes i militær sammenheng når man har identifisert et kapabilitetsbehov. Analysemetoden er sett i sammenheng med anskaffelse av nytt materiell til forsvarssektoren, og tar for seg de viktigste aspektene som må tas i betraktning når kapabiliteter skal utvikles eller anskaffes. Opprinnelig stammer metoden fra JCIDS (Joint Capabilities Integration Development System) (JCIDS, 2012) da kjent under akronymet DOTMLPF. I NATO har man lagt til en «I» i akronymet, for «interoperabilitet» (Kucukaksoy, 2016). Det er NATO sin standard vi kommer til å følge som metode og verktøy for drøfting og besvarelse av vår problemstilling. (Gyllensporre, Hellebjerg , Takanen, & Sundseth , 2012)

2.2 Struktur

I oppgaven kommer vi innledningsvis til å redegjøre for relevant militærteori og ledelsesteori. Deretter vil vi redegjøre for Hærens organisasjon og rolle, samt operasjonsmiljøet og konteksten Hæren skal operere i, før vi kort forklarer visjonen om et Nettverksbasert Forsvar og redegjør for Forsvarsdepartementets satsningsområder. Etter dette går vi inn på 5G som begrep, teknologien i 5G, Nasjonal Sikkerhetsmyndighet sine sertifiseringskrav, samt kryptografi, anskaffelsesprosessen, og sist, men ikke minst programvaren Tactical Assault Kit. Teorien legger grunnlaget for neste del, hvor vi drøfter problemstillingen sett i lys av hver kategori i DOTMLPFI (Doktrine, Organisasjon, Trening, Materiell, Ledelse, Personell, Fasiliteter og Interoperabilitet). Avslutningsvis vil vi oppsummere drøfting og delkonklusjoner før vi kommer med vår konklusjon og anbefaling.

2.3 Metodebeskrivelse

DOTMLPFI som analyse er noe som i utgangspunktet skal gjennomføres for alle anskaffelser i forsvarssektoren. Metoden kan bidra til å identifisere utfordringer knyttet til doktrine, organisasjon, trening, materiell, ledelse, personell, fasiliteter og interoperabilitet, slik at disse kan løses før anskaffelsen gjennomføres. Metoden gjør det mulig å identifisere hvilke konsekvenser en anskaffelse og implementering, som den vi beskriver i problemstillingen, sannsynligvis vil ha. Metoden tar for seg de ulike kategoriene hver for seg, og som en helhet. Dette sørger for at man får et bredt spekter med mulige løsninger før man starter anskaffelsesprosessen. Ved undersøkelse av hver enkelt kategori selvstendig gjør dette at man potensielt får belyst flere aspekter.

2.4 Datainnsamling

Taktisk 5G og bruk av COTS-enheter til militær bruk, er i skrivende stund kun på prototype- og konseptutprøvings-stadiet. Årsaken er at 5G som kommunikasjonsbærer fortsatt er under utvikling, og konsept for bruk av nettverket enda ikke er utarbeidet. Testing i Forsvaret av 5G gjennomføres av FFI og FMA på et konseptuelt nivå. Det er derfor vanskelig å tilrettelegge for flere tilfeller av deltakende observasjon i den korte bachelortiden vi har til rådighet. Vi kommer derfor til å basere empirien vår på observasjoner gjort ifm. øvelse Jøssing i Stavanger, samt øvelse Joint Viking 23. Et av hovedmomentene ved øvelse Jøssing er testing av taktisk 5G som kommunikasjonsbærer. Metoden vi har benyttet oss av for

innsamling av data er deltakende observasjoner (Johannessen, Tufte , & Christoffersen , 2010).

2.5 Kildegrunnlag

Av doktriner og andre førende publikasjoner, har vi valgt å forholde oss hovedsakelig til Prop. 14 S (2020-2021) - Langtidsplan for Forsvarssektoren, FFOD 2019, Morgendagens Hær, og Forsvarets grunnsyn på ledelse. Forsvarets doktrine for landoperasjoner (FDLO) ville vært naturlig å henvise til, men siden denne ikke har blitt oppdatert siden 2004 ser vi det som lite hensiktsmessig. Den teknologiske utviklingen går stadig raskere, og begreper, konsepter og prosedyrer fra to tiår tilbake vil ha begrenset relevans i dag. Videre vil vi drøfte på grunnlag av kildegrunnlag fra åpne kilder, men om mulig bruke elementer fra reglementer og publikasjoner som i sin helhet er BEGRENSET. Vi vil ikke gjengi detaljer som gjør at denne oppgaven får høyere gradering enn UGRADERT. Øvrige kilder vi henviser til vil være artikler og kilder fra internett. Disse er funnet gjennom søkemotorene Google, Google Scholar, og ved anbefalinger fra fagpersoner innenfor gitt felt. Søkeordene som er brukt er eksempelvis: 5G, military use of 5G, ATAK. Vi vil i tillegg bruke empiri basert på egne observasjoner der dette er relevant.

3. Teori

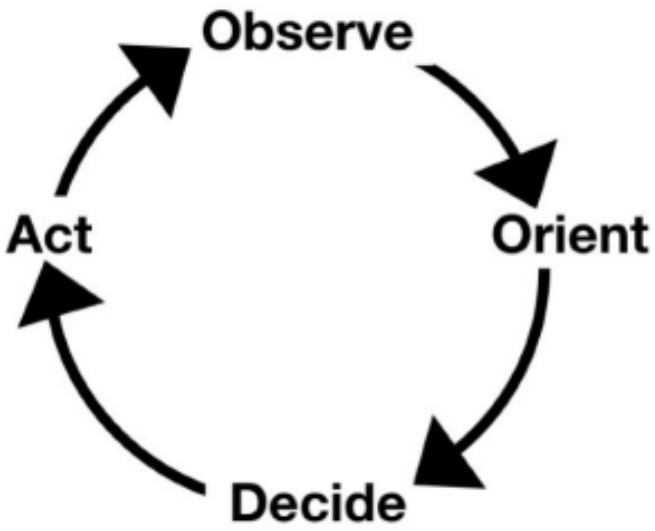
3.1 Doktrine

Et meget kjent sitat, som er grunnleggende for vår forståelse av krig, er: «War, is thus an act of force to compel our enemy to do our will» (Clausewitz, 1976, p. 75). FFOD legger et Clausewitzisk syn på krigens natur til grunn, dette innebærer at krigens *natur* anses som konstant, mens krigens *karakter* alltid utvikler og forandrer seg (Forsvaret, 2019, s. 19). Momenter som usikkerhet, fare og fysisk utmattelse er alltid tilstede i strid, og vil sinke og vanskeliggjøre operasjoner, og det er disse m.fl. som utgjør det vi kaller *friksjon* (Forsvaret, 2019, s. 19). Friksjonens tilstedeværelse stiller høye krav til lederskap, erfaringsnivå og høy treningsstandard som virker å være de eneste reelle motmidlene (Forsvaret, 2019, s. 19). Det er under slike forhold Forsvaret og Hæren skal kunne operere.

3.1.1 OBL og OODA-loop

Hærens operasjonskonsept preges av en *manøvertankegang* (Forsvaret, 2019, s. 103). En forutsetning for en manøverorientert måte å føre krig på, er en ledelsesfilosofi som fasiliterer for operasjonelt tempo, overraskelse, ildkraft og å målrettet angripe motstanderens vilje i stedet for hans evne. I Norge har vi valgt oppdragsbasert ledelse (OBL) som vår ledelsesfilosofi (Forsvaret, 2020, s. 13). OBL innebærer kort oppsummert at sjefer formidler en ønsket sluttilstand/mål, en *hensikt* og metode, for deretter å overlate *hvordan* oppdraget i detalj skal løses til sine undergitte (Forsvaret, 2020). Det er likevel vanlig å gi *bindinger* (skal gjøres) og *begrensinger* (skal ikke gjøres) som rammer for utførelsen. Denne friheten til å velge fremgangsmåte forutsetter stor grad av tillit mellom nivåer og en grundig forståelse av egen sjefs intensjon. I tillegg må ledere på alle nivå evne å tenke selvstendig og ta initiativ, og i tillegg våge å trosse egen sjef dersom dette er det som vil tjene hans intensjon best. Ledere på lavt nivå er som regel de som sitter med den mest komplette og oppdaterte situasjonsforståelsen, og i det situasjonen endres betydelig, tilsier det ofte at egen plan må endres eller tilpasses. Dette muliggjøres gjennom OBL, ved at en har muligheten til å gripe muligheter som oppstår på slagmarken, selv om dette måtte bryte med opprinnelig plan. Så lenge en handler innenfor rammen av sjefens intensjon, og kan argumentere for hvorfor, kan en justere og tilpasse egne planer uten å måtte bruke verdifull tid på å få godkjennelse fra høyere nivå. Gitt krigens natur kan man ikke regne med å alltid ha forbindelse med sjef eller høyere nivå, selv om det er ønskelig med effektiv K2. OBL er en robust ledelsesfilosofi: Så lenge sjefens intensjon er forstått, vil en alltid kunne handle på grunnlag av denne, selv uten samband og langt fra andre egne.

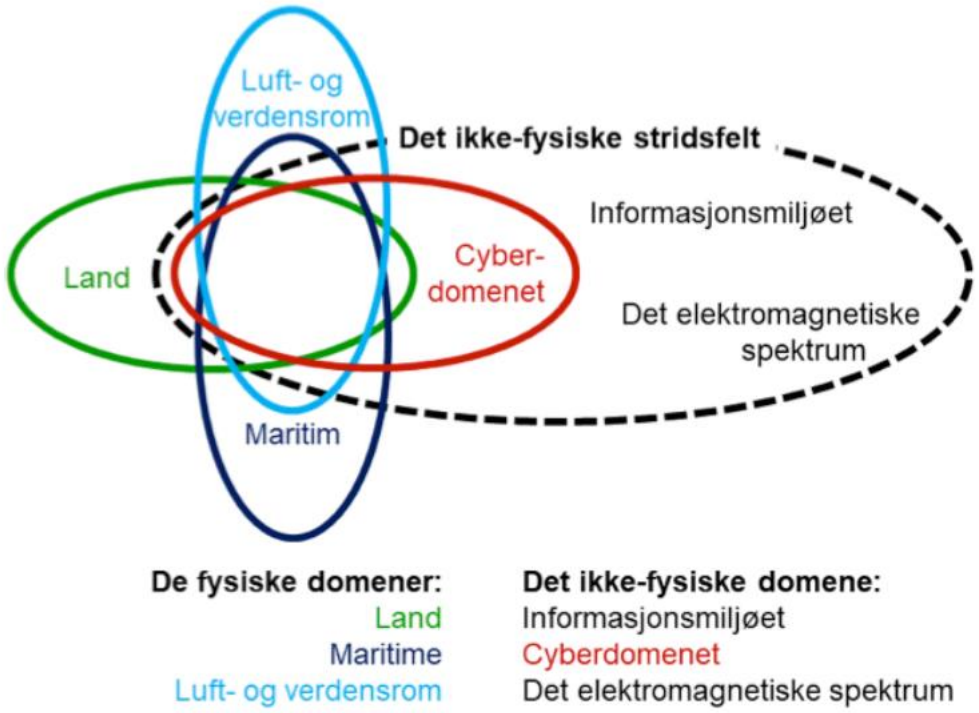
Med vårt manøverorienterte syn på landmakten og vår ledelsesfilosofi er evnen til å føre operasjoner med høy grad av overraskelse og tempo svært viktig. Her kommer Boyds OODA-loop inn i bildet. Opprinnelig ble den utviklet av den amerikanske jagerflypiloten John Boyd. Boyd innså senere at lignende tenkemåter kan spores helt tilbake til antikken og Sun Tzu (Richards, 2020). Siden har OODA-loopen blitt en omdiskutert del av militærteorien, som har blitt tolket på mange forskjellige måter. Den mest populære tolkningen av Boyds OODA loop er at trinnene *Observe, Orient, Decide* og *Act*, er trinn som utføres i sekvens og så raskt som mulig, om igjen, og om igjen gjennom en operasjon, og at den som klarer dette raskest vil oppnå et større og større overtak (Richards, 2020, s. 3). OODA-loopen er eksemplifisert i Figur 1.



Figur 1: OODA loop (Richards, 2020)

3.1.2 Operasjonsmiljøet

Operasjonsmiljøet kan deles inn i ulike domener. De fysiske domener er landjorda, sjøen, og luft- og verdensrom, mens de ikke-fysiske domer er cyberdomenet, informasjonsmiljøet og det elektromagnetiske spektrum, se for øvrig Figur 2 (Forsvaret, 2019, ss. 21-22). Egen evne til å dele, analysere og beskytte store datamengder er i økende grad noe militære styrker søker å utvikle, fordi det kan gi så enorme utslag i egen kampkraft (Forsvaret, 2019, s. 25). Dette fører til at Cyberdomenet får en stadig mer fremtredende rolle: «For å etablere en felles situasjonsforståelse, utøve kommando og kontroll og benytte plattformer, sensorer og effektorer effektivt, er de militære styrkene avhengig av aktivitet i, fra eller gjennom cyberdomenet.» (Forsvaret, 2019, s. 25).



Figur 2: Operasjonsmiljøet (Forsvaret, 2019, s. 22)

3.1.3 Nettverksbasert Forsvar

En fellesnevner for konseptuell og doktrinell utvikling til nå, har vært at forbedret- og ny teknologi tilpasses tradisjonelle operasjonskonsepter og innføres stegvis, i den hensikt å forbedre og effektivisere dem (Beadle & Diesen, 2015, s. 41). I takt med at teknologisk utvikling fortsetter å akselerere, kan dette være i ferd med å endre seg: «Militærteknologisk vil utviklingen de neste 10–20 år trolig preges av at spesielt informasjonsteknologien vil endre militære organisasjoner og operasjonskonsepter.» (Beadle & Diesen, 2015, s. 41). For å forstå nåtidens og fremtidens trusler, kommer vi ikke utenom begrepet Anti-Acces, Area Denial (A2AD). Begrepet er komplekst, og omfatter mer enn kun det militære. Kort oppsummert beskriver *Morgendagens Hær* det slik: «A2AD består av flere lag av fysiske og politiske tiltak som i sum skal hindre tilgang til-, eller nekte evnen til å operere i et gitt område. Ettersom trusler eksisterer i alle krigføringens domener, omfatter A2AD også evne til nektelse i de samme domenene.» (Forsvaret, 2021, s. 7). Ifølge Beadle og Diesen, kan vi se for oss at utvikling på spesielt tre områder kan føre til de største omveltningene:

A. Sofistikert sensorteknologi, med påfølgende forbedring av *SA*.

B. IKT-systemer med høy båndbredde og simultankapasitet, som i sanntid deler informasjon til samtlige enheter i et nettverk.

C. Langtrekkende og presise, fellesoperative effektorer kan bekjempe mål på tvers av troppearter, forsvarsgrener og domener, i hierarkiske strukturer.

Dette er bl.a. kjent som *nettverkssentrisk krigføring* og har lenge vært diskutert i teorien, men mange har konkludert med at teknologien har vært for umoden. i FFOD 2019 har man konseptualisert denne tenkemåten i begrepet *Nettverksbasert Forsvar* som: «[…] nettverkstenkningen som handler om å utvikle både mennesker, organisasjon og teknologi med et mål om å organisere ressursene mest mulig effektivt for å oppnå en størst mulig effekt av de ressursene som settes inn gjennom systemintegrasjon, situasjonsbevissthet og forståelse av sjefens intensjon.» (Forsvaret, 2019, s. 242).

3.2 Hæren

3.2.1 Hærens organisasjon

Hæren er organisert på en tradisjonell hierarkisk måte, fra lavest til høyest: lag/patrulje – tropp – kompani/batteri/eskadron – bataljon – brigade/regiment (Leraand, 2022). Denne måten å organisere en hær på har lange tradisjoner. Med taktisk nivå menes nivået under strategisk og operasjonelt nivå og over stridsteknisk nivå. FFOD 2019 beskriver det taktiske nivå som: «Anvendelse av militære styrker for å utføre oppdrag for å nå militære målsettinger.» (Forsvaret, 2019, s. 251). I Norge er det nivåene under Forsvarets operative hovedkvarter som utgjør det taktiske nivå (Forsvaret, 2019, s. 251). Dette vil i praksis si brigadenivået (eksempelvis Brigade Nord eller Finnmark Landforsvar) og i noen tilfeller bataljonsnivået.

3.2.2 Hærens rolle

Forsvarets oppgaver er mange og komplekse. Forsvaret skal bl.a.:

«1. Sikre troverdig avskrekking med basis i NATOs kollektive Forsvar.

2. Forsvare Norge og allierte mot alvorlige trusler, anslag og angrep, innenfor rammen av NATOs kollektive forsvar.

3. Avverge og håndtere episoder og sikkerhetspolitiske kriser med nasjonale ressurser, herunder legge til rette for alliert engasjement

[…]

5. Hevde norsk suverenitet og suverene rettigheter» (Det Kongelige Forsvarsdepartement, 2020, s. 11).

Hærens rolle i dette komplekse bildet kunne vært gjenstand for en egen avhandling. Likevel er det noen betraktninger en kan trekke ut på generelt grunnlag. Det er slik at vi lever mesteparten av våre liv på landjorda, og det er her de fleste av verdiene vi ønsker å forsvare befinner seg, som naturressurser, produksjonsanlegg og ikke minst samfunnene mennesker har etablert (Forsvaret, 2019, ss. 22-23). En forutsetning for å kunne operere på landjorda, og fylle rollene beskrevet over, er K2IS som tilrettelegger for størst mulig kampkraft med ressursene vi har.

3.3 Forsvarsdepartementet satsingsområder

Som tidligere nevnt, er MIME (ikke en forkortelse, norrøn gud for visdom og kunnskap) et virksomhetsprogram i FMA (Forsvarsmateriell). MIME har ansvar for å modernisere taktiske kommunikasjons- og informasjonssystemer for ledelse, samt effektivisere prosesser knyttet til anskaffelse og implementering av nye løsninger og systemer (Forsvarsmateriell, 2020). I Regjeringens plan for fremtidige anskaffelser til Forsvarssektoren (FAF) 2022-2029 beskrives bl.a. MIMEs aktivitet i perioden. Mellom 3 og 4,5 milliarder kroner er planlagt investert i «taktisk ledelsessystem for landdomenet», slik at en: «[…] opprettholder, moderniserer og forbedrer evne til effektiv ledelse og utnyttelse av Forsvarets styrkestruktur på taktisk og stridsteknisk nivå i landdomenet.» (Forsvarsdepartementet, 2022, s. 30). Dette ledelsessystemet vil, som vi allerede har vært inne på, i fremtiden bestå av både militær teknologi og sivil hyllevare slik *Hybridkonseptet* dikterer. Investeringene skal hovedsakelig gå til IKT med software og hardware som: «[…] danner en taktisk informasjonsinfrastruktur av mobile og deployerbare nettverkselementer som gir evne til å utøve effektiv kommando og kontroll.» (Forsvarsdepartementet, 2022, s. 30).

Denne taktiske kommunikasjonsinfrastrukturen (TKI) eksisterer allerede, og summen av kommunikasjonsbærere, materiell og tjenester kalles Army C4IS (Forsvaret, 2021, s. 40). Bærere som kan anvendes i dag er bl.a. radiolinje på SHF- og UHF-frekvenser, kablet internett eller 4G/Long-term evolution (LTE) (Forsvaret, 2021, s. 40). Det er fordeler og ulemper med de eksisterende bærerne. Radiolinje-samband har begrenset bitrate, rekkevidde og er avhengig av line of sight (LOS). Samtidig er ikke radiolinjesamband avhengig av sivil infrastruktur, og kan derfor etableres og brukes selv om all sivil infrastruktur skulle være ødelagt i et område. 4G/LTE har god bitrate, dekning i stort sett hele fastlands-Norge, og signalet svekkes ikke nevneverdig av bygninger, vegetasjon osv. Ulempen er at 4G-dekning skapes av sivile basestasjoner, spredd rundt i hele landet. Forsvaret har ingen råderett over

nettverket, og basestasjonene er sårbare for sabotasje. Som vi skal se i neste delkapittel, kan 5G løse mange av problemene og begrensningene vi opplever i dag.

3.4 Femtegenerasjons mobilnettverk (5G)

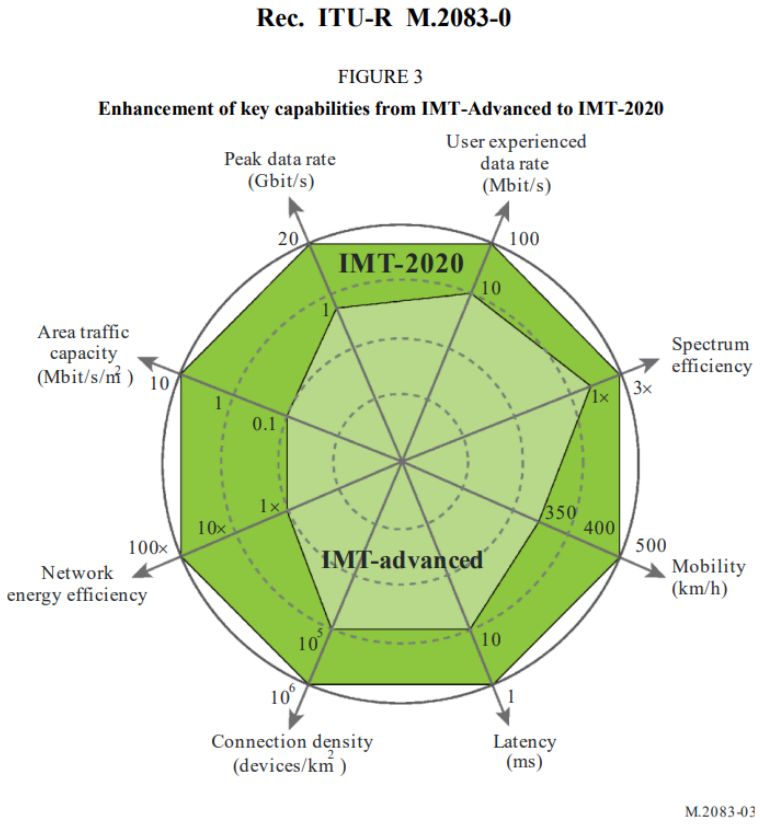
Det er sentralt å forstå begrepet 5G i oppgaven vår. Derfor er det på sin plass med en grunnleggende forklaring av begrepet, hvilke muligheter dette nettverket tilbyr, og hva som utgjør den største forskjellen sammenlignet med tidligere mobilnettverk. I det følgende kapittel vil vi derfor avklare utviklingen innenfor kommersiell mobilteknologi, introdusere de største fordelene og ulempene ved 5G, og forklare operativ bruk av 5G.

5G teknologien baserer seg på en sammensetting av flere ulike teknologier. Dette innebærer at oppgradering og utvikling skjer på flere arenaer, som for eksempel frekvensbånd, kostnad og forsinkelse for å nevne noen (Voldhaug , et al., 2021, s. 15). Sammenlignet med tidligere mobilnett er mulighetene mange både sivilt og militært. Den sivile teknologien ligger i dag flere steg foran militærteknologien, og det er av den grunn viktig med integrering av sivil teknologi i krigføringen, spesielt innenfor IKT. Mulighetene er mange, særlig innenfor mobilnett når det gjelder kommunikasjon.

I dag er den mest utbredte mobilteknologien 4G. Teknologien tilbyr relativt god overføringshastighet på minst 10Mbit/s ifølge IMT-advanced (ITU-R, 2015). 4G som vi benytter oss av i dag er et såkalt All IP Nettverk (AIPN-nettverk) noe som indikerer at det benytter seg av lik kommunikasjonsform som internett, Transmission Control Protocol/Internet Protocol (TCP-IP). Dette betyr at 4G egentlig ikke er noe annet enn en rask trådløs internettilkobling, som brukes på lik linje med det vi er kjent med fra kablet internettilkobling (Valle, 2009). I utgangspunktet er 4G altså er tilstrekkelig for den jevne forbruker. Dette er dokumentert av Telia, etter at 5G NSA ble lansert i Norge 2020 (Vellan, 2020). Selv om det vi har i dag er godt nok går utviklingen innenfor IKT svært raskt. 5G er derfor fremtidens mobilnettverk med de muligheter dette bringer teknologisk.

Kravene til 5G nettverket er utstedt av International Telecommunication Union Radiocommunication Sector (ITU-R) i deres visjon International Mobile Telecommunications-2020 (IMT-2020). I rapporten er kravene listet som 8 punkter. FFI har definert disse innenfor tre ulike dimensjoner. Dette er *høye overføringshastigheter*, *mange enheter* og *ultrapålitelig nettverk med lav forsinkelse* (ITU-R, 2015, s. 14) (Voldhaug , et al., 2021, ss. 16-18). Figur 3 illustrerer forskjellene fra 4G til 5G teoretisk sett ut ifra

visjonene til ITU. Ut ifra figuren kan man se at alle kategoriene *effektivitet, arealkapasitet, avstand, hastigheter, pålitelighet* og *forsinkelse* forbedres. Figuren er ikke lineær, men hvert steg innebærer en 10-dobling. Størst forskjell er det i kategorien nettverkeffektivitet og arealkapasitet, begge med en teoretisk endring på 100x. Økningene er forårsaket av nye teknologier, samt utvikling av nåværende teknologi.



Figur 3: Teoretiske forskjeller mellom 4G og 5G (ITU-R, 2015)

3.4.1 Teknologiene i 5G

Vi skal videre forklare teknologien som gjør det mulig med de teoretiske mulighetene eksemplifisert over.

En av de nye teknologiene som er introdusert ved 5G er ny radioteknologi. Denne er brukt på den trådløse forbindelsen mellom basestasjon og brukerutstyret og heter 5G New Radio (NR). Sammenlignet med 4G bruker 5G NR flere frekvensområder. I kombinasjon med ny moderne antenneteknologi, slik som Massive MIMO, fasiliterer disse i kombinasjon for høyere overføringshastigheter.

3.4.1.1 Massive MIMO

Massive *multiple-input and multiple-output* (MIMO) er en antenneteknologi som betyr at antennen på basestasjonen er sammensatt av flere antenner i gruppe som virker for å kunne sende og motta flere signaler samtidig. Det er uansett viktig å forstå at denne type antenneteknologi kun muliggjør de store hastighetene ved korte avstander mellom basestasjon og brukerutstyret (Voldhaug , et al., 2021).

Nåværende antenneteknologi kalles for MIMO, og benytter seg av opptil 8 antenner, fire for sending og fire for mottak. Ved oppgraderingen Massive MIMO vil antennene til sending/mottak oppgraderes til inntil 64+64. Denne utvidelsen gjør at man i 5G nettverket kan forme antennediagrammet, og derav har større muligheter til å tilpasse signal etter behov. Sammenlignet med tidligere antenneteknologier har man nå muligheten til å styre følsomhet i en gitt retning. Teknologien som brukes i Massive MIMO er på en måte ikke helt ny, det er bruken av teknologien i storskala til mobilnett som er ny (Vellan, 2020).

3.4.1.2 Stråleforming

For at man skal kunne forhindre forstyrrelser på nettverket brukes i tillegg teknologien kalt beamforming, oversatt til norsk som *stråleforming*. Det er begrepet beamforming som er mest brukt i både engelsk og norsk litteratur, men vi kommer til å benytte oss av det norske begrepet stråleforming. Stråleforming er en signalbehandlings-teknikk som brukes i telekommunikasjon, den innebærer manipulering av et signal for å lede det i en bestemt retning. Teknologien brukes ofte for å forbedre kvaliteten på et overført signal, øke signaleffekten og redusere forstyrrelser fra uønskede kilder. I telekommunikasjon brukes stråleforming i trådløse kommunikasjonssystemer for å forbedre signal-støyforholdet (SNR) ved å fokusere det overførte signalet i retning av mottakeren. Dette oppnås ved å bruke en rekke antenner til å overføre signalet. Ved å justere vekten til hver antenne kan det overførte signalet styres mot mottakeren, øke signaleffekten og redusere forstyrrelser fra andre kilder. Av overnevnte faktorer forstår man hvorfor stråleforming er brukt til å forsterke signaleffekten i 5G.

Det andre FFI uthever, sett i lys av IMT-2020, er økningen av antall enheter som kan være tilkoblet til nettverket. Sammenlignet med de tidligere mobile nettverkene tar 5G i bruk andre protokoller, og gjør tilpasninger innenfor de lavere frekvensene som fører til at en kan utvide dekningen for enheter som sender små mengder data. I praksis betyr dette at en sensor

som ikke beveger seg kan sende en tilbakemelding til nettverket om å benytte «dvalemodus». Sensoren trenger derfor ikke å bruke strøm på å holde forbindelsen oppe til nettverket. Dette gjør at sensorene får betraktelig lenger levetid, med tanke på bruk av batterikapasiteten, sammenlignet med tidligere. Sensoren bruker derfor mindre strøm og man frigjør plass i nettverket siden enhetene kan gå i dvalemodus. (Vellan, 2020) (Voldhaug , et al., 2021)

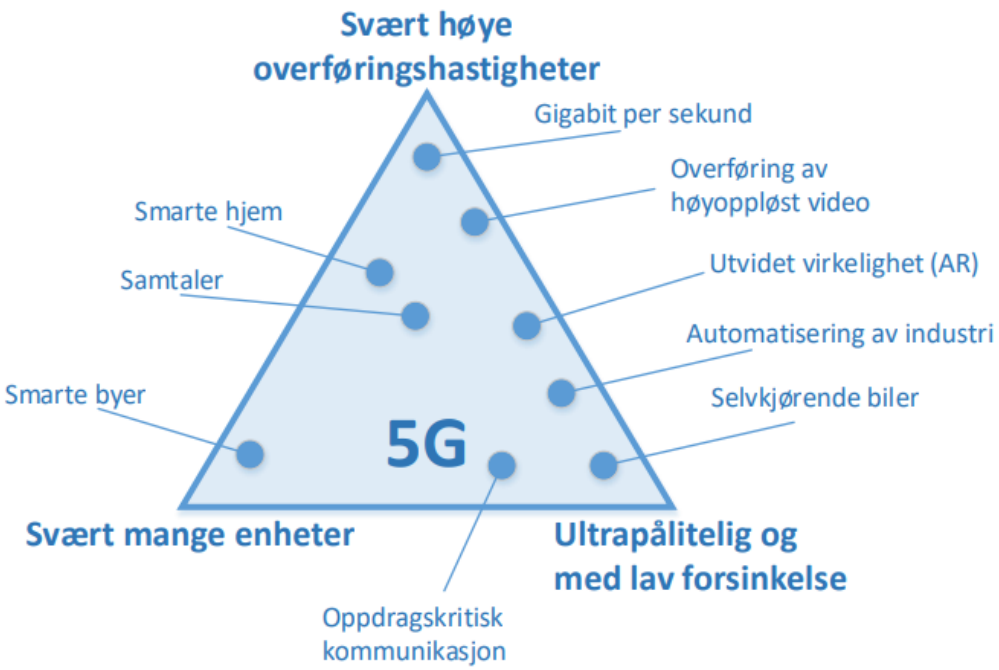
3.4.1.3 Internet of Things (IoT)

I forbindelse med oppgraderingen til 5G nettverket er Internet of Things (IoT), også beskrevet som tingenes internett på norsk, et viktig begrep. I fremtiden ser man for seg at «alt» vil ha en fordel av å være tilkoblet til internett. Alt fra telefoner, kameraer, bevegelsessensorer, kjøretøy, med mer. Trådløst mobilt nettverk er bare en del i dette begrepet siden det også omfavner kablet nettverk. Selv om IoT gjelder mer enn kun mobilt nettverk er fordelene ved utvidelsen av kapasiteten på 5G nettverket en av de viktige utbyggingene for å kunne etablere IoT i et bredere spekter. Mulighetene ved 5G og IoT er eksemplifisert i Figur 4. IoT er viktig av mange grunner, den første er knyttet til effektivitet og produktivitet: IoT kan bidra til å øke effektiviteten og produktiviteten i ulike bransjer ved å automatisere prosesser og samle inn data. For eksempel kan IoT-sensorer i en fabrikk overvåke maskiner og varsle når de trenger vedlikehold, slik at reparasjoner kan utføres før det oppstår en feil som kan føre til nedetid. For det andre, kan IoT føre til bedre beslutningsprosesser. Data fra IoT kan gi bedre innsikt og informasjon til bedriftsledere, som kan brukes til å ta bedre beslutninger og forbedre forretningsprosesser. For eksempel kan en detaljist bruke IoT-data til å analysere salgsdata og kundeatferd for å tilpasse produkttilbudet og markedsføringen. For det tredje, kan IoT gjøre det lettere å tilfredsstille eget informasjonsbehov. Ved bruk av flere elektroniske sensorer og enheter gjør dette at organisasjoner får et forbedret bilde av helheten. Om dette så er innhenting av direkteoverført video, eller logistikkstatus i Forsvaret for å konkretisere fordelene til vår profesjon. Dette er kun tenkte eksempler, og det er viktig å forstå seg på hvilke muligheter IoT medbringer som del av et sterkere 5G nettverk.

For at man skal kunne utnytte 5G nettverket til sitt fulle potensial, altså pålitelig og med lav forsinkelse, forutsetter dette at vi bygger mobilnettene på nye måter. Dette er det mest krevende målet å realisere sett ut ifra IMT-2020. Fra et teknisk ståsted, inneholder det komplette sivile 5G-nettverket et transportnett mellom basestasjonene som baserer seg på fiberforbindelser, og et kjernenett som inneholder funksjonalitet for å fordele datastrømmene

til riktig mottaker. Kjernenettet skal også sørge for at kun de som har tilgang til det via godkjent SIM-kort får tilgang. I tillegg skal 5G NR basere seg på teknologi som gjør at man kan minimiere feil ved overføring av data mellom brukeren og basestasjonen det sendes til.

Dette gjøres ved at selve feilen oppdages tidligere, og den dataen som går tapt kan sendes på nytt.



Figur 4: Grafisk fremstilling av muligheter ved 5G NR og IoT (Voldhaug et al., 2021)

3.4.1.4 Edge computing

Bruk av edge computing fasiliterer også for lav forsinkelse siden teknologien gjør at datastrømmen ikke må sendes via store datasenter, men heller kan holdes lokalt og nært brukeren. Forskjellen sammenlignet med dagens teknologi er altså at man flytter serveren nærmere brukeren. I IMT 2020 fremkommer det at forsinkelsen ved 5G nettverket skal forkortes til 1ms. Dette er en betraktelig mindre tid sammenlignet med det en er vant til i dag. Lavere forsinkelse muliggjør at man kan åpne for nye teknologier som for eksempel selvstyrende kjøretøy, mobile roboter og AR/VR. (Accenture, 2023) (Voldhaug , et al., 2021)

3.4.1.5 Skivedeling

Den siste nye teknologien som vi ser som relevant for oppgaven er 5G sin mulighet for skivedeling. Skivedeling gir mulighet for mer fleksibel og effektiv bruk av nettverksressurser. Hver skive kan tilpasses for å møte de spesifikke kravene til en applikasjon eller tjeneste, som for eksempel båndbredde, forsinkelse, pålitelighet og sikkerhet. På denne måten kan 5G-nettverket støtte et bredt spekter av applikasjoner og tjenester, inkludert selvkjørende biler, virtuell virkelighet, helseovervåkning og mer. Skivedeling i 5G-nettverk innebærer også å isolere nettverkstrafikken fra forskjellige skiver, slik at de ikke påvirker hverandre negativt. Hver skive har sitt eget sett med nettverksressurser, som kan tildeles dynamisk og automatisk etter behov. Dette gjør det mulig å optimalisere nettverkstilgjengeligheten, kapasiteten og ytelsen for hver skive. I sum gir skivedeling i 5G-nettverk en svært fleksibel og skalerbar plattform for å støtte et bredt spekter av applikasjoner og tjenester, samtidig som den optimaliserer ytelsen og ressursbruken på nettverket. Denne teknologien er ikke tilgjengelig i dagens mobile nettverk, noe som gjør at Forsvaret må basere seg på basestasjonene som finnes i sivil infrastruktur. Dette gjør at kapasiteten til nettverket må deles på alle brukere, både militært og sivilt. Dette slipper man ved bruk av 5G og egen skive i nettverket. Da vil skiven potensielt kun autentisere godkjente SIM-kort. Skivedelingsteknologien er ikke kun ment til Forsvaret, men er også diskutert til bruk i nødetatene, ved sykehus, til arrangementer og lignende. Kort oppsummert kan man opprette et privat nett som kun godkjente brukere vil ha tilgang til.

3.5 Nasjonal Sikkerhetsmyndighet – NSM

NSM har ansvar for å godkjenne og sertifisere kryptoutstyr som skal brukes av Forsvaret og andre offentlige virksomheter i Norge for å sikre konfidensialiteten og integriteten av kommunikasjonen. Hvis Forsvaret ønsker å anskaffe nytt kommunikasjonsmateriell er det flere regler som må følges for å sikre at utstyret er sikkert og samsvarer med NSMs krav til kryptoutstyr. De konkrete reglene som gjelder for anskaffelse av nytt utstyr vil avhenge av flere faktorer, inkludert formål, sikkerhetskrav, og andre tekniske spesifikasjoner. For det første, *sertifisering*: Forsvaret må sikre at radioen som anskaffes, er sertifisert av NSM for bruk i sikker kommunikasjon. Dette innebærer at radioen må oppfylle visse tekniske krav og være testet og godkjent av NSM før den kan tas i bruk.

For det andre, *kryptering*: Radioen må ha tilstrekkelig krypteringsteknologi for å sikre konfidensialiteten og integriteten av kommunikasjonen. NSM har utarbeidet spesifikke krav til krypteringsteknologi som må oppfylles.

For det tredje, *sikkerhetsklarering*: Personell som skal bruke radioen, må ha tilstrekkelig sikkerhetsklarering og opplæring i bruk av kryptoutstyr.

Til slutt, *overvåking*: NSM vil ha mulighet til å overvåke utstyrets bruk og utføre sikkerhetskontroller for å sikre at gitt utstyr blir brukt på en sikker måte, og at sikkerhetskravene blir opprettholdt. (NSM, 2020)

Forsvarets sikkerhetsavdeling (FSA) sørger for operativ sikkerhet og forebyggende sikkerhetstjeneste. De er Forsvarets link mot NSM og sørger i så måte at alt utstyr er i henhold til de føringer som ligger i grunn fra NSM, som belyst over. Ved implementering av en ny enhet vil FSA være en viktig sparringspartner for å kartlegge riktig behandling av sensitiv informasjon.

3.5.1 Sertifiseringskrav

Sertifiseringskravene omfatter en rekke tekniske, operative og administrative krav som skal sikre at utstyret oppfyller visse sikkerhetsstandarder. NSM har utviklet en rekke sertifiseringsprosedyrer som omfatter ulike sikkerhetsnivåer, avhengig av graden av sensitivitet av informasjonen som skal beskyttes. I tillegg til kravene som stilles til selve utstyret, krever NSM også at Forsvaret implementerer visse administrative og operasjonelle tiltak for å sikre sikkerheten til det nye utstyret. Dette kan inkludere krav til opplæring og trening av personell, styring av sikkerhetspolitikk og prosedyrer, og implementering av sikkerhetsoppdateringer og vedlikehold.

Sertifiseringsprosessen innebærer en grundig evaluering av utstyret, inkludert testing av sikkerhetsfunksjoner og vurdering av eventuelle risikoer og sårbarheter. NSM vil også gjennomføre sikkerhetskontroller av utstyret for å sikre at det oppfyller kravene til sikkerhet. Sertifiseringen fra NSM gir en bekreftelse på at utstyret oppfyller de nødvendige sikkerhetsstandardene, og kan brukes i tråd med Forsvarets sikkerhetsregler. Dette sikrer at informasjonen som utveksles via utstyret er beskyttet mot uautorisert tilgang eller manipulasjon. I sammenheng med anskaffelse av nytt materiell vil sertifiseringskravene fra NSM være en viktig faktor som må tas i betraktning, og Forsvaret vil måtte samarbeide tett

med NSM for å sikre at utstyret oppfyller kravene til sikkerhet og at sertifiseringsprosessen går smidig. (Sikkerhetsloven , 2019) (NSM, 2020)

3.5.2 Kryptografi

I dagens digitale verden har kryptografi blitt en viktig faktor for forsvarssektoren, spesielt når det gjelder å sikre kommunikasjon og sensitive data mot uønsket innsyn og manipulering. I denne oppgaven velger vi å ikke gå inn på spesifikke kryptografiske løsninger ev hensyn til graderingsnivå. Forsvarssektoren i Norge bruker kryptografi for å beskytte kommunikasjon og data i alle faser av driften, fra feltoperasjoner til administrasjon og beslutningstaking. En viktig faktor for Forsvaret er valg av kryptografiske algoritmer og protokoller som gir tilstrekkelig sikkerhet mot trusler, samtidig som de tillater rask og effektiv kommunikasjon. Forsvaret må også vurdere trusselnivåer og ta hensyn til den stadig økende kapasiteten til angripere, samt de nyeste teknologiske fremskrittene innen kryptografi. I tillegg til de teknologiske aspektene av kryptopolitikken, er det også viktig for Forsvaret å utvikle og implementere passende politikk og retningslinjer for bruk av kryptografi. Dette kan omfatte krav til sikkerhetsopplæring for personell som bruker kryptografiske systemer, samt etablering av retningslinjer for håndtering av kryptografiske nøkler og sertifikater. Samlet sett er kryptopolitikken for Forsvaret en kompleks tematikk, derfor har vi valgt å ta utgangspunkt i "Kryptopolitikk for Forsvarssektoren" (Bakke-Jensen & Tybring-Gjedde , 2019) utarbeidet av Forsvarsdepartementet i 2019 for å se på de ulike føringer som er lagt vedrørende kryptopolitikk. Dokumentet fremlegger flere viktige momenter ved kryptering, og vi velger å vise til de viktigste for vår oppgave:

Alle krypteringstjenester som brukes av Forsvarssektoren skal ha høyt sikkerhetsnivå og godkjennes av NSM.

All kommunikasjon som inneholder gradert informasjon, skal krypteres.

Forsvarssektoren skal ha egne retningslinjer for kryptering av mobilkommunikasjon.

Forsvarssektoren skal ha egne retningslinjer for sikkerhet ved bruk av internettjenester og eksterne nettverkstjenester. (Bakke-Jensen & Tybring-Gjedde , 2019)

3.5.3 Anskaffelsesprosessen

Når det gjelder anskaffelse av nytt sambandsmateriell til Forsvaret, så er sikkerhetsklarering en viktig faktor i anskaffelsesprosessen. For å kunne anskaffe og benytte sambandsmateriell som inneholder gradert informasjon, så må personell som skal håndtere slikt materiell ha en tilstrekkelig sikkerhetsklarering. Sikkerhetsklarering innebærer en omfattende bakgrunnssjekk og vurdering av en persons egnethet og lojalitet til å håndtere gradert informasjon. I tillegg til kravene til sikkerhetsklarering for personell, så må også det sambandsmateriellet som anskaffes oppfylle visse sikkerhetskrav. Dette kan innebære krav til kryptering, autentisering, beskyttelse mot avlytting og annen uautorisert tilgang. Anskaffelse av sambandsmateriell til Forsvaret vil derfor som regel være underlagt krav til sikkerhetsklarering for personell og sikkerhetskrav til selve materiellet som skal anskaffes. Disse kravene vil være nærmere beskrevet i anskaffelsesdokumentene som utarbeides for den aktuelle anskaffelsen. (Sikkerhetsloven , 2019) (NSM, 2022)

Når det gjelder sikkerhetskrav fremkommer følgende:

- Kryptering: Sambandsmateriellet må ha tilstrekkelig kryptering for å sikre at gradert informasjon ikke kan leses av uautoriserte personer eller enheter.
- Autentisering: Enheten må ha en mekanisme for autentisering, som sikrer at kommunikasjonen kun kan skje mellom godkjente enheter eller personer.
- Beskyttelse mot avlytting: Det materiellet som anskaffes må ha mekanismer som beskytter mot avlytting og uautorisert tilgang til kommunikasjonen.
- Robusthet: Sambandsmateriellet må være robust og pålitelig, og tåle tøffe miljøer og værforhold.
- Integrering: Sambandsmateriellet må kunne integreres med andre systemer og være kompatibelt med eksisterende infrastruktur og utstyr.
- Sertifisering: Sambandsmateriellet må være sertifisert av relevante myndigheter og standarder for å sikre at det oppfyller de nødvendige sikkerhetskravene. Sikkerhetskravene vil avhenge av hvilket sikkerhetsnivå det graderte utstyret vil være på og hvilken type informasjon som skal kommuniseres.

De lovverk og føringer som er redegjort for ovenfor er generelle. Det vil fremkomme tydeligere i drøftingsdelen under, hvilken relevans de ulike sikkerhetskrav har for en lavgradert enhet i Hæren.

3.6 The Android Team Awareness Kit

Android Tactical Assault Kit (ATAK) er en amerikansk BMS programvare, opprinnelig utviklet av Air Force Research Laboratory (AFRL). Programvaren finnes i en sivil utgave, da kalt *Android Team Awareness Kit* (ATAK-CIV eller CIVTAK). Denne kan lastes ned til smarttelefoner med android operativsystem. Den militære utgaven har enkelte funksjoner utover hva den sivile utgaven kan tilby, men alle applikasjoner og produkter fra TAK er interoperable med hverandre (Android Team Awareness Kit (ATAK), 2023). ATAK ble utviklet som et kartverktøy og hjelpemiddel for å skape og dele felles situasjonsforståelse, gjennom et felles operativt bilde av stridsfeltet (Android Team Awareness Kit (ATAK), 2023). Brukeren kan navigere ved hjelp av GPS (Savage, 2023). I tillegg tillater Plug-in arkitekturen brukeren å skreddersy funksjonalitet til egne behov (Savage, 2023).

Øvrige funksjoner omfatter bl.a.:

- Kart- og navigasjonsverktøy online og offline, 2D og 3D med svært høy oppløselighet
- Sentrering på egen eller andres posisjon i kartet
- Overlay-manager, med støtte for import av en rekke filformater
- Markering og deling av posisjon, inkludert historikk
- Tegning og deling av grafikk og ikoner
- Chat, fildeling (de fleste formater, foto og video), **videostrømming**
- Verktøylinje som kan skreddersys etter behov
- Radiofunksjonalitet (talesamband)

(Android Team Awareness Kit (ATAK), 2023)

4. DOTMLPFI

I dette kapittelet vil vi med utgangspunkt i hver kategori i forkortelsen DOTMLPFI, legge frem ulike funn vi har gjort gjennom deltakende observasjon. For hver bokstav presenteres funn, eksisterende grunnlag og anbefaling i en tabell. Under dette følger en utdypende drøfting av de ulike funnene i henhold til de spørsmål vi stilte oss i forkant av prosjektet.

4.1 D – Doktrine

4.1.1 Hvordan kan en mobilenhet med TAK-programvare bidra i et Nettverksbasert Forsvar?

Tabell 1: FEA 4.1.1

Funn	Eksisterende grunnlag	Anbefaling
5G åpner for høy hastighet og overføringskapasitet til å overføre store datamengder uten nevneverdig forsinkelse. ATAK har funksjonalitet og kan skreddersys slik at fildeling og videostrømming blir mulig.	Per i dag er det store begrensninger i bitrate på NorBMS med MRR på VHF som bærer. Det er mulig å bruke andre bærere med høyere bitrate, men det er hovedsakelig VHF som brukes. Hovedsakelig er det vognoppsatte avdelinger som har tilgang på NorBMS.	Mobilenheter med ATAK-programvare bør implementeres og gjøres interoperable med eksisterende systemer i Hæren for å oppfylle visjonen om et Nettverksbasert Forsvar.

Morgendagens Hær bruker ikke begrepet nettverksbasert krigføring eller Nettverksbasert Forsvar direkte, men indirekte antyder det langt på vei at vi bør gå i den retningen når den legger blant annet følgende til grunn for utvikling av Hæren:

Ifølge *Morgendagens Hær* skal Hæren blant annet:

- Bidra til felles situasjonsforståelse.
- Moderne C4IS som transitterer, sammenstiller og behandler store mengder data.
- Effektiv kommando og kontroll

- Hurtigere utnyttelse av teknologi for en tilpasset og relevant effektpåføring.
- Styrkebeskyttelse og utholdenhet.

(Forsvaret, 2021, s. 24)

Så er spørsmålet, hvordan kan en mobilenhet med ATAK-programvare bidra til et Nettverksbasert Forsvar? For det første, og kanskje mest åpenbare: Små bærbare enheter med ATAK-programvare, kan gi infanterienheter og andre et godt Battle Management System, der det i dag er tungvint eller umulig å bruke NorBMS. Funksjonaliteten til de to applikasjonene overlapper til en viss grad, men med ATAK og 5G som bærer blir det mulig å dele og behandle datamengder som langt overstiger det NorBMS med MRR VHF som bærer, kan håndtere. Dette åpner igjen for å dele stillbilder eller situasjonsbilder i form av skjermdumper, videoopptak med høy bildekvalitet eller strømming av video i sanntid. Her kan både mobilenheters integrerte kameraer, så vel som ulike sensorer brukes. Dette er informasjon som vil kunne gi beslutningstagere på høyere nivå kritisk situasjonsforståelse.

Videre kan ATAK bidra til å løse utfordringer knyttet til ildgeometri og ildkoordinering for effektorer med både flat- og krum bane. Med NorBMS kan en se «blåprikk» som markerer andre egnes posisjon, med mulighet for å programmere hvor ofte egen posisjon oppdateres. Gjøres dette for ofte, risikerer en å overbelaste nettverket, da bitraten med VHF som bærer er begrenset, og fungerer som en flaskehals. I tillegg er det kun forband med NorBMS som vil synes i situasjonsbildet, og i praksis vil dette ekskludere en del personell, da vi i dag hovedsakelig har enheter tilpasset kjøretøysmontert bruk. Det er mulig ved hjelp av batterier å konvertere kjøretøysmonterte enheter til bærbar bruk, men dette vil igjen bli en ekstra byrde for jeger- og oppklaringsenheter som allerede har mye vekt å transportere. I tillegg vil problemet melde seg så fort mekanisert infanteri opererer til fots/avsittet. Her kan små, lette mobilenheter med ATAK-programvare i første rekke tilby alle som ikke er på vogn en mer egnet enhet for deres bruk. I andre rekke, kan de med ATAK overføre data i et helt annet omfang, enn å være begrenset til kun å dele egen posisjon og kunne sende tekstmeldinger med NorBMS og VHF-radio. I tredje rekke, kan en med posisjonen til alle fotoppsatte enheter med mye større sikkerhet bruke ulike effektorer i nærhet av, men uten å være redd for å ramme egne. På den andre siden, dersom en skal utstyre hver eneste fotsoldat med en mobilenhet, vil det kreve mye ressurser, selv om enhetene i seg selv ikke er spesielt dyre i forhold til spesifikt utviklede enheter og sambandsmidler. Men det kreves ikke nødvendigvis en enhet per soldat, tross alt skjer det sjelden eller aldri at enkeltindivider opererer helt

selvstendig. Man må begynne et sted, og en mobilenhet per lag eller patrulje, vil sannsynligvis være tilstrekkelig for å oppnå gevinstene som er beskrevet i dette avsnittet.

Figur 5: ATAK programvaren under testing viser direktevideo med retning brukeren filmer i kartet.

4.1.2 Kan mobilenheter med TAK-programvare hjelpe oss å ta raskere og bedre beslutninger?

Tabell 2: FEA 4.1.2

Funn	Eksisterende grunnlag	Anbefaling
ATAK kan bidra til bedre SA gjennomgående i organisasjonen, og kan hjelpe oss å ta bedre beslutninger, raskere.	Infanteriet og andre fotoppsatte avdelinger opererer i stor grad uten systemer for beslutningsstøtte og BMS. Bærbare klienter for NorBMS har betydelige mangler.	ATAK kan innføres som verktøy for beslutningsstøtte i Hæren.

Her blir Boyds OODA-loop igjen relevant. Om beslutningssyklusen skal forstås bokstavelig som en sekvensiell prosess eller en mer dynamisk prosedyre, er ikke så interessant for oss i denne sammenheng. Det som er interessant, er hvorvidt den økte situasjonsbevisstheten ATAK åpner for, kan gi oss et fortrinn med tanke på å gjennomføre bedre beslutningssykluser, og om det med ATAK blir mulig å ta bedre avgjørelser raskere.

En troppssjef eller kompanisjef i infanteriet er som regel avhengig av selv å være langt framme i striden og hyppig bruk av samband for å klare å opprettholde en viss SA på hvor egne og fienden befinner seg. Sjefen er nødt til å ta beslutninger basert på den SA han eller hun har på et gitt tidspunkt, og ofte må beslutninger tas under ekstremt tidspress. I godt trente avdelinger sørger soldater, lagførere og befal for at sjefen har så god SA som mulig, gjennom gode og hyppige innrapporteringer, og sjefen vet selv hvor han må være for å skaffe seg så god oversikt over situasjonen som mulig. Hvis vi i denne situasjonen legger Boyds beslutningssløyfe til grunn, vil spesielt de to første trinnene, *Observe* og *Orient*, potensielt kunne ta tid. Dersom en kun har talesamband, kart og egne øyne til hjelp, vil det nesten uansett hvor godt avdelingen er drillet, ta noe tid å gjennomføre en hel beslutningssyklus. Med ATAK eller lignende programvare, behøver sjefen i teorien kun å kaste et blikk på sin mobilenhet, for å få posisjon på alle egne underenheter, naboavdelinger og posisjon på lokaliserte fiender, samt *hva* en er i kontakt med. Med en enkel grafisk fremstilling som den ATAK tilbyr, kan sjefen på få sekunder få en nokså fullstendig oversikt over situasjonen, og dermed hurtig ta en beslutning (*Decide*) og iverksette denne (*Act*).

4.2 O – Organisasjon

4.2.1 Hvor i organisasjonen er det hensiktsmessig å ta enheten i bruk?

Tabell 2: FEA 4.2.1

Funn	Eksisterende grunnlag	Anbefaling
En liten, lett og bærbar mobilenhet med TAK-programvare vil være mest hensiktsmessig for personell på lavere nivå (Kompani/eskadron/batteri og ned).	Det er et gap hva gjelder BMS/ hjelpemidler for å bygge SA hos enkelte avdelinger, dette gjelder i all hovedsak de som ikke har tilgang på NorBMS eller NORCCIS, og som har behov for å dele filer av en viss størrelse.	Enheten vi beskriver kan som et minimum implementeres hos ledere på lag/patrulje, tropps- og kompaninivå i Hæren, i alle avdelinger som opererer til fots hele- eller deler av tiden.

Eksisterende Battle Management Systems i Hæren er NorBMS og NORCCIS. Generelt brukes NorBMS både på kjøretøysmonterte klienter på tropps- og kompaninivå, og på stasjonære klienter på Forsvarets sikre plattform (FSP). NORCCIS brukes på stasjonære klienter på FSP, i kommandoplasser på bataljonsnivå og oppover. Begge systemene krever en klient med operativsystem fra Windows, NorBMS krever kun konnektivitet via en sambandsbærer som VHF, HF eller 4G, må klienter med NORCCS være tilkoblet en server, samt et større kablet nettverk. Kjøretøysmonterte klienter med NorBMS kan konverteres til bærbare klienter ved hjelp av batterier og diverse adaptere, men klientene er fortsatt store, tunge og med begrenset batteritid. Små mobilenheter med TAK-programvare vil trolig være den beste løsningen for avdelinger som hele- eller deler av tiden opererer til fots, grunnet deres nåværende mangel på slike systemer. Også for vognoppsatte avdelinger vil det være hensiktsmessig å ha tilgang på disse enhetene med TAK-programvare, kanskje spesielt for mekanisert infanteri med tanke på samvirke mellom vognlaget og fottroppen. Mulighetene for dataoverføring og strømming gjør at beslutningstagere i «andre enden» gjennom en eller annen løsning, må ha tilgang til dataene. Og her kommer vi inn på en utfordring som dette vil medføre. Ved å innføre *enda* et system, oppstår det nye problemer bl.a. fordi de nye systemene vil kreve opplæring, og fordi nye og gamle systemer ikke uten videre er interoperable. Mest fordelaktig er det kanskje om de nye systemene kan dekke bruksområdet til flere av de gamle, slik at en står igjen med færre systemer å forholde seg til, og de eldre systemene kan fases ut. Dette vil vi komme tilbake til, under henholdsvis *Trening* og *Interoperabilitet.*

4.3 Trening

4.3.1 Krever en implementering av mobilenheter med ATAK-programvare endring i utdanning og trening?

Tabell 4: FEA 4.3.1

Funn	Eksisterende grunnlag	Anbefaling
Ved bruk av 5G NR vil det bli mulig med større overføringshastigheter som vil muliggjøre overføring av store datamengder.	Veldig begrenset kapasitet på NorBMS med VHF som bærer.	Norske styrker er ikke vant til denne potensielt store mengden informasjon i sanntid. Dette vil få betydning for bl.a. stridsteknikk, taktikk og utdanning og vil trolig ta tid å implementere og operasjonalisere.

Dersom en mobil lavgradert enhet med TAK-programvare implementeres i Hæren, med 5G NR som bærer, vil enkelte endringer måtte gjøres. Blant annet er det flere funksjoner som vil være tilgjengelige som i dag ikke brukes i Forsvaret, eller som brukes på en annen måte. 5G NR kommer til å ha, som beskrevet i punkt 3.2, høyere hastigheter og større båndbredde enn tidligere teknologi. Tidligere har en vanligvis ikke hatt muligheten til å dele mer enn egen posisjon og sende korte tekstmeldinger, over NorBMS med VHF som bærer. Videostrømming fra sensor via en mobilenhet til beslutningstager, presis posisjonsdata med «blåprikk» på alle eller nær alle soldater på stridsfeltet, eller filoverføring av beslutningsgrunnlag fra en kommandoplass til en patrulje i felt, er kun noen av funksjonene mobilenheter med TAK-programvare fører med seg. Dette åpner opp for nye eller forbedrede teknikker og prosedyrer, som igjen kan få følger for taktikk. Dersom nye TTP-er (taktikk, teknikker og prosedyrer) utvikles, må sannsynligvis nye håndbøker og reglementer utarbeides, og utdanning av rekrutter, soldater, befal og offiserer må alle inkorporere disse endringene.

4.3.2 Kan implementering av lavgraderte mobilenheter med 5G som bærer gi nye muligheter i form av AR-teknologi?

Tabell 5: FEA 4.3.2

Funn	Eksisterende grunnlag	Anbefaling
5G NR og kompatible mobilenheter gir mulighet for lav forsinkelse og dataoverføring i sanntid, og kan derfor legge til rette for bl.a. AR-teknologi og strømming av direkte video.	Trenes ikke med i dag.	Ved bruk av direkte video, samt AR, kan dette endre hvordan vi trener og driver utdanning.

AR, eller Augmented Reality kan bli mulig ved hjelp av 5G NR. Årsaken til dette er den lave forsinkelsen og høye båndbredden. Edge computing, som forklart i 3.2.1.4, gjør det mulig å laste bilder nærmere endebrukeren. Dette var ikke en mulighet ved tidligere generasjoner mobilteknologi. AR gjør det mulig å få virtuelle objekter som et overlegg til virkeligheten (Microsoft, 2023). Hvis dette blir mulig ved bruk av TAK systemet, i kombinasjon med interaktive briller eller et heads-up-display (HUD), kan betydningen potensielt være stor for hvordan man trener og driver utdanning. Skal vi tro Microsoft, en av verdens teknologi-giganter, kan AR-teknologi drastisk forbedre utdanning og opplæring av medarbeidere, samt være til støtte uavhengig av fysisk avstand mellom veileder og medarbeider (Microsoft, 2023). I Figur 6 er det eksemplifisert hvordan AR kan bistå i feilsøking i industrien. Trolig kan dette være et verdifullt hjelpemiddel for feilsøking av mekaniske og sambandstekniske problemer i Hæren. Eksempelet viser et enkeltbrukergrensesnitt hvor piler, og fargekoder er visuelle hjelpemidler for feilsøking.

Det er viktig å påpeke at dette trolig ligger et stykke inn i fremtiden, men det er likevel viktig å nevne i sammenheng med hvilke muligheter 5G kan tilby oss, i kombinasjon med ny kommersielt utviklet software og hardware. For Hærens vedkommende er en av utfordringene at teknologi som tas i bruk og testes i det sivile, ikke automatisk er tilpasset militær bruk. Problematikken drøftes under «Materiell» og «Interoperabilitet». Det vi kan si med sikkerhet, er at ved å ta i bruk 5G NR som en bærer med høy overføringshastighet og kapasitet, samt moderne mobilenheter med høy prosessorkapasitet, ligger mange av

forutsetningene til rette for at Hæren på sikt kan benytte seg av AR-teknologi for å styrke egen utdanning, trening og øving, samt i skarp sammenheng.

Figur 6: Eksempel på bruk av AR i industrien (Marr, 2018).

4.4 Materiell

4.4.1 COTS vs MOTS

Tabell 6: FEA 4.4.1

Funn	Eksisterende grunnlag	Anbefaling
COTS og MOTS byr begge på fordeler og ulemper	Det er gjort lite testing av COTS og MOTS sammen med militære systemer	Gå for et MOTS-produkt som tilfredsstiller krav til robusthet og funksjonalitet

Et av de viktigste spørsmålene når det kommer til anskaffelse av mobile lavgraderte enheter til Hæren er utvelgelse av hvilken enhet som skal anskaffes. En av problemstillingene en da står overfor er hva som er mest hensiktsmessig av sivil hyllevare eller modifisert materiell. Utfordringen henger sammen med pris, holdbarhet og nytte, for å nevne noen eksempler. Det er også viktig å tenke på at ifølge Anskaffelsesregelverk for forsvarssektoren (ARF), har Norge som NATO-medlem et ansvar for å etterleve standardiseringsavtaler eller STANAG-

er (ARF, Del II, Kapittel 16, § 16-4). Videre skal vi se på ulemper og fordeler ved både COTS og MOTS

COTS

Sivil hyllevare også omtalt som commercial-off-the-shelf (COTS), betegnes som produkt eller programvare som er kommersielt produsert, og tilgjengelig for salg på åpent marked (NIST, 2019). Vi tar utgangspunkt i en av FMA sine modeller, som vist i Figur 7 under. Dette for å belyse dagens fordeler og ulemper ved COTS. Den kanskje største risikoen en tar ved å velge COTS-produkter er at disse ikke lever opp til militære standarder (MIL-STD). Én slik standard er (US) MIL-STD-461. Standarden påser at militært utstyr ikke slipper ut elektromagnetisk stråling som kan skape interferens med andre systemer (Brett, 2020). Det finnes svært mange nasjonale og internasjonale standarder, både militære og sivile som setter krav til hva et produkt skal tåle. Deler og komponenter som brukes i COTS er ikke tilpasset militært bruk, derav har slike produkter heller ikke like strenge sertifiseringskrav. Det elektromagnetiske støyet kan føre til at man jammer ut eget radiomateriell, som vil resultere i begrenset ytelse eller i verste fall systemfeil (Brett, 2020). I en skarp operasjon, hvor menneskers liv, og store verdier står på spill, er dette en risiko man ikke ønsker å ta.

Én fordel med bruk av COTS er at utstyret allerede er produsert, og tilgjengelig fra kommersielle produsenter (Trick, 2022). Andre fordeler med COTS-produkter er at de utvikles raskere, og som regel har en lavere kostnad, nettopp fordi de ikke trenger modifisering eller å skreddersys (Trick, 2022). Det er derfor attraktivt å benytte i en militær sammenheng fordi det er enkelt å få tak i, og derav enkelt å bytte ut (Trick, 2022). Sammenlignet med produkter tilpasset for militært bruk er COTS-produkter som regel ikke bestandig mot de påkjenningene operasjonsmiljøet vil utsette dem for, eksempelvis lave temperaturer, fuktighet, slag, støt, vibrasjoner osv. Dette gjør at enhetene må beskyttes og tilpasses på annen måte.

Figur 7: Eksempel på deksel til COTS enhet med varmefolie integrert. Bilde innhentet fra FMA med godkjenning om bruk i oppgaven.

MOTS

En middelvei mellom materiell spesialprodusert for militær bruk og COTS, er MOTS eller modified-off-the-shelf. Her blir COTS-varer modifisert av kjøper, leverandør eller en tredjepart (Trick, 2022). Fordelen med denne modifiseringen er at en får utstyr som er bedre tilpasset de krav brukeren stiller, men materiellet er likevel ikke spesifikt utviklet etter brukerens krav og holder således prisen nede. Det oppleves riktignok som en gråsone og et vanskelig definisjonsspørsmål, for hvor går skillet mellom COTS og MOTS? Blir et COTS-produkt et MOTS-produkt dersom en setter på et enkelt deksel? Definisjonene er mange og avvikende. Vi forholder oss derfor heretter til MOTS, som COTS-varer med modifikasjoner som i betydelig grad øker en enhets robusthet, eller endrer funksjoner eller egenskaper betydelig. Som vi allerede har vært inne på, er produkter spesielt utviklet for militære formål ofte kostbare og tar lang tid å utvikle. Alt dette taler for at COTS-produkter, som er modifisert slik at de kan etterleve kravene som stilles av brukeren, kan gi noen av fordelene spesialutviklet materiell har, til en brøkdel av kostnaden.

Den beste løsningen som brukes i dag for å beskytte en mobilenhet som ikke er bygd for å være solid og beskyttet fra elementene og temperatur, er forskjellige typer deksler. Under observasjonene vi har gjort oss har vi sett at disse dekslene som regel kjøpes inn fra en separat leverandør, eksempelvis amerikanske Juggernaut som på bildet. Ved bruk av deksler og tilbehør fra eksterne aktører medfører dette også en utfordring knyttet til innkjøp av slike. Det sier seg selv at markedet for deksler og tilbehør til militære formål er svært lite sammenlignet med det sivile markedet, og for at en potensiell produsent skal tjene på handelen, må det være lønnsomt også for dem. Skal man bruke mobile enheter som er COTS i operasjonsmiljøet Hæren opererer i, må det også anskaffes deksler som beskytter enhetene i tilstrekkelig grad. Et annet vesentlig aspekt når det kommer til bruk av mobilenheter i arktisk klima, er strøm og batteri. De fleste av oss har opplevd at vår egen mobiltelefon får betydelig dårligere batteritid i sterk kulde, og at de etter hvert vil skru seg av. For at vi skal kunne benytte enheten i det arktiske klimaet, må enheten beskyttes mot varmetap eller varmes opp av en varmekilde. I verste fall kan kritiske komponenter fryse i stykker, og bli ødelagt. Det vil derfor være nødvendig med isolering eller oppvarming, og konstant tilførsel av strøm. For brukeren sin del er det også nødvendig at enheten kan brukes med hansker, eller med en penn som er kompatibel med skjermen.

Sett i lys av de strenge krav militær anskaffelse og bruk setter til enheten, vil det være en viktig og kompleks prosess å velge hvilket produkt som skal anskaffes. Eksterne faktorer som vil påvirke denne prosessen, er bl.a. norske og internasjonale lover og regelverk, samt Norges forpliktelser til NATO, og standardiseringsavtalene dette medfører. Vi har ovenfor kun skrapt i overflaten på hva en slik anskaffelsesprosess må ta høyde for, og hensikten har vært å skape et bilde på kompleksiteten i et slikt arbeid, ikke å komme med noen definitive slutninger eller anbefalinger for de som skal gjennomføre en slik anskaffelse. Ikke desto mindre har vi, basert på de fordeler og ulemper vi har identifisert med COTS, MOTS og materiell utviklet spesifikt for forsvarssektoren, sett tydelige fordeler ved å gå for et MOTS-produkt. Summen av faktorene vi har sett på i et nytte/kostandsperspektiv, taler for dette.

Figur 8: Eksempel på en enhet fra MILDEF som innfrir militære standarder.

4.4.3 UGRADERT vs BEGRENSET?

Tabell 7: FEA 4.4.3

Funn	Eksisterende grunnlag	Anbefaling
Det vil være vanskelig å kommunisere nok informasjon ved lav gradering.	Gamle radioer er i bruk som LFR og PFR.	En gradering vil gjøre at man har mulighet til å bruke enheten til å skape et større og bedre situasjonsbilde via toveiskommunikasjon.

4.4.1.1 Sikkert kjøremiljø

En av de viktigste faktorene ved implementering til Hæren er et sikkert kjøremiljø på enheten. Dette betyr at informasjonen man innhenter og deler på enheten er riktig sikret i henhold til NSM sine føringer, som tidligere utdypet. For å kunne innfri kravene til sikkert kjøremiljø er NIST sine sertifiseringslister en god måte å sørge for at enheten er innenfor de føringer som er gitt fra Nasjonal sikkerhetsmyndighet.

4.4.1.2 Gradering

Et av spørsmålene ved integrering av en slik type enhet med TAK programvare er hvilken type gradering skal enheten ha. Ettersom vi har avgrenset oss til lavgraderte systemer tar vi utgangspunkt i UGRADERT (U) og BEGRENSET (B). Vi løftet problemstillingen med personer innenfor FMA og FFI for å få flere synspunkter på dilemmaet mellom de to. Et spørsmål som tydelig måtte besvares var følgende: *Hva slags informasjon ønsker man at skal deles via enhetene?*

I løpet av de deltakende observasjonene er det tydelig at informasjon som posisjon, observasjoner, og toveiskommunikasjon er viktige faktorer ved bruk av en slik enhet. Ved UGRADERT betyr dette at man vil ha vanskelig for å kunne dele posisjonsdata eller formidle ordre over applikasjonen. Hvis man benytter UGRADERT, vil ikke enheten kunne motta data fra systemer i f.eks. en kommandoplass. Årsaken er at slike systemer normalt har høyere gradering. Det er derfor viktig å se på mulighetene man har med TAK-systemet. Ved bruk av UGRADERT vil enhetens bruksområde være begrenset til å behandle data som ikke har fått gradering, i stedet for å benytte det fulle potensialet til applikasjonen. Hvis man graderer enheten BEGRENSET, vil dette åpne for bl.a. toveis kommunikasjon med andre systemer md samme gradering. Totalt sett, hvis man ønsker å få mest nytte av enheten på

lavt nivå, vil det i henhold til våre observasjoner være mest hensiktsmessig å gradere enheten BEGRENSET.

4.5 Lederskap

4.5.1 I hvilken grad kan enheten og ATAK støtte opp under Oppdragsbasert ledelse?

Tabell 8: FEA 4.5.1

Funn	Eksisterende grunnlag	Anbefaling
En mobilenhet med ATAK-programvare kan gi ledere på flere nivåer mer komplett situasjonsforståelse, og dermed redusere behovet for cross-talk, samt fasilitere for initiativ og gode anbefalinger.	Mye tid på nett brukes på å spre SA oppover og sideveis.	Mobilenheter med ATAK-programvare kan dersom det implementeres, gjøre mye snakk på samband på overflødig.
Mobilenheter med ATAK kan gi større grad av kontroll, og gi bedre forutsetninger for balansert lederskap.	Ledere på høyere nivå har som regel begrenset grad av oversikt og kontroll over det som utspiller seg på bakken.	Mobilenheter med ATAK-programvare kan dersom det implementeres gi bedre SA og grad av kontroll gjennomgående i organisasjonen.

Viktige poenger i OBL er desentralisering av beslutningsmyndighet i den hensikt å kunne utnytte endringer i situasjon, og mulighetsvinduer uten at dette går på bekostning av tempo (Forsvaret, 2020, s. 13). Å ha en mobilenhet med ATAK eller lignende programvare, i hendene på en lagfører/patruljefører, en troppssjef eller kompanisjef, betyr at mengden SA han eller hun sitter på, kan øke drastisk. At ledere på lavt nivå har bedre og mer komplett SA, vil også gjøre det lettere for dem å se mulighetsrom og ta initiativ og komme med gode anbefalinger til sin sjef. Posisjonen til egne underenheter, naboavdelinger, observasjoner av fiender, koordineringstiltak som meldelinjer og satslinjer, og forhåndsuttatte artillerimål er

alle elementer som allerede kan framstilles grafisk i applikasjonen NorBMS. De fleste kjøretøy og plattformer, og enkelte infanterienheter har tilgang på NorBMS gjennom diverse enheter.

Det NorBMS derimot ikke kan tilby på nåværende tidspunkt, er funksjoner som strømming/deling av video og sensordata direkte fra soldaten til beslutningstager. Denne funksjonen vil kunne åpne mange dører, og øke beslutningstagers situasjonsforståelse til nesten den samme som soldater på bakken. For ledere på høyere nivå, vil det i enkelte situasjoner være ønskelig å kunne følge med på en situasjon som utfolder seg «på bakken». Et god historisk eksempel på en beslutningstager på aller høyeste nivå som hadde muligheten til å følge med på en skarp operasjon i sanntid, er president Barack Obama under operasjonen hvor Osama Bin Laden ble drept. Et meget kjent bilde tatt under den pågående operasjonen, er fra konferanserommet hvor den amerikanske presidenten med sine nærmeste medarbeidere, tilsynelatende nervøst, følger med på en storskjerm.

At beslutningstager ser mye av det samme som det utførende leddet, vil i tillegg gjøre at betydelig mindre tid går med til å muntlig formidle situasjonsforståelse. Basert på egne erfaringer, brukes det på tropps- og kompaninivå mye tid på nett til å utveksle SA mellom sideordnede forband og til sjefen, for at alle skal ha så lik forståelse av situasjonen som mulig. Med bruk av maler og drill, kan dette gjøres nokså effektivt, men en grafisk fremstilling av alle egnes posisjon, posisjonen til lokaliserte fiender og videostrøm fra egne fremste vil mye av denne innrapporteringen være overflødig. Tiden en sparer kan brukes til f.eks. å diskutere justeringer i plan, koordineringer i tid og rom etc. i stedet for å forklare situasjonen til hverandre.

4.5.2 Kan enheten og ATAK være til hinder for Oppdragsbasert ledelse?

Tabell 9: FEA 4.5.2

Funn	Eksisterende grunnlag	Anbefaling
Å ha enda et system å forholde seg til, kan gjøre det vanskeligere for beslutningstagere å sortere ut relevant informasjon	Ledere på laveste nivå har som regel kun talesamband å forholde seg til. Jo høyere opp i systemet, jo flere systemer og kanaler må en forholde seg til	Mobilenheter med ATAK-programvare bør dersom det implementeres, ha funksjoner for å filtrere vekk irrelevant informasjon.

Men kan økt situasjonsforståelse hos sjef på høyere nivå virke mot sin hensikt? Vil ikke det at en kompanisjef sitter på nesten samme SA som lagføreren, gjøre det fristende for sjefen å detaljstyre lag og tropper, og dermed forbigå/overstyre både troppssjef og lagfører? Oppdragsbasert ledelse fratar ikke sjefen muligheten til å gi ordre og lede på den måten situasjonen måtte kreve. Under omstendigheter hvor beslutningstager har et økt kontrollbehov, har han eller hun rett til å gi ordre som i detalj beskriver utførelse, mens i andre situasjoner er det ønskelig å delegere stor grad av beslutningsmyndighet til laveste nivå (Forsvaret, 2020, s. 13). Evnen til å tilpasse lederskap til oppdraget, personell og situasjon er det viktige, både gjennom å veksle mellom lederskap og styring, og anvende samspills- og relasjonsorientert ledelse, oppdragsorientert ledelse og utviklingsorientert ledelse (Forsvaret, 2019, ss. 8-9). Vi ser ingen grunn til at mer SA på høyere nivå vil svekke lederes evne til å utøve oppdragsbasert ledelse. Trolig vil nok et verktøy i verktøykassa kun gi flere muligheter for lederen til å utøve og tilpasse sitt lederskap, og ATAK vil kanskje gjøre det lettere å identifisere om en har et økt behov for kontroll, eller om undergitte er i ferd med å avvike fra gitt intensjon. Om dette er tilfellet vil det være lettere å gå over til en mer detaljstyrende ledelsesform, fordi en har tilstrekkelig SA til å gjøre dette på en god måte. Samtidig vil det bli enda viktigere å være disiplinert i egen oppfølging av undergittes oppdragsløsning, og ikke bryte inn for å korrigere før en er sikker på at det er strengt nødvendig. Autonomi og frihet til å løse oppdrag slik en selv mener er best, er trolig en viktig faktor for ledere på lavt nivå, og dersom en fratar lagførere og troppssjefer muligheten til å planlegge og utføre egne planer vil dette kunne virke svært demotiverende.

Det som derimot kan bli en utfordring er mengden informasjon lederen blir utsatt for; skal en ha både talesamband på øret, ATAK på én skjerm, og NorBMS på en annen, kan det

oppleves som forstyrrende, og dermed virke mot sin hensikt. Beslutningsstøtte- og BMS-applikasjoner skal gi bedre SA, men bør ikke gå på bekostning av lagførere og troppssjefers anledning til å lede sine soldater. Skulle ATAK bli innført i en viss form eller farge, vil det bli viktig å ha muligheten til å filtrere mengden informasjon situasjonsbildet viser, slik at det viser alt som er nødvendig, men ikke noe mer.

4.6 Personell

4.6.1 Hvordan håndterer nåværende generasjon en slik implementering?

Tabell 10: FSA 4.6.1

Funn	Eksisterende grunnlag	Anbefaling
Generasjon Z har egenskaper og er tilpasningsdyktige når det kommer til avansert teknologi. Dette tilsier at de burde ha gode forutsetninger for å ta i bruk kommende teknologiske nyvinninger.	Generasjonsskiftet på lavere nivå i Hæren er allerede startet. Dette vil si at man kan observere generasjonenes ulike forutsetninger for å bruke dagens- og fremtidige systemer.	Basert på våre observasjoner virker det som det ikke vil være en uoverkommelig utfordring for personellet å håndtere teknologi som stadig er under utvikling.

Generasjon Z, personer født fra 1995 til og med 2010, er i dag fra 13-28år gamle (Boye, 2019). Dette betyr at den eldste delen av generasjonen er de som utgjør majoriteten av personellet på lavt nivå i Forsvaret, for eksempel førstegangstjenestegjørende, lagførere, troppssjefer og kompanisjefer. Vi ser på denne generasjonen som primære brukere av utstyr og systemer de kommende årene Det er derfor viktig å belyse hvilke egenskaper generasjonen har, for å forstå hva som må til ved eventuell implementering.

For det første kjennetegnes Generasjon Z som en generasjon vokst opp med mobiltelefon og sosiale medier, og de omtales gjerne som digitalt innfødte (Boye, 2019). Nikolai Boye skriver at generasjonen er: «Veldig endringsvillige, tilegner seg ny kunnskap raskt innen ny teknologi og software» (Boye, 2019). Dette vil være en fordel hvis man tenker seg å

implementere et BMS system på en mobiltelefon. Som tidligere nevnt går teknologiutviklingen i dagens samfunn veldig raskt. Teknologi byttes ut etter kun få år, og ny og forbedret teknologi kommer på markedet. Et godt eksempel er mobilindustrien; det kommer nye oppgraderte enheter hvert år eller oftere fra ledende leverandører som Samsung, Nokia og Apple, parallelt med oppdaterte operativsystemer. Dette er noe generasjon Z har vokst opp med og er vant til, og er et godt eksempel på det Nikolai Boye viser til som endringsvillighet og rask tilegning av ny kunnskap. Erfaringer fra våre deltakende observasjoner tilsier at det for eldre personell krever mer opplæring for å holde tritt med oppdateringer av applikasjoner og systemer. Der Generasjon Z i stor grad har vokst opp med å bruke varierte brukergrensesnitt og berøringsskjermer, har eldre personell ikke nødvendigvis hatt det samme forholdet til teknologi fra ung alder. Dette kan være en utfordring for bruk i Forsvaret, men vi ser det som en fordel at Generasjon Z som brukere er vant til å ta i bruk teknologi som stadig oppdateres. Ser vi fremover i tid, utgjør yngre generasjoner en stadig større andel av soldater, befal og offiserer i Forsvaret. Når TAK-systemet i tillegg delvis kan skreddersys etter brukerens behov, vil slike oppdateringer trolig være overkommelige sett fra et brukerperspektiv. Sett i lys av dette, ser vi det som sannsynlig at Generasjon Z og kommende generasjoner vil være godt egnet som brukere av enheter og TAK-programvare.

4.6.2 Kan det bli for mye informasjon for ledelseselementet?

Tabell 11: FEA 4.6.2

Funn	Eksisterende grunnlag	Anbefaling
Med flere systemer og større overføringskapasitet, er det sannsynlig at det kan oppleves som forstyrrende og kontraproduktivt.	Personellet er ikke nødvendigvis vant til kontinuerlig flyt av store datamengder.	Funksjoner i brukergrensesnittet for å filtrere bort irrelevant informasjon vil være viktig, samtidig som utdanning, trening og øving må forberede brukere på å håndtere større mengder informasjon.

Digitalisering og utviklingen innenfor mobilt nettverk gjør det mulig for sjefer på ulike nivå å innhente større mengder, mer nøyaktig data. Dette kan gi et betydelig fortrinn hva gjelder situasjonsforståelse sammenlignet med tidligere teknologier. På den andre siden vil ikke teknologien isolert gi et funksjonelt kommandosystem, og studier fra U.S. Army viser at ledere ikke nødvendigvis håndterer informasjon raskere (Freeman , Cohen , Serfaty , Thompson , & Bresnick , 1997, s. 1). Det vil være viktig for ledere å trene på å bli utsatt for svært store informasjonsmengder, og samtidig hvordan filtrere ut den relevante informasjonen. Dette ansvaret ligger selvfølgelig ikke bare hos ledere, men også hos f.eks. utdanningsinstitusjoner. Rapporten fra U.S Army viser i tillegg at filtrering av informasjon og «overbelastning» av egen evne til å oppfatte informasjon angår stabsmedarbeidere så vel som ledere, da disse er en viktig komponent for å gi sjefen et riktig beslutningsgrunnlag (Freeman , Cohen , Serfaty , Thompson , & Bresnick , 1997, s. 1). Dette er et aspekt som burde tas i betraktning ved implementering av en mobilenhet med TAK-programvare, da dette medfører et potensial for betydelig økte mengder informasjon. Ledere må derfor være forberedt på å håndtere denne informasjonsstrømmen. Tiltak som kan bidra her, kan være spesifikk trening og utdanning på Information Management for både ledere og stabsmedarbeidere, samt funksjoner for å filtrere informasjon i programvaren. Dette er en utfordring det trolig finnes mange løsninger på, men som sannsynligvis vil bli høyst reell dersom en mobilenhet med BMS-programvare og 5G som bærer implementeres.

4.7 Fasiliteter

4.7.1 Hvor robust vil kommersielle 5G SA basestasjoner være, når 5G SA er bygd ut i Norge?

Tabell 12: FEA 4.7.1

Funn	Eksisterende grunnlag	Anbefaling
5G basestasjoner er relativt robuste mot jamming, men vil være attraktive mål, og uplink-signal fra brukerenheter vil være en sårbar komponent i systemet	Teknologien er fortsatt umoden, og kommersiell 5G SA dekning er ikke bygd ut i Norge.	Teknologien vil trolig bli enda bedre på å motstå EK. Mange tiltak kan gjøres, som å bygge redundante nett, slik at en ikke mister dekning selv om en basestasjon jammes ut eller ødelegges fysisk.

Vi har forutsatt at 5G SA er utbygd i hele Norge, og at Forsvaret blir tildelt en egen skive/slice i dette nettverket. Mobilenheten vil altså være avhengig av å kunne koble seg til militær slice i 5G-nettet, via en kommersiell 5G-basestasjon, eller en av Hærens mobile basestasjoner. De kommersielle basestasjonene vil trolig være montert en tilsvarende måte som dagens 4G- og 5G-NSA basestasjoner dvs. master av forskjellig type på fjelltopper, hustak osv. I skrivende stund har Telenor alene over 8000 slike basestasjoner over hele landet (Telenor, 2023). Det sier seg selv at det vil bli vanskelig å bevokte alle disse i tilfelle krise/krig. Om en slik situasjon skulle inntreffe, vil en del av Heimevernets oppdrag være å bevokte kritisk infrastruktur. For Hæren sitt vedkommende betyr dette at en *kan* få støtte fra HV til å beskytte basestasjoner som vurderes som ekstra utsatte for f.eks. sabotasje. Det er likevel usannsynlig at det lokale HV-området har kapasitet til å beskytte alle basestasjoner samtidig. Det vil derfor være viktig å være i stand til å gjenopprette dekning i områder hvor basestasjoner blir sabotert eller ødelagt.

På den andre siden er det ikke bare fysisk ødeleggelse av basestasjoner som er en potensiell trussel mot 5G-dekningen. Elektronisk krigføring (EK) er noe Hæren alltid vil måtte forholde seg til, også i forhold til 5G. Det er mange måter å påvirke/jamme ut et

sambandssystem/nettverk. *Barrage-jamming* vil si at en forsøker å jamme hele frekvensområdet til målet ved å sende store mengder støy, for å heve støygulvet for mottakeren, slik at støynivået blir høyere enn signalet (Birutis, Mykkeltveit, Ulversøy, Borlaug, & Kårstad, 2022, s. 41). Dette fungerer godt når en ikke har kjennskap til signalet en forsøker å jamme ut. En annen metode er partial-band jamming, hvor en kun jammer ned en del av frekvensområdet til målet med støy. Dette krever mindre energi, men er like effektivt dersom en har informasjon om signalet en søker å jamme ut (Birutis, Mykkeltveit, Ulversøy, Borlaug, & Kårstad, 2022, s. 41).

Det finnes lite data på 5Gs motstandsdyktighet mot, da 5G SA ennå ikke er lansert mange steder, og teknologien er utviklet av sivile aktører som ikke trenger å ta høyde for EK. Til tross for dette har Forsvarets Forskningsinstitutt (FFI) gjennomført en rekke tester på en simulert kommersiell 5G basestasjon, samt en helt vanlig smarttelefon. Basestasjonen hadde 4G-antenner og to 5G-antenner med massiv MIMO fra Huawei, på et 4G-kjernenett, og systemet opererte på en 5G NSA-arkitektur jamming (Birutis & Mykkeltveit, 2022, s. 59). Jammeren var spesialbygd for formålet, og brukte et frekvensmodulert sinusformet signal (Birutis, Mykkeltveit , Ulversøy , Borlaug , & Kårstad , 2022, s. 60). Basestasjonen og mobilenhet ble utsatt for barrage jamming og partial-band jamming, og det viste seg at uplink (signalet fra mobilenhet til basestasjonen) var mest sårbart for jamming, primært grunnet den begrensede sendeeffekten (Birutis, Mykkeltveit, Ulversøy, Borlaug, & Kårstad, 2022, s. 3). Videre viste testene at når 5G systemet ble utsatt for jamming, responderte det med å senke moduleringen og fortsatte å operere, men med redusert kapasitet så lenge jammesignalet var tolererbart (Birutis & Mykkeltveit, 2022, s. 66). Når interferensen var for ødeleggende, ble 5G-økten terminert, og forbindelsen gikk ned til en uforstyrret 4G-kanal (Birutis & Mykkeltveit, 2022, s. 66). Testingen identifiserte en terskel, når basestasjonen ble utsatt for jammesignal (barrage-jamming) på 5dB eller mer, kunne ikke basestasjonen lenger gi tilfredsstillende god tjeneste (Birutis & Mykkeltveit, 2022, s. 66). En av flere konklusjoner fra disse testene, er at 5G basestasjoner vil være attraktive mål, og at uplink-signalet (fra mobilenhet til basestasjon) er en sårbar komponent i 5G-radiosystemet (Birutis & Mykkeltveit, 2022, s. 66). Basert på dette kan vi selv konkludere med at det er *mulig* å jamme ut en 5G basestasjon. Dette vil for det første være svært energikrevende. For det andre er det ikke nødvendigvis nok å jamme ut en basestasjon for å fjerne dekningen i et område, da det ofte er mer enn en basestasjon i et gitt område. Alt vil komme an på materiellet, kompetansen og ambisjonsnivået til motstanderen. For mer informasjon om forsøk og testing av 5G NR

basestasjoners motstandsdyktighet mot jamming, henviser vi til FFI sin studie: «Practical Jamming of a Commercial 5G Radio System at 3.6 GHz» (Birutis & Mykkeltveit, 2022).

4.8 Interoperabilitet

4.8.1 Kan enheten være med på å utvikle hærens interoperabilitetsvisjon?

Tabell 13: FEA 4.8.1

Funn	Eksisterende grunnlag	Anbefaling
TAK operativsystemet er fleksibelt og kan sammenkobles på tvers av bærere.	NORCCIS har TAK integrasjon – sammenkobling med server for deling av situasjonsbilde til/fra TAK.	Å se på muligheter for å få implementert systemet som del av nåværende struktur.
TAK er en potensiell programvare som kan brukes multinasjonalt siden flere av de største nasjonene har tatt det i bruk innenfor landdomenet.	TAK er nylig tatt i bruk hos flere NATO land.	Se på en løsning som tar i bruk ATAK på mobil bærer for å kunne dele SA i et multinasjonalt scenario.

I Morgendagens hær står følgende om interoperabilitet: «Samvirke og interoperabilitet med fellesoperative ressurser er avgjørende for å lykkes i et slikt operasjonsmiljø, for å kunne beskytte seg mot påvirkning fra andre domener, og for å kunne påvirke motstanderen på uventede måter. Videre krever en slik operasjonsform særlig utvikling innen teknologi, prosedyrer, taktikk og ledelse.» (Forsvaret, 2021, s. 16). Hvis en ser dagens kommunikasjonsbærere (LFR, MRR, HF, SHF, UHF) opp imot interoperabilitetsvisjonen som Morgendagens hær beskriver er det tydelig at det er behov for teknologi og materiell som fungerer interoperabelt. Problemet vi i dag står overfor er at de ulike nasjonene i NATO bruker ulike radioer, med ulik kryptering, som gjør det helt umulig for militært personell fra en nasjon å få sikkert samband med andre nasjoner uten å kryssunderlegge personell og byttelåne sambandsmateriell. Dette er en lite hensiktsmessig måte å oppnå interoperabilitet.

Et godt eksempel på dette observerte vi på OJT under Øvelse Joint Viking 23. En av terminalvogn fra Sambandsbataljonen ble underlagt HNLMS Rotterdam (Nederlandsk marinefartøy). Med seg måtte de ha en egen liaison fra Brigade Nord for at kommunikasjonen mellom fartøyet og norske styrker i det hele tatt skulle være mulig. Dette er kun et eksempel fra egne erfaringer om at kommunikasjon mellom nasjoner i dag er problematisk. Sett i lys av Morgendagens Hær er det tydelig at dette problemet også er anerkjent i Hæren.

Standardisering er en forutsetning for å klare å oppnå interoperabilitet. Ifølge Anskaffelsesregelverket for forsvarssektoren (ARF) er formålet med standardisering: «å gjennomføre effektive nasjonale og allierte militære operasjoner» (Anskaffelsesregelverk for forsvarssektoren, 2013). Spesielt tilsier §16-4. at STANAG-er skal følges for den enkelte nasjon for å opprettholde interoperabilitet mellom NATO-nasjonenes styrker. «STANAG-er som er formelt godkjent (ratifisert) til bruk i forsvarssektoren, skal benyttes ved anskaffelser av materiell eller tjenester» (Anskaffelsesregelverk for forsvarssektoren, 2013). STANAG 4677 – «kommunikasjon mellom soldatsystemer» er viktig ved implementering, men dokumentet er gradert og vi går ikke nærmere inn på de spesifikke detaljene (NATO, 2017). Skal Hæren ta i bruk et soldatsystem er det viktig at slike standarder følges for å oppnå interoperabilitet med allierte nasjoner.

Videre vil vi se på noen erfaringer med TAK-programvare i andre NATO-land. Nylig valgte den britiske hæren å ta i bruk TAK som Battle Management Application (BMA) for sine fotoppsatte styrker. Ifølge representant for britiske Ministry of Defence (MoD) David Dalby, falt valget på TAK, på grunn av programvarens muligheter for integrasjon med internasjonale partnere, samt at programmet reduserer treningsbyrden for soldatene i form av enkelhet i opplæring (Savage, 2023). Fra tidligere av er applikasjonen TAK tatt i bruk i USAs forsvar, mest relevant er erfaringene gjort i US Army (Bandy , Parsons, Goldan, & Mitchell , 2018) En av erfaringene som blir trukket frem er TAK sin fleksibilitet og mulighet for tilpasning av brukeren. Programvaren brukt i TAK inneholder koding som gjør det mulig for utviklere å utarbeide løsninger på softwareproblemer som oppstår. Sammenlignet med programvare utviklet spesifikt for militær bruk, har denne sjelden åpen kildekode, og man har derfor ikke denne muligheten. Denne fleksibiliteten i TAK systemet gjør det mulig å drive løpende utvikling av TAK systemene for å holde tritt med utviklingen. For Hæren sitt vedkommende betyr dette at en implementering av TAK, vil kunne øke vår evne til interoperabilitet med to av våre viktigste allierte, og på sikt, kanskje også flere. I tillegg har

et av systemene som allerede er i bruk i Hæren, NORCCIS, integrert støtte for utveksling av situasjonsbildeoppdateringer med TAK-enheter (Forsvarsmateriell/IKT-kapasiteter, 2021, s. 4). Det er viktig å ikke glemme at interoperabilitet er en forutsetning for å kunne drive fellesoperasjoner på en god måte, ikke bare mellom nasjoner og forsvarsgrener, men også mellom systemer innad i egen forsvarsgren.

5. Konklusjon

I denne oppgaven har vi hatt til hensikt å besvare problemstillingen: «*Hvordan kan en mobil lavgradert enhet med 5G som bærer implementeres på taktisk nivå i Hæren?*». Dette har vi gjort ved å drøfte utvalgte spørsmål knyttet til hver kategori i DOTMLPFI, opp mot relevant teori og egne observasjoner. Summen av alt vi har redegjort for, drøftet og undersøkt, leder oss til vår endelige oppsummering av prosjektet, og vårt svar på problemstillingen.

Mobilenheten vi ser for oss vil være utviklet sivilt, dvs. enten commercial-off-the-shelf eller modfied-off-the-shelf. Vi har forutsatt at 5G stand-alone vil bli bygd ut i hele Norge, og at Hæren vil få en egen skjermet del av dette nettverket, samt at Hæren vil ha tilgang på egne mobile basestasjoner som kan opprette dekning der sivil infrastruktur er ødelagt, eller der det fra før ikke eksisterer slik infrastruktur. Vi har i tillegg forutsatt at enheten vil få graderingen UGRADERT eller BEGRENSET. Vi har avgrenset oss til å se på én type enhet, med en applikasjon å forholde seg til. Oppgaven har hatt til hensikt å utforske problemstillingen på konseptuelt nivå, med et operativt fokus. Videre har vi avgrenset oss til hovedsakelig å se på lag/patrulje, tropp og kompani, men har også diskutert hvordan systemer på dette nivået kan interagere med høyere nivå. Andre sambandssystemer har kun vært beskrevet der dette har vært relevant for vår problemstilling.

For det første, har vi kommet fram til at denne enheten må graderes BEGRENSET. Dette er for å ivareta informasjonssikkerheten best mulig, samtidig som at utveksling av informasjon kan gå begge veier. Vi har kommet fram til at en mobilenhet med 5G som bærer, åpner opp for at store datamengder kan overføres, og slik bidra til visjonen om et *Nettverksbasert Forsvar*. Videre bør en slik enhet ha et BMS, og vår anbefaling til applikasjon er Tactical Assault Kit. Formfaktoren, og TAK-programvaren vil kunne gi avdelinger som hele- eller deler av tiden opererer til fots, et godt BMS, med muligheten til å overføre sensordata eller andre filer, samt strømme video direkte til kommandoplasser og beslutningstagere. På denne måten kan SA utveksles på en helt annen måte enn i dag. Dette vil gjøre noe med evnen til

beslutningstagning, da en på kortere tid kan få bedre situasjonsforståelse og derfor ta mer velinformerte avgjørelser på kortere tid. Behovet for en slik kapasitet er størst for lag, tropp og kompani, som hele- eller deler av tiden opererer til fots, og andre forband hvor det i dag er tungvint å få tilgang til NorBMS eller NORCCIS. Så lenge det er mulig å overføre dataene til de som har behov for dette, er det på laveste nivå selve mobilenhetene hører hjemme. Økt mengde informasjon, vil trolig kunne åpne for nye måter å operere på, og utvikling av nye SOP-er og TTP-er vil medføre at håndbøker, reglementer og utdanning må tilpasses og oppdateres. Med en høykapasitets bærer som 5G, samt moderne mobilenheter, kan det etter hvert bli mulig å ta i bruk *Augmented Reality* for å heve kvalitet på utdanning, trening og øving, og kanskje også ytelse under skarpe operasjoner. For å holde kostandene ved anskaffelse av en slik enhet nede samtidig som brukerens og operasjonsmiljøets krav ivaretas, anbefaler vi at en slik enhet er *modified-off-the-shelf*. Merk at dette trolig vil medføre utfordringer knyttet til bl.a. elektromagnetisk kompatibilitet og etterlevelse av standarder Norge er forpliktet til å oppfylle som NATO-medlem. Vår ledelsesfilosofi vil ikke bli mindre relevant eller hensiktsmessig i møte en mobilenhet med TAK-programvare, men fører med seg nye muligheter og potensielle fallgruver knytte til bl.a. *Information Management.* Personellet som skal ta det nye materiellet i bruk er tilpasningsdyktige og mer teknologisk kompetente enn tidligere generasjoner, allerede før de mottar spesifikk utdanning. Elektronisk krigføring vil trolig alltid være en faktor i et moderne operasjonsmiljø, og 5G som bærer er ikke immun mot slik påvirkning. Likevel er teknologien lovende og under utvikling. En mobilenhet med TAK-programvare er allerede tatt i bruk av to av våre nærmeste allierte. Integrasjon i eksisterende systemer er et allerede påbegynt arbeid, og fleksibiliteten i programvaren gir gode muligheter for tilpasninger i interoperabilitetsøyemed. Vi ser på en mobilenhet gradert BEGRENSET og 5G som bærer, som et svært allsidig verktøy som personell i lederroller i Hæren vil ønske å ha i sin verktøykasse.

Med dette anser vi vår problemstilling som besvart. Dette prosjektet er på ingen måte en uttømmende oppskrift på hvordan anskaffelse og implementering av sambandsmidler i Forsvaret bør foregå, men en utforskende studie som kanskje kan inspirere andre til å ta opp arbeidet med å føre C4IS i Hæren inn i fremtiden. Våre funn og våre konklusjoner er ikke nødvendigvis ugyldige sett bort fra forutsetningene og avgrensningene vi har lagt til grunn. Arbeid knyttet til utfordringer ved anskaffelser og implementering av ny teknologi i

Forsvaret kan ha en universell verdi, med overførbare funn og konklusjoner. Utviklingen av teknologi går hurtig, og om bare få år kan noe av det vi har sett for oss være realisert, eller kanskje har utviklingen tatt en hel annen retning. Uansett har prosjektet vært både lærerikt og givende for oss som kommende sambandsoffiserer i Hæren. Vi ser på det som viktig å være fremoverlente, kreative og løsningsorienterte i en tid med en usikker sikkerhetspolitisk situasjon, og en Hær som er avhengig av å få maksimal kampkraft av ressursene vi har. Arbeidet har inspirert oss til å fortsette å være fremoverlente, og i dialog med orlogsmester Aase, har vi blitt gjort oppmerksomme på at det i Forsvaret er mulig å søke om CD&E-midler i den hensikt å bidra i konseptutvikling og eksperimentering. Dette er noe vi kunne tenke oss å gjøre, da vi om kort tid tiltrer som sambandsoffiserer i Hæren.

6. Litteraturliste

Accenture. (2023 *What is edge computing.* fra Accenture: https://www.accenture.com/us-en/insights/cloud/edge-computing-index#:~:text=Edge%20computing%20is%20an%20emerging,led%20results%20in%20real%20time.

Android Team Awareness Kit (ATAK). (2023, Mars 20). Android Team Awareness Kit or ATAK / CivTAK. Hentet Mars 20, 2023 fra https://www.civtak.org/atak-about/

Anskaffelsesregelverk for forsvarssektoren. (2013). *Lovdata*. Hentet fra FOR-2013-10-25-1411: https://lovdata.no/forskrift/2013-10-25-1411

Bakke-Jensen , F., & Tybring-Gjedde , I. S. (2019). *Norsk Kryptopolitikk* . Oslo : Forsvarsdepartementet .

Bandy , D. W., Parsons, J. D., Goldan, A. L., & Mitchell , E. A. (2018, Des). *NAVAL POSTGRADUATE SCHOOL* . Hentet fra https://apps.dtic.mil/sti/pdfs/AD1069441.pdf

Beadle, A., & Diesen, S. (2015). *Globale trender mot 2040 - implikasjoner for Forsvarets rolle og relevans.* Forsvarets Forskningsinstitutt. Hentet Mars 20, 2023 fra https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/1183/15-01452.pdf

Birutis, A., & Mykkeltveit, A. (2022, September 22). Practical Jamming of a Commercial 5G Radio System at 3.6 GHz. *Procedia Computer Science*(205), 58-67. Hentet Mars 23, 2023 fra https://www.sciencedirect.com/science/article/pii/S1877050922008729

Birutis, A., Mykkeltveit , A., Ulversøy , T., Borlaug , Ø. D., & Kårstad , J. (2022, April 27). *FFI* . Hentet fra A study of 5G New Radio and its vulnerability to jamming: https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/3022/22-00906.pdf

Birutis, A., Mykkeltveit, A., Ulversøy, T., Borlaug, Ø. D., & Kårstad, J. (2022). *A study of 5G New Radio and its vulnerability to jamming.* Forsvarets Forskningsinstitutt. Hentet Mars 23, 2023 fra https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/3022/22-00906.pdf

Boye, N. (2019, Mai 11). *Generasjon Z*. Hentet Mars 30, 2023 fra nho.no: https://www.nho.no/regionkontor/nho-vestfold-telemark/artikkelarkiv/generasjon-z/#:~:text=Generasjon%20Z%20er%20v%C3%A5r%20yngste,den%20digitale%20revolusjonen%20under%20huden.

Brett, D. (2020, Juni 26). *MIL-STD-461: Everything You Need to Know*. Hentet Mars 27, 2023 fra trentonsystems.com: https://www.trentonsystems.com/blog/mil-std-461-everything-you-need-to-know

Clausewitz, C. v. (1976). *On war*. Princeton: Princeton University Press.

Det Kongelige Forsvarsdepartement. (2020, oktober 16). Prop. 14 S (2020-2021). *Langtidsplan for forsvarssektoren*. Oslo. Hentet Mars 28, 2023 fra https://www.regjeringen.no/no/dokumenter/prop.-14-s-20202021/id2770783/

Forsvaret. (2004). *Forsvarets doktrine for landoperasjoner.* Oslo: Forsvarsstaben.

Forsvaret. (2019). *Forsvarets fellesoperative Doktrine.* Oslo: Forsvarsstaben. Hentet September 2022

Forsvaret. (2020). *Forsvarets grunnsyn på ledelse.* Forsvaret.

Forsvaret. (2021). *Konsept for utvikling av Hæren - Morgendagens Hær.* Forsvaret.

Forsvarets Stabsskole. (2007, Juni 15). Forsvarets Fellesoperative Doktrine. Oslo: Forsvarsstaben.

Forsvarsdepartementet. (2022). *Framtidige anskaffelser til forsvarssektoren (FAF) 2022-2029.* Oslo: Forsvarsdepartementet.

Forsvarsmateriell. (2020, August 5). *Mime.* Hentet Februar 23, 2023 fra Forsvarsmateriell: https://www.fma.no/anskaffelser/virksomhetsprogrammet-mime

Forsvarsmateriell. (2022, oktober 4). *5G i felt for Norges forsvar*. Hentet fra fma.no: https://www.fma.no/aktuelt-og-media/2020/5g-i-felt-for-norges-forsvar

Forsvarsmateriell/IKT-kapasiteter. (2021, Januar 5). NORCCIS Tak Integration. (1.1). (J. Løkke, Red.) Forsvarsmateriell. Hentet Mars 22, 2023 fra https://ds1ufumc0003.u-nor.u.mil.no:8080/norccis/helpcenter/Document/NORCCIS%20Communications%20TAK%20Integration%20(U).pdf

Freeman , J., Cohen , M., Serfaty , D., Thompson , B., & Bresnick , T. (1997). *Training in Information Management for Army Brigade and Battalion staff: methods and*

preiminary findings. Hentet fra Google scholar, utgitt av: United States Army Research Intitute for the Behavorial and Social Sciences: https://books.google.no/books?hl=en&lr=&id=g64rAAAAYAAJ&oi=fnd&pg=PA1&dq=information+management+army&ots=G8fp66cwQ8&sig=hD2WDGqlDHUfuPHcjvrhyZBsa0Q&redir_esc=y#v=onepage&q=information%20management%20army&f=false

ITU-R. (2015). *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond.* Geneva: ITU.

JCIDS. (2012). *MANUAL FOR THE OPERATION OF THE JOINT CAPABILITIES INTEGRATION*. fra Acqnotes: https://www.acqnotes.com/Attachments/JCIDS%20Manual%20for%20the%20Operation%20of%20the%20JCIDS%20%2019%20Jan%202012.pdf

Johannessen, A., Tufte , P., & Christoffersen , L. (2010). *Introduksjon til samfunnsvitenskapelig metode.* Oslo: Abstrakt forlag.

Kucukaksoy, I. (2016). NATO CAPABILITY DEVELOPMENT. *The Three Swords Magazine*, ss. 12-15. Hentet fra https://www.jwc.nato.int/images/stories/_news_items_/2016/LT_GEN_Lofgren_interview.pdf

Leraand, D. (2022, desember 2022). *hær*. Hentet Mars 28, 2023 fra snl.no: https://snl.no/h%C3%A6r

Marr, B. (2018, Jul 30). *9 Powerful Real-World Applications Of Augmented Reality (AR) Today*. Hentet fra forbes.com: https://www.forbes.com/sites/bernardmarr/2018/07/30/9-powerful-real-world-applications-of-augmented-reality-ar-today/?sh=25443d952fe9

Microsoft. (2023). *What is augmented reality or AR?* Hentet Mars 28, 2023 fra Microsoft Dynamics 365: https://dynamics.microsoft.com/en-us/mixed-reality/guides/what-is-augmented-reality-ar/

NATO

NATO. (2022). *AJP 3-2 ALLIED JOINT DOCTRINE FOR LAND OPERATIONS* (Edition B, Version 1. utg.). Brüssel: NATO STANDARDIZATION OFFICE.

NIST. (2019, Jul). *COMPUTER SECURITY RESOURCE CENTER*. Hentet Mars 28, 2023 fra NIST: https://csrc.nist.gov/glossary/term/commercial_off_the_shelf

NSM. (2020, Juni 11). : https://nsm.no/fagomrader/digital-sikkerhet/it-sikkerhet/

Sikkerhetsklarering: https://nsm.no/fagomrader/personellsikkerhet/sikkerhetsklarering/

Oktay, J. S. (2012). *Grounded Theory* . Oxford : Oxford Univeristy Press .

Richards, C. (2020). Boyd's OODA-loop. *Necesse*.

Savage, O. (2023, Mars 07). British Army selects TAK for Dismounted Situational Awareness programme. Hentet Mars 20, 2023 fra https://www.janes.com/defence-news/news-detail/british-army-selects-tak-for-dismounted-situational-awareness-programme

Sikkerhetsloven . (2019, Jan 01). *Sikkeretsloven*. Hentet fra Lov om nasjonal sikkerhet (sikkerhetsloven): https://lovdata.no/dokument/NL/lov/2018-06-01-24#KAPITTEL_5

Telenor. (2023). *Alt du vil vite om dekning*. Hentet Mars 23, 2023 fra telenor.no: https://www.telenor.no/dekning/

Trick, C. (2022, Juni 17). *What is COTS (Commercial-off-the-shelf)*. Hentet Mars 27, 2023 fra trentonsystems.com: https://www.trentonsystems.com/blog/what-is-cots-commercial-off-the-shelf

Valle, M. (2009, Jan 16). *Tek.no* . Hentet fra Hva er egentlig 4g? : https://www.tek.no/nyheter/guide/i/dObWyO/hva-er-egentlig-4g#hva-kan-jeg-bruke-det-til

Vellan, S.-E. (2020, Mai). *5G*. : http://smooth-storage.aptoma.no/users/drp-nettavisen-upload/files/Nyheter/Telia_5G.pdf

Voldhaug , J., Hansen , B. J., Lund , K., Mykkeltveit , A., Rytir , M., & Bentstuen , O. (2021). *Hvordan kan ny IKT gjøre Forsvaret bedre?* Oslo: FFI.

7. Vedlegg

Publiseringsavtale

En avtale om elektronisk publisering av bachelor/prosjektoppgave

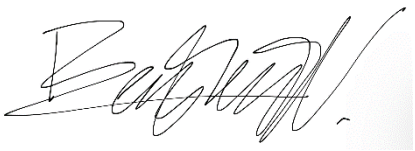
Kadetten(ene) har opphavsrett til oppgaven, inkludert rettighetene til å publisere den.
Alle oppgaver som oppfyller kravene til publisering vil bli registrert og publisert i Bibsys Brage når kadetten(ene) har godkjent publisering.
Oppgaver som er graderte eller begrenset av en inngått avtale vil ikke bli publisert.

Jeg (Vi) gir herved FHS Krigsskolen rett til å gjøre denne oppgaven tilgjengelig elektronisk, gratis og uten kostnader	Ja	Nei
Finnes det en avtale om forsinket eller kun intern publisering? (Utfyllende opplysninger må fylles ut) Hvis ja: kan oppgaven publiseres elektronisk når embargoperioden utløper?	X Ja Ja	 X Nei Nei

Plagiaterklæring

Jeg (Vi) erklærer herved at oppgaven er mitt eget arbeid og med bruk av riktig kildehenvisning. Jeg (Vi) har ikke nyttet annen hjelp enn det som er beskrevet i oppgaven.
Jeg (Vi) er klar over at brudd på dette vil føre til avvisning av oppgaven.

Dato: 31.03.2023



Kadett, signatur – Benjamin S. Nordén
31.03.23

Kadett, signatur – Emil Øhre Skiaker
31.03.23