FORSVARET
Forsvarets høgskole

Russisk teknologi og nye trusler

- *norsk hærkultur til besvær?*

Rine Veberg

Masteroppgave
Forsvarets høgskole
vår 2020

Forord

Har du noen gang tatt fatt på en masteroppgave og tenkt at du ikke ble grepet eller spesielt truffet av forordet? Det har jeg. Jeg har tatt meg selv i å ikke fullt ut forstå hvilket formål oppgavens forord tjener, med dens dype bekjennelser, gjennomsyret av takknemlighet. Så begynte jeg på denne reisen, som det virkelig er. Som du trolig ikke har full respekt for før du står der, observerer det på nært hold eller kjenner på den jevne strømmen av dårlig samvittighet og akademisk utilstrekkelighet. Den personlige reisen, den kan sammenlignes med lite annet. Nå tenker jeg blant annet at det er utrolig fascinerende hvordan man starter med blanke ark, som en oppriktig idealist med genuine ønsker om å forandre verden, og ender opp som en noe mer kynisk realist. Denne formingsprosessen er nok helt nødvendig og ordinær for enhver som skriver master, men ikke mindre interessant av den grunn.

Og plutselig satt jeg der selv og skrev det samme forordet, med de samme stereotypiske formuleringene. For jeg trodde faktisk ikke at jeg ville være i stand til å møte innleveringskravet på masteren i året 2020. Men, heldigvis er det mange arbeidstimer i et helt år. Og i tillegg, mange som på tross av sin tidsklemme klarer å klemme inn sparring, tilbakemeldinger, moralsk støtte og direkte korrigeringer. Det har jeg både tidligere kollegaer, nåværende kollegaer og en inspirerende veileder å takke for. For å lede noen på veien mot en master må man være en akademisk balansekunster og realist, hvilket jeg vil berømme Kjell Inge Bjerga ved IFS for å være. Takk for utfordring, støtte og et herlig engasjement gjennom året!

Sammendrag

Denne oppgaven er todelt og ser på hva som kjennetegner en russisk teknologisk motstander i landdomenet, og på hvordan et utvalg av ledere i Hæren forstår det teknologiske stridsfeltet, med mulige forklaringer på deres fortåelseshorisont og forestillingsevne.

Striden i landdomenet preges i dag av en teknologisk utvikling som skaper mer potente trusler. Utviklingen som påvirker striden blir knyttet til syv kategorier som studien redegjør for. Satsingen på kapasiteter og områder som asymmetrisk demmer opp for vår egen utvikling utgjør en større fare i dét de blir mer presise, mer effektive og tempoet øker. Det er ikke banebrytende teknologi som representerer taktskiftet i striden som føres i landdomenet – det er først og fremst *teknologisk evolusjon*. Dette bidrar til at Russland bør anses som en teknologisk motstander for landmakten.

Oppgaven ser deretter på hva et utvalg ledere i Hæren kan om teknologiske trusler og hvordan de vurderer egen kompetanse. Analysen viser at militære ledere bare har en begrenset evne til å forestille seg det teknologiske stridsfeltet. Dette gjelder ikke-kinetiske maktmidler og mer tekniske aspekter ved dagens krigføring. Her viser også utvalget av ledere en tendens til å overvurdere egen kompetanse. Flere kognitive skjevheter kommer til syne når militære ledere skal behandle spørsmål knyttet til mer komplekse trusler.

I lys av dette går studien videre inn på hypoteser. Det blir fremlagt seks hypoteser med forklaringskraft for hvorfor kunnskapen er lavere på enkelte felter og hvorfor de overvurderer egen kunnskap og innsikt. Felles for alle hypotesene er at de kan sammenfattes med *organisasjonskultur*. Å møte på det teknologiske stridsfeltet med gårsdagens lærdommer kan bli dødelig. Studien konkluderer derfor med at organisasjonskulturen i Hæren svekker militære lederes forestillingsevne om det teknologiske operasjonsmiljøet.

Summary

This thesis is divided into two main components: One analyzes how a Russian technological opponent within the land domain looks and what technological capacities consists of. The second part analyzes how much knowledge military commanders in the Army have about a technological opponent, and how they perceive their own competence and insight.

The technological battlespace will be affected by a technological development that creates more potent threats. This development is tracked through seven categories that this study accounts for. Investment in capacities and in areas that represent an asymmetric development to the Western approach creates new threats as technology advances towards a higher degree of precision, more effect and a significantly higher tempo. It is not high end technology or innovative and unimaginable devices that evokes the operational shift in the land domain – it is first and foremost *technological evolution.*

The thesis goes on to examine the competency of military commanders related to technological threats, and how they perceive their own competence. The analysis displays that military commanders at a tactical level in the Army have a very limited view and notion of technological threats. When addressing non-kinetic sections of the battlefield and how they relate to kinetic means, the commanders show an inadequate ability to envision how they can be utilized. The analysis substantiates that military commanders in the Army are affected by cognitive biases when assessing a possible future armed conflict.

Based on this analysis, six main hypotheses are presented in order to shed light on why certain areas of knowledge and expertise are limited, and why there is a tendency for commanders to overrate their own knowledge. The common denominator for all of these factors is – *organizational culture.* The study therefore claims that a dimensional threat on the technological battlefield is our own military commanders - and how they think and perceive.

Innholdsfortegnelse

Figurliste

1 Innledning

> Den teknologiske utviklingen skjer nå i et omfang og med en hastighet og en potensiell effekt på samfunnet som har likhetstrekk med en teknologisk revolusjon. Endringene påvirker alle politikkområder og sektorer, hvor konsekvensene for samfunnet og for forsvarssektoren er sammensatte og krevende å forutse. (Forsvarsdepartmentet, 2020, s. 18).

Forsvarsdepartmentet omtaler i den nye langtidsplanen noen av dagens sikkerhets- og forsvarspolitiske rammer og føringer. Etter global maktforskyvning og endringer i verdensorden følger teknologiens betydning og bruken av sammensatte virkemidler. Det vies det stor oppmerksomhet til kunstig intelligens, automatisering, robotisering, nanoteknologi og stordatabehandling. På disse feltene er det viktig å både konkurrere om fortrinnet og ha nær kontroll inn i fremtiden. Imidlertid vil studien hevde at det ikke denne utviklingen som preger stridsfeltet lenger nede i hierarkiet i dag, og som skaper en ny dynamikk. Derfor kan det være viktig å ikke bli for fremoverskuende i teknologiutviklingen – fordi dagens utvikling er moderat og evolusjonær, men representerer fortsatt et betydelig skifte på det teknologiske stridsfeltet.

Det teknologiske stridsfeltet ses på gjennom to linser i denne studien. Den første delen ser på hvordan russisk teknologisk landmakt ser ut og hva som vil prege teknologisk strid. Den andre delen undersøker i forlengelsen av dette hvor oppdaterte militære ledere er om disse teknologiske truslene og hvordan de oppfatter eget kompetansenivå. Så går studien videre i å analysere hypoteser som kan være med på å forklare militære lederes forståelse for og innsikt i teknologisk strid.

I den første delen vil studien vise at Russland bør oppfattes som en teknologisk motstander for landmakten. Evolusjonsbasert teknologi knyttes sammen og utgjør stadig mer potente trusler i landdomenet. Dette er med på å utforme en ny dynamikk i hvordan kamper utkjempes på taktisk nivå.

I den andre delen vil studien vise at Hærens ledere bare i begrenset grad klarer å forestille seg kompleksiteten i de teknologiske truslene og hvordan dette vil utspille seg som deler av

operasjonsmiljøet. Studien vil også vise at en overvekt av lederne overvurderer egen kompetanse om teknologiske trusler, med konsekvensene dette kan innebære for fremtiden.

Så vil studien sannsynliggjøre at det er organisasjonskulturen som former militære lederes forestilling av teknologisk strid. I dette bildet fremstår utvalget av militære ledere som et produkt av en sterk, konservativ og tradisjonsrik hærkultur. Dette utgjør en dimensjonerende trussel i møte med sammensatte virkemidler i et teknologisk drevet operasjonsmiljø.

1.1 Problemstillinger

Norge har siden 2014 vært på toppen blant verdens 5 mest digitaliserte land (Business Finland, 2019, s. 58). På felter som omhandler eksempelvis kunstig intelligens eller autonome systemer blir også Norge fremhevet som en verdensledende nasjon (FFI, 2016, s. 12). Hva gjelder teknologi og digitalisering, kan studier som dette forsterke inntrykket av at Norge ligger langt fremme på verdensbasis. Russland, på den andre siden, blir gjerne fremstilt som en stormakt som i økende grad har blitt stilt overfor økonomiske dilemmaer som har potensialet til å gå på bekostning av forsvarsinvesteringer og teknologisk utvikling (Dyndal, 2019). Dette synet på Russland kan fordreie inntrykket av den reelle komparative kampkraften på stridsfeltet. Gjennom den amerikanske hærens nye doktrinetilnærming med *Multi-Domain Operations* ser man at konseptene springer ut fra erkjennelsen av at Russland til dels har et overtak innenfor artilleri, EK, kampkjøretøy, luftvern, cyber og romkapasiteter (Werkheiser, 2020, s. 4). Det at man vil bli utfordret og må utkjempe en kamp i alle domener synes å være svært retningsgivende for både USA og NATO.

Den teknologiske utviklingen medfører at kostnader på deler og kapasiteter reduseres kraftig og tilgjengeligheten øker dramatisk. Dette, koblet med industrispionasje, lekkasjer, konkurranseutsetting og kommersialisering i sivil-militære markeder og en mer global forsvarsindustri, leder til at nye produkter raskere vil finne veien til det militære systemet og mellom systemene. Spredning av informasjon og teknologi foregår i en så høy hastighet at kapabilitetsoverlegenhet er et høyst flyktig fenomen. Overlegenhet er både temporært og kortlivet (Schmuel, 2017). Det er under disse skiftende omstendighetene at det neste slaget kan komme til å stå, og det vil være noe annet enn Afghanistan eller Irak, hvor vestlig teknologisk dominans har vært realiteten.

Dette leder til følgende forskningsspørsmål for masteroppgaven:

1. *Hvilke teknologiske kapasiteter besitter Russland og hva vil kjennetegne en mer teknologisk strid?*
2. *Hvilken forestillingsevne har et utvalg ledere i Hæren om en teknologisk motstander?*
3. *Hva kan forklare ledernes kunnskapsnivå, forestillingsevne og selvforståelse?*

1.2 Avgrensninger

Det er sentralt at oppgaven forblir ugradert, for å gjøre både oppgaven, diskusjoner og debatt tilgjengelig. Dette vil gi mer verdi for organisasjonen Forsvaret og Hæren. Det vil medføre at enkelte relevante detaljer vil måtte utelates og at nyansene ikke vil fremstilles like klart som i vurderinger fra eksempelvis Etterretningstjenesten. Dette kan trolig bidra til at Russlands kapasitetsutvikling kan fremstå som overdimensjonert eller som mer truende enn hva virkeligheten tilsier. Dette vil nok ikke representere den fulle sannhet, men være nødvendig for å skape et samlet bilde av Russlands utvikling.

Med tanke på læring og nytteverdi er det viktig at oppgaven vil anses som enkel, forståelig og inviterende for ulike målgrupper i Hæren. Dette kan representere en svakhet i det at kapasitetene ikke fremstår som detaljerte eller tekniske nok, men er et bevisst valg for å favne om et bredere publikum. Det vil si at tekniske aspekter vil reduseres, men heller visualiseres og generaliseres.

Oppgaven vil sentreres rundt det taktiske nivået i Hæren, hvor jeg selv har kompetanse, innsikt og forståelse til å tilføre ny kunnskap eller nye perspektiver. Det taktiske nivået vil også være utgangspunktet fordi mer og mer ressurser blir delegert nedover i organisasjonen. Forsvarets Fellesoperative doktrine understreker også betydningen av at det vil foregå et taktisk samvirke på lavere nivåer enn tidligere (FFOD, 2019, s. 3). Flere av ressursene på eksempelvis russisk side er organisk underlagt andre forsvarsgrener enn Hæren, men er nødvendige å belyse. Dette kommer av at oppgaven ønsker å presentere kompleksiteten for

den lederen på det taktiske nivået, der man med overhengende sannsynlighet kan si at styrkene vil samvirke med Hæren eller operere parallellt. Likevel vil maritime styrker og luftmakten regnes ut av oppgaven, for å gjøre oppgaven håndterlig og forståelig nok.

Spesialister defineres også som Hærens ledere og kunne således vært innlemmet i denne oppgaven. Fordi utdanningen innenfor taktikk og samvirke skiller seg mellom offisersutdanningen og den videregående befalsutdanningen (VBU), vil jeg likevel ikke se mot begge lederne i «command teamet». Offiseren gjennomgår en tyngre utdanning innen plan- og beslutningsprosessen på tropp-, kompani- og bataljonsnivået enn hva sersjantkorpset gjør, i tillegg til at offiseren står i kommandoforholdet med det ultimate ansvaret for sin avdeling. Jeg vil derfor konsentrere meg om offiseren.

1.3 Metode og kilder

Oppgavens design er basert på en kvalitativ tilnærming, hvor en todelt struktur vil bli benyttet. Første del vil kartlegge russiske teknologiske kapasiteter basert på en kvalitativ dokumentstudie av primært forskningsrapporter. Her vil oppgaven bruke kilder med faglig tyngde, som institutter og fagavdelinger i USA, England, Sverige, Estland og lignende. Deretter vil arbeidet kompletteres av norske kilder og forskning, samt åpne kilder (som Wikipedia og Army Recognition) for å kalibrere kilder med siste trender for teknologisk krigføring. Dette defineres i samfunnsvitenskapelig metode som sekundærkilder, og nyttes fordi det ikke finnes praktisk, pålitelig eller tilgjengelige primærkilder som kan integreres i oppgaven (Jacobsen, 2018, s. 171). Det kan være krevende å finne informasjon som nyanserer utviklingen av teknologi, budsjettbevilgninger og den faktiske utviklingen i Russland. Dette kan føre til en metodisk skjevhet i favør av motstanderen, hvilket vil synliggjøres i studien.

Andre del av studien vil gjennomføres som individuelle kvalitative intervjuer med et utvalg av seks militære ledere i Hæren, fra Krigsskolen til og med kompanisjef. Intervjuene vil være semi-strukturerte, hvor første del tar for seg generelle spørsmål knyttet til hvor viktig det er å ha oppdatert kunnskap om operasjonsmiljøet, hvor man henter informasjon og hvem som bærer ansvaret for at personellet er oppdatert. Den andre delen vil først introdusere funnene fra kapittel 2 i en PDF (Vedlegg 2). Hvert intervjuobjekt får 15-20 minutter til å lese gjennom

PDFen på egenhånd. Deretter vil de få fire spørsmål rettet mot hvordan de vurderer informasjonen på syv kapasitetesområder hvor man kan spore teknologisk utvikling. Avslutningsvis vil de få spørsmål om de har fått tilført ny kunnskap utledet av kapittel 2, og om de har øvrige kommentarer.

Utvalget av militære ledere på taktisk nivå skal representere offiserer og ledere med ekspertise innenfor landmakt. Det er valgt ut seks intervjuobjekter til denne kvalitative forskningsdelen. Dette er i seg selv et lite antall intervjuobjekter, men nødvendig for å kunne håndtere dataene innenfor tidsrommet som er gitt for masteroppgaven (Jacobsen, 2018, s. 178). Utvalgets oppfatninger og fortolkninger vil anonymiseres for å kunne bevare interessante perspektiver uten frykt for konsekvenser. Intervjuene vil også gjennomføres over skype eller facetime og tas opp. Dette er for å kunne gjennomføre med planlagt utvalg, fordi flere har status som pendlere og har blitt rammet av koronakrisen i Norge. Dette anses ikke som en optimal metode, men som et nødvendig tiltak.

1.4 Oppgavens struktur

Jeg vil her enkelt fremstille oppgavens struktur og kort redegjøre for målet med hvert kapittel. Oppgaven vil konsentreres rundt henholdsvis kapittel 2, 3 og 4 for å besvare forskningsspørsmålene.

Kapittel 2 vil kartlegge og beskrive hvilke teknologiske kapasiteter Russland primært besitter i dag innenfor syv kapasitetsområder. Kapittelet vil fokusere på det taktiske nivået med støtte og ressurser som kan spores til russiske operasjoner. Det sentrale er teknologiske kapasiteter og implikasjoner dette kan få for en motstander. Dette vil danne utgangspunktet for intervjuene i neste kapittel, i rammen av russisk aggressjon mot Finnmark (Vedlegg 2).

I Kapittel 3 vil intervjuobjektene svare på hva de kan om en teknologisk motstander, og om militære ledere har en virkelighetsnær og god forestilling av den teknologiske striden.

Kapittel 4 vil se nærmere på mulige forklaringer på ledernes kunnskapsnivå, forestillingsevne og selvforsåelse.

Kapittel 5 vil oppsummere funn fra kapitlene. Helhetlig sett vil oppgaven gi svar på hvordan en teknologisk motstander ser ut, hva ledere kan om teknologiske trusler og hvordan de forestiller seg dette stridsfeltet, og til slutt skissere en forklaringsmodell for hvorfor kunnskap om teknologiske trusler er relativt lav.

1.5 Teori

For å analysere datamaterialet fra intervjuene i studien vil en underkategori av feltet kognitiv psykologi benyttes. Kognitiv psykologi kan favne bredt om menneskelige mentale prosesser, som oppfatning, tenkning og kunnskapservervelse (Store Norske Leksikon, 2020). Disse prosessene kan blant annet bestå av persepsjon, forestillingsvirksomhet, hukommelse, bedømming, resonnering og problemløsning (Store Norske Leksikon, 2020). Prosessene utgjør et interessant rammeverk for å vurdere og analysere hvordan militære ledere oppfatter sin egen kunnskap og innsikt, og hvordan de resonnerer rundt tidligere kunnskap koblet med tilgangen på mulig ny kunnskap.

Et mer avgrenset område innenfor kognitiv psykologi tar for seg heuristikker og kognitive biaser. Heuristikker er regler i hjernen som bidrar til å forenkle mer komplekse utfordringer. Dette er nødvendig for å være mer effektive i å løse problemer i hverdagen, men kan også føre til snarveier som over tid kan utgjøre mer systematiske mentale skjevheter (Beadle, 2016, s. 101). Dette blir også ofte referert til som kognitive fallgruver, fordi skadepotensialet ved disse ubevisste prosessene kan være stort. Dette arbeidet er også satt i en norsk militær kontekst gjennom Beadles FFI rapport fra 2016; *Å forske på Forsvaret i fremtiden: muligheter, begrensninger og kogntive fallgruver*. I denne rapporten utvides perspektivet også fra det rent psykologifaglige til en mer helhetlig tilnærming som tar opp i seg også kontekstuelle forhold og mer sammensatte forklaringer når det gjelder hva som kan påvirke forståelsen av militære forhold (se figur 1 nedenfor).

I figuren er det gjengitt eksempler og beskrivelser på en del kognitive mekanismer som er relevante for militære yrkesutøvere. Som et eksempel kan dette være bekreftelsestendensen. Dette kjennetegnes ved tendensen til å søke etter eller legge merke til informasjon som bekrefter det vi allerede vet (Beadle, 2016, s101). På den andre siden kan dette gjøre at vi ikke tar hensyn til ny informasjon som tilsier at vi burde ha endret mening. Derfor kan det være farlig for ledere å eksempelvis «låse» seg til løsninger på taktiske problemer og søke informasjon som bekrefter dette. I ytterste konsekvens kan det gjøre lederen tilbøyelig til å undervurdere eller forkaste informasjon som endrer forutsetningene for planen. Disse kognitive skjevhetene er menneskelige og delvis nødvendige, men de er også viktige å ha et bevisst forhold til, kanskje spesielt som militære ledere. Det må tilføyes at tabellen neppe er utfyllende, men den er hensiktsmessig som et utgangspunkt for analysene i kapittel tre og fire i denne oppgaven.

Psykologiske mekanismer	***Beskrivelse***
Kognitiv letthet (cognitive ease)	En tilstand av tilfredsstillelse, der vi ikke opplever et behov for mentale anstrengelser. Denne lettheten kan skapes av gjentagelser, klare visuelle fremstillinger, fet skrift, godt humør og opplysninger som gjør oss mindre på vakt. Det gir samtidig en falsk sikkerhetsfølelse, fordi det svekker vår kritiske sans, gjør oss mer tilbøyelig til å tro at ting er sant og at vi vet mer enn vi gjør.
Kognitiv anspenthet (cognitive strain)	Det motsatte av kognitiv letthet. Anspenthet utløses av en opplevelse av at det er et problem som må løses og som krever mobilisering av tankekraft, f.eks. når du leser tekst med uklare bokstaver eller vanskelig språk. Det gjør deg samtidig mer årvåken, engasjert og du vil trolig begå færre feil i vurderingen.
Heuristikker (heuristics)	Samlebetegnelse for enkle, effektive regler som hjernen vår bruker til å gjøre vurderinger og ta avgjørelser. De er mentale snarveier som reduserer komplekse problemer til enklere kognitive oppgaver og gjør at vi bestemmer oss raskere. I de fleste tilfeller gjør snarveiene hverdagen enklere og mer effektiv, men de kan også lede til systematiske skjevheter (*kognitive biaser*), som fører til alvorlige feil i alt fra risikoanalyser til rettsaksavgjørelser.
Kognitive biaser (cognitive biases)	Utsagn, valg og vurderinger som systematisk avviker fra det som stemmer overens med virkeligheten, f.eks. sannsynligheter.
Bekreftelsestendens (confirmation bias)	Det at vi legger merke til eller søker etter informasjon som bekrefter det vi allerede tror. Denne tendensen gjør samtidig at vi overser informasjon som tilsier at vi burde endre oppfatning.
Kognitiv refleksjon (cognitive reflection)	Evnen til å motvirke umiddelbare og intuitive vurderinger, som kan testes ved hjelp av f.eks. tennisracket og ball-oppgaven.
Kognitiv lukking (cognitive closure)	Det som skjer når vi gir etter for aversjonen mot tvetydighet og usikkerhet. Vi forsøker da å oppnå lukkethet så raskt som mulig og beholde denne lukketheten så lenge man kan. Behovet for lukkethet er sterkere hos noen personer og i pressede situasjoner.
Troen på de små talls lov (belief in the law of small numbers)	Der vi forventer at observasjonene vi gjør av små utvalg er mer representative for populasjonen enn de egentlig er, undervurderer den store variasjonen vi kan få, og forventer at ett ekstremt utslag vil bli utlignet av et annet – slik det er ved *store* utvalg.

Representasjonsheuristikk (representativeness)	Der vi bedømmer sannsynlighet ut fra likhet og typiskhet. Dette fører til konjunksjonsfeilslutninger, der vi antar at spesifikke forhold er mer sannsynlige enn generelle, f.eks. at det er større sannsynlighet for at en person som beskrives som feminin er både bankkasserer *og* feminist, ikke bare én av delene. *The wrong side of maybe* En feilslutning der vi i retrospekt har en tendens til å tolke vage formuleringer slik at de faller på riktig side av *maybe*-grensen (50/50). Konsekvensen kan være at vi fortsetter å predikere galt uten at det får konsekvenser for fremgangsmåten.
Etterpåklokskap (hindsight bias)	Der vi har en overdreven tro på at det som skjedde, kunne predikeres («Jeg visste det hele tiden»). Jo verre konsekvensene av en hendelse er, jo mer tilbøyelig er vi også til å tro at de som ikke forutså hendelsen var skjødesløse. Tenk på 9/11 eller 9. april.
Overkonfidens (overconfidence)	Der vi er sikrere på våre prediksjoner enn det er grunnlag for å være. Svar som folk oppgir å være «99 % sikre», er ofte gale. Overkonfidens kan øke sjansen for risikable valg og redusere tilbøyeligheten til å revurdere tidligere beslutninger.
Mulighetseffekten (possibility effect)	Der hendelser med svært lav sannsynlighet (som 1 %, 2 % og 5 %) blir vektet uforholdsmessig mye, fordi vi opplever en kvalitativ endring av at noe går fra å være «ikke mulig» til «mulig». Dette har vi en tendens til å overreagere på, spesielt dersom det er dramatiske følger involvert. Vi opplever f.eks. terrorangrep og flystyrter som langt mer sannsynlig enn de statistisk sett er.
Blindhet for sorte svaner (Black Swan blindness)	Der vi undervurderer rollen til store, overraskende hendelser, eller overvurderer betydningen av én spesifikk en. Fordi sorte svaner skaper uvisshet, later vi i stedet som om at de ikke finnes. Dette kan skje hvis hendelsene aldri har skjedd før eller fordi konsekvensene er så uvirkelige at vi ikke klarer å tenke på dem en gang (som en atomkrig). I forsvarsplanlegging er faren at vi forveksler det ukjente med det umulige.
Ankring (anchoring)	Der vi starter med et tall (ankeret) og justerer beregningene våre deretter. Dette ankeret, f.eks. en statistisk opplysning, dominerer så totalinntrykket. Et dårlig anker kan bety at vi ikke justerer nok, og det er overraskende lett å begynne med et dårlig anker.
Underreaksjon (underreaction)	Der vi justerer vurderingene våre for lite i lys av ny informasjon, bl.a. fordi vi har en *sterk* tilknytting til saken det angår.
Overreaksjon (overreaction)	Der vi justerer vurderingene våre for mye i lys av ny informasjon, bl.a. fordi vi har en *svak* tilknytting til saken det angår.
Oppfatningsutholdenhet (belief perseverance)	Tendensen til å opprettholde vår opprinnelige oppfatning når det kommer ny informasjon som utfordrer vår eksisterende tro.
Bumerangeffekten (boomerang effect)	Der en persons dedikasjon til en bestemt posisjon øker når vedkommende blir angrepet for den, også selv om den i utgangspunkt ikke var veldig sterk. Dette skjer spesielt hvis konsekvensene av beslutningene de allerede har tatt, har vært uheldige.
Kohortforskjell (cohort difference)	Der grupper av personer i en populasjon som opplever en betydningsfull livsbegivenhet i samme tidsrom skiller seg fra andre grupper som ikke gjorde det, f.eks. den kalde krigen eller 9/11.
Affektheuristikk (affect heuristic)	Der vi lar våre følelser, ubevisst eller bevisst, påvirke vurderinger, beslutninger og hvilke overbevisninger vi har. De politiske preferansene dine vil f.eks. styre hvilke argumenter du finner overbevisende. Den største faren er at følelsene våre påvirker nytteverdien og risikoene vi tillegger innføring av nye systemer og ny teknologi, uten at vi har informasjon om begge deler.
Glorieeffekten (halo effect)	Der vi har en tendens til å like eller mislike alt ved en person, også ting vi ikke har observert. Militære omstillingsprosesser forbindes ofte med enkeltindivider, der et tidligere førsteinntrykk kan styre hva vi synes om det personen foreslår senere, selv om dette er to helt forskjellige saksforhold.
Tilgjengelighetsheuristikk (availability heuristic)	Der sannsynligheten for noe vurder es ut i fra hvor *lett* man kan kommer på lignende tilfeller, ikke hvor vanlig de er statistisk sett. Tilgjengeligheten forsterkes av følelsesmessige reaksjoner, der dramatiske hendelser som en flystyrt eller russisk invasjon, gjør lignende hendelser mer «tilgjengelig» og derfor vurderes som mer sannsynlig, f.eks. i våre egne nærområder.

Figur 1. Relevante psykologiske mekanismer for Forsvaret.. Fra «Å forske på forsvaret i fremtiden - muligheter, begrensninger og kognitive fallgruver», FFI-rapport 2016/01810, av Beadle, 2016, s. 101-103.

2 Russland - en teknologisk motstander

Hvordan ser en relevant teknologisk motstander ut og hva kjennetegner teknologisk strid? Dette er hovedspørsmålene som vil bli besvart i dette kapittelet. Analysen tar utgangspunkt i Russland og en avgrenset del av den russiske hæren. Hvilke teknologiske felter representerer et mulig skifte fra tidligere motstandere? Hvordan har dette påvirket operasjonsmetoder og prosedyrer på bakken? Hvilke implikasjoner kan dette få for den norske hæren ved en konfronatsjon med russiske landstyrker?

For å kartlegge motstanderen er det nødvendig å først rette et blikk mot faktorer som kan bidra til å forstå utviklingen mer overordnet. Derfor vil organisasjonsstruktur, personellreformer, trening og lederskap være den overordnede forutsetningen for å sette teknologien i en sammenheng.

2.1 Rammer og faktorer for teknologisk utvikling

Russland har det siste tiåret vært preget av militære reformer hvor forsvarssatsingen har blitt opprettholdt, selv under økonomisk stagnasjon (Etterretningstjenesten, 2020, s. 47). Erfaringene fra konflikten i Georgia 2008, med påfølgende erfaringer fra Ukraina og Syria virker å ha vært dimensjonerende for hvordan reformene har utviklet seg (Kofman, 2018, s. 3; Defence Intelligence Agency [DIA], 2017, s. 12-13; Skjelland et. al., 2019, s. 18-21).

Den første endringen som er viktig å hensynta er den profilerte distriktsreformen fra 2008, som en del av *New Look* reformen (Grau og Bartles, 2016, s. 28). Fra 2008 har styrkene omorganisert fra å bestå av seks militærdistrikter til fire, og fra store og tunge divisjons- og regimentstrukturer til flere mindre brigader og en flatere organisasjonsstruktur (Asymmetric Warfare Group [AWG], 2016, s. 1). Det vil si mindre enheter med flere støtteressurser underlagt i sin organisasjon. For å møte kravet om å bli mer asymmetriske og nettverkssentriske, måtte også strukturen tilpasses til mindre og mer mobile bataljonsstridsgrupper i det gjeldende våpenprogrammet, 2018-2027 (DIA, 2017, s. 52). En mobil og ekspedisjonær styrke med evnen til å utføre operasjoner i hele Russlands sfære, kom til uttrykk gjennom annekteringen av Krimhalvøya og konflikten i Øst-Ukraina (DIA, 2017, s. 52). Etter 2013 mener det svenske forskningsinstituttet å kunne sannsynliggjøre at det vestlige

og sørlige militærdistriktet, er styrket i evnen til å føre væpnet konflikt. Strukturreformer har trolig bidratt positivt til utviklingen av kampkraft i den russiske hæren (Persson et. al., 2016, s. 92).

Den andre endringen i rammefaktorene er personellreformene. Omorganiseringen til mindre brigadeenheter i 2008 siktet på å fullbemanne den russiske strukturen og stille til rådighet mer robuste og selvforsynte enheter (Lavrov, 2018, s. 2). Mellom 2008 og 2017 har reformene også endret personellsammensetningen fra en stor andel offiserer, befal og vernepliktige til en mye større andel profesjonelle soldater (Lavrov, 2018, s. 2; Radin et. al., 2019b, s. 42; IISS, 2019, s. 169). Dette bidro til at Russland kunne bruke utelukkende profesjonelle soldater både på Krim, øst i Ukraina og Syria - i stedet for vernepliktige (Lavrov, 2018, s. 3). Hver brigade skal etter planen sette opp én bataljon bestående av kun profesjonelle soldater. I støttestrukturen blir det i større grad benyttet vernepliktige soldater, men på grunn av grunnloven og prioritering av personell, ser det fortsatt ut til at profesjonelle soldater blir foretrukket der Russland er i en form for væpnet konflikt. I tillegg kan det også spores endringer i lønn og status, samt tiltak mot korrupsjon fra 2008 (Radin et. al., 2019b, s. 53-57). Denne profesjonaliseringen av soldatkorpset vil også bære potensialet til å skape en organisasjon med større kampkraft.

Personellets kompetanse er tredje faktor av betydning. Kompetanseheving kan ses igjen i tiltak rettet mot trening og øving, spesielt etter 2013. Det har blitt gjennomført et større antall inspeksjoner av avdelingene, mer komplekse tosidige øvelser, store nasjonale øvelser, internasjonale øvelser og sportskonkurranser. I tillegg har Russland iverksatt *snap-exercises*, hvor beredskap og mobilitet har blitt spesielt testet gjennom uventede øvelser på nasjonal basis (Radin et. al., 2019b, s. 58). I disse øvelsene har man siden 2013 også involvert sivilt reservepersonell (Radin et. al., 2019b, s. 58). Disse tiltakene har trolig bidratt til å heve personellets kompetanse og treningsnivå (Lavrov, 2018, s. 4). At kompetansen har økt kan også sannsynliggjøres gjennom et økt ammunsjonsforbruk med fem til syv ganger siden 2012, og drivstofforbruket med tre ganger (Lavrov, 2018, s. 4.). Dette må ses i sammenheng med operasjonene Russland har vært involvert i siden 2014, hvor mange styrker har fått kamperfaring. Syria og Ukraina har også blitt arenaer hvor nye taktikker og nytt materiell har blitt testet, og således økt treningsstandarden på personellet. Det er meget sannsynlig at mer relevant trening, øving og operasjoner skaper mer kompetente og kampklare avdelinger.

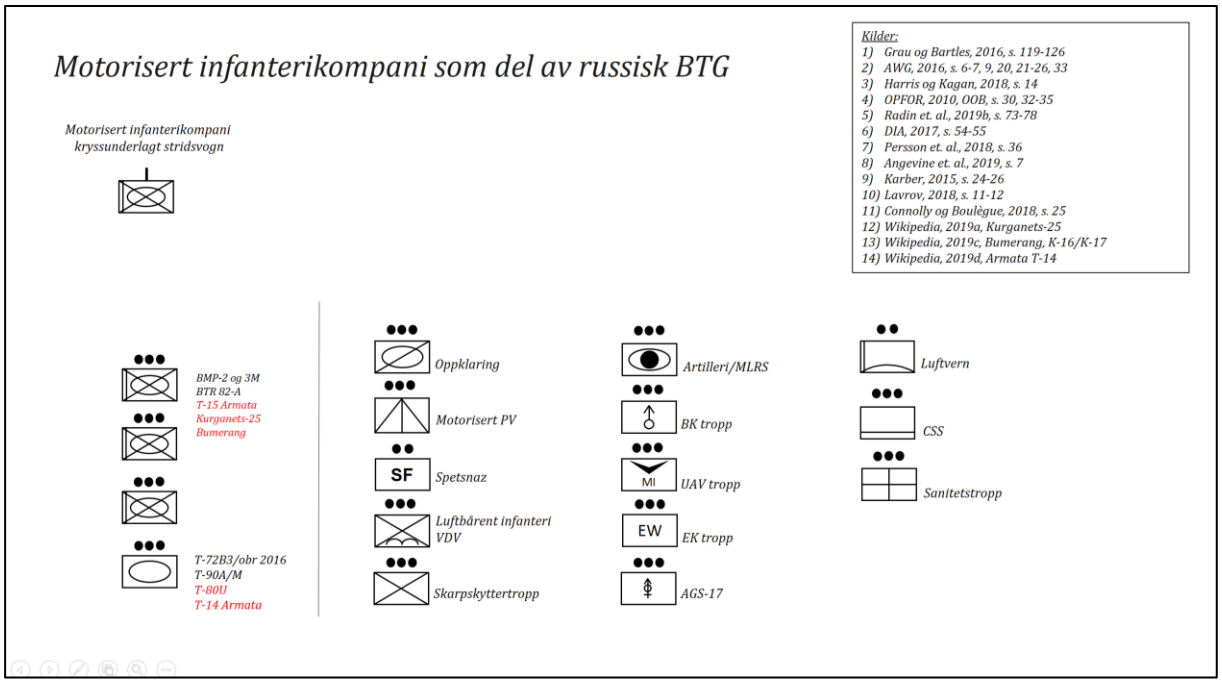
Den siste faktoren er lederskapet i den russiske hæren. På grunn av store utskiftninger i lederstillinger i de russiske styrkene, sitter nå tilnærmet alle ledere på brigadenivå og over med erfaringer fra kampene i Syria (Kofman, 2018, s. 3). Dette gjenspeiler trolig også ledernivåene nedover i hierarkiet. Den nylige kamperfaringen kan antas å påvirke hæren til å omsette erfaringer til praksis og til å stimulere til videre utvikling.

Samlet sett bidrar disse rammefaktorene til at vi kan forvente mer operasjonelt uavhengige brigader med støtteressurser, mer erfarent personell med høyere treningsstandard og moral, samt mer effektivt lederskap. Det er imidlertid flere forhold som kunne bidratt til å nyansere denne utviklingen. Som den reelle fyllingsgraden av personell, hvor effektive personellreformene egentlig har vært, hvor høyt det faktiske treningsnivået er og hvor relevante kampene i Øst-Ukraina og Syria har vært. Dette er spørsmål det er krevende å finne informasjon om. Likevel fremstår det som relevant at det eksisterer en vilje til å gjennomføre dyptgripende reformer gjennom hele styrkestrukturen for å møte målet om å bli mer moderne og teknologisk kapable (Dick, 2019, s. 4). Dette påvirker operasjonsmiljøet for det taktiske nivået.

2.1.1 Organisasjonen – kompaniet i en bataljonstridsgruppe

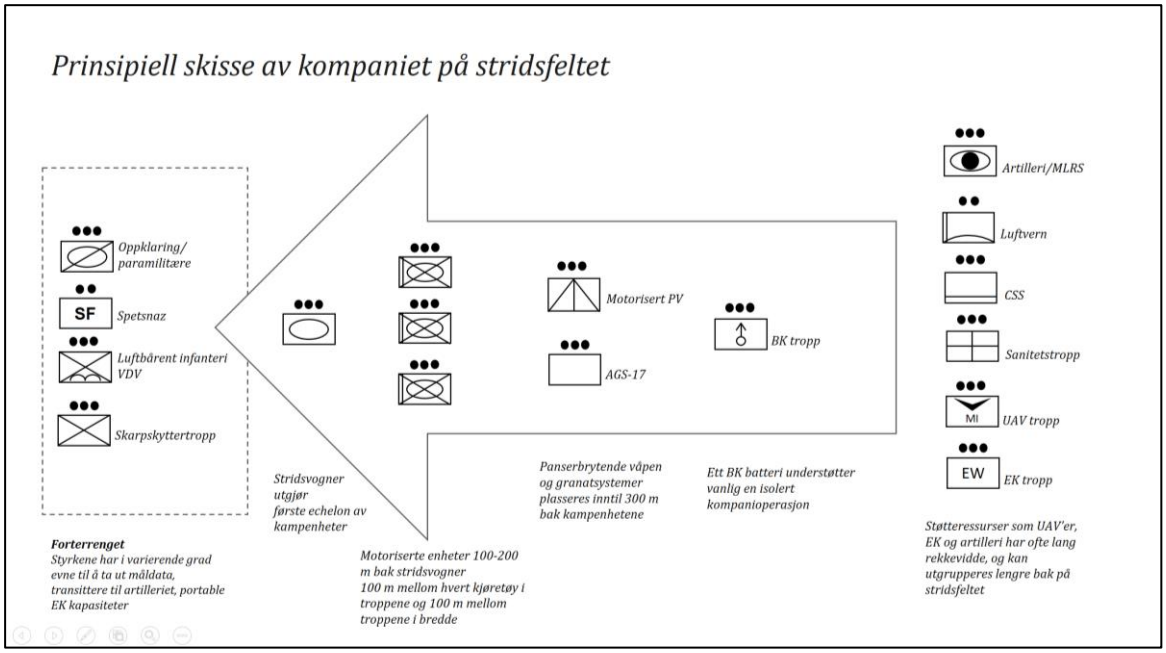
For å konkretisere analysen har en bataljonstridsgruppe i det vestre militærdistriktet blitt brukt som utgangspunktet. Bataljonstridsgruppen blir referert til som en *Battalion Tactical Group,* heretter kalt BTG. En bataljonstridsgruppe består i norsk kontekst av 300-400 soldater forsterket av flere organiske (tilhørende) støtteressurser (DIA, 2017, s. 52; AWG, 2016, s. 3). Det vestre militærdistriktet blir brukt for å kunne sannsynliggjøre relevans, oppbygning, utvikling og trusselen den kan representere. BTG har vært den primære strukturelle oppdragsorganiseringen for den russiske hæren siden kampene i Afghanistan 1979-1989, og vil også trolig være organiseringsformen i fremtiden, underordnet brigader og divisjoner (DIA, 2017, s. 55). Etter 2012 fikk hver brigade i den russiske hæren ordrer om å opprette én tilnærmet fullvervet profesjonell BTG (DIA, 2018, s. 55; Radin et. al., 2019b, s. 52). For forklaring til organisasjonskart og skissen av stridsfeltet, se vedlegg 1. Ut fra sentrale kilder utviklet mellom 2015 og 2019, er det sannsynlig at et kompani i rammen av en BTG kan se ut

figur 2 forsøker å illustrere. Det er viktig å merke seg at alle ressursene ikke naturlig tilhører et kompani, men er visualisert som dette for å fremstille alle enheter og kapasiteter som blir mer integrerte og oppnår samvirke som en følge av mer teknologi.



Figur 2. Russisk organisasjon som et kompani i rammen av en BTG. For en mer utfyllende forklaring av organisasjonen, se vedlegg 2.

For å forstå hvordan disse enhetene opererer i forhold til hverandre, hvilke avstander de opererer med og hvordan de understøtter hverandre, er det under presentert en prinsipiell skisse. Lengst til venstre opererer eliteinfanteri og proxystyrker på dypet, deretter følger kampavdelingene, direkteskytende og indirekte ildplattformer, så artilleri, luftvern, EK, UAV, cyber og informasjonsoperasjoner. På tross av at ikke alle kapasitetene og enhetene er fysisk tilstedeværende eller synlige på stridsfeltet, er det viktig å kunne forestille seg at dette virker sammen og kompletterende. Dette er en viktig forutsetning for å forstå at teknologiske bestanddeler som knyttes sammen blir mer effektive.



Figur 3. Prinsipiell skisse av kompaniet i kampformasjon (Delvis gjengitt fra Grau og Bartles, 2016, s. 119-126).

2.2 Teknologiutvikling innenfor russisk landmakt

Fra kilder og materiale mellom 2014 og 2019 er det utledet syv teknologikategorier, eller kapasitetsområder som får påvirkning på det taktiske nivået i den russiske hæren. Disse representerer teknologiske endringer som fremtvinger nye teknikker, taktikker, prosedyrer eller antatte endringer i tempo og effekt. Forhold som i stor grad vil påvirke en forsvarer.

Kategoriene er:

- *Kampvogner*
- *Indirekte ild*
- *UAVer*
- *Eliteinfanteri og proxykrigere*
- *Elektronisk krigføring*
- *Informasjonskonfrontasjon og cyber*
- *Kommando, kontroll og interoperabilitet*

Hver kategori blir videre beskrevet med utvikling man kan spore både relatert til kapasitetene og den taktiske bruken av dem. Beskrivelsen av hver kategori avsluttes med mulige

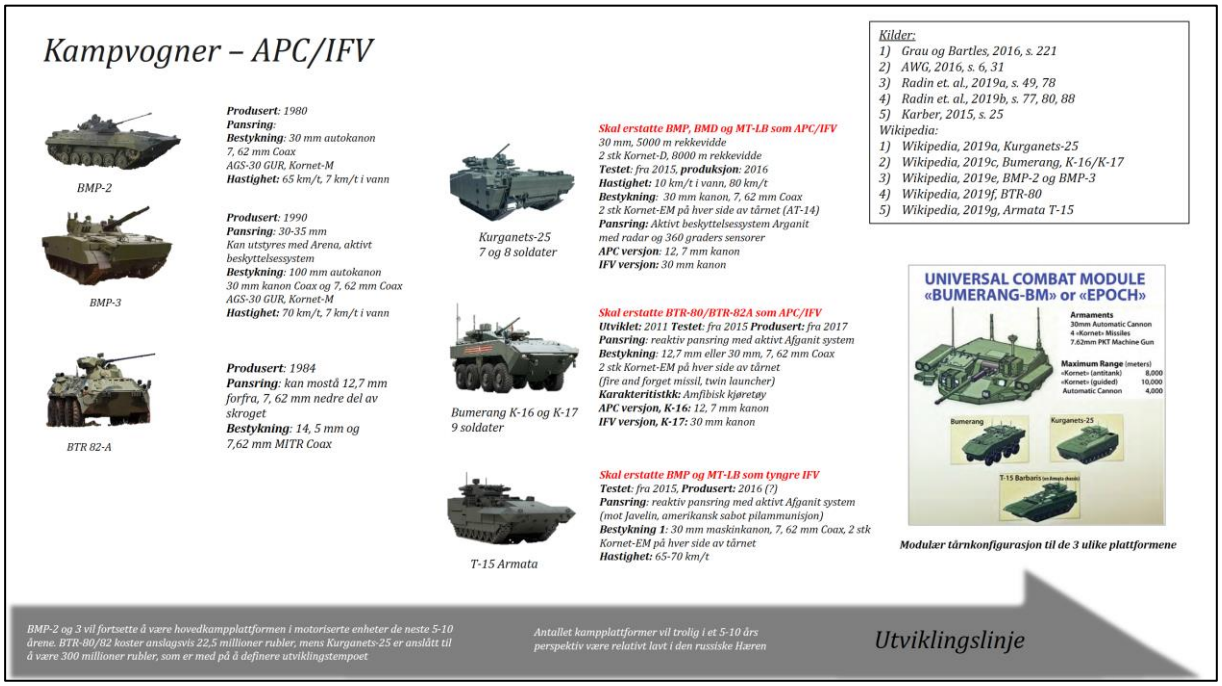
implikasjoner for en forsvarer. Hvert kapasitetsområde kan en forsvarer møte ved å enten utvikle nyere og bedre teknologi eller velge lavteknologiske løsninger som vektlegger mer asymmetriske aspekter ved striden. Implikasjonene vil derfor søke å belyse enkelte perspektiver ved begge disse sidene. *Kampvogner, indirekte ild, UAV* og *kommando og kontroll* er de kategoriene som organisatorisk hører til på det taktiske nivået. *Eliteinfanteri og proxykrigere, EK, cyber og informasjonskonfrontasjon* tilskrives vanligvis strategisk til operasjonelt nivå. For denne studien vil det imidlertid visualiseres i samme organisasjon, for å illustrere hvordan samvirket rammer taktiske enheter. Først vil kampvogner som utviklingskategori gjøres rede for.

2.2.1 Kampvogner

Hovedplattformene for motorisert infanteri har tradisjonelt sett vært på kampkjøretøy og pansrede personellkjøretøy, henholdsvis BMP og BTR. BMP er et beltegående kampkjøretøy, mens BTR er et hjulgående amfibisk pansret personellkjøretøy. Gjennom det russiske Våpen- og anskaffelsesprogrammet til 2027, kan man se at denne organisasjonen forsterkes. Vogner med lang arvelinje tilbake i tid moderniseres med eksempelvis 700 BMP-3, 1800 BMP-2 og 500 BMP-1 (DIA, 2017, s. 84). Utviklingen på begge disse plattformene ser ut til å være noe konservativ, hvor ildkraft og mobilitet har vært prioritert over beskyttelse. Dette gjenspeiles av at BMP og BTR-82A har blitt bestykket med grovere kaliber, 30 mm kanon, men at pansringen har vedvarende svakheter. Motoriserte vogner har eksempelvis hatt en stor dødelighet på stridsfeltet i Øst-Ukraina, da spesielt mot artilleriammunisjon, panserbrytende våpen (missiler) og kanoner fra 12,7 mm til 30 mm og oppover (Karber, 2015, s. 26; Radin et. al., 2019 b, s. 73). Videre har artilleriammunisjonen bestående av *clustere* (flere små) og termobariske stridshoder av fuel og oksygen vist seg å være svært effektfulle mot motoriserte kampvogner (Karber, 2015, s. 26).

Gjennom utvikling, samt kampene i Ukraina og Syria har det også blitt observert nye vogner, som; Armata T-15, K-17 Bumerang, Kurganets-25 og BMP-3 Dragoon (Connolly og Boulègue, 2018, s. 24). De nyeste plattformene viser en dreining mot mer fleksible og modulære systemer med betydelig bedre pansring, utviklede kommando og kontrollsystemer (C2), optikk og skytter-/lederverktøy i tårnet. Flere av vognene er satt opp med samme tårnkonfigurasjon for å skape mer universelle kampplattformer som forenkler logistikkkjeden (Grau & Bartles, 2016, s. 221). C2 systemene gir bedre muligheter for å tracke egne enheter

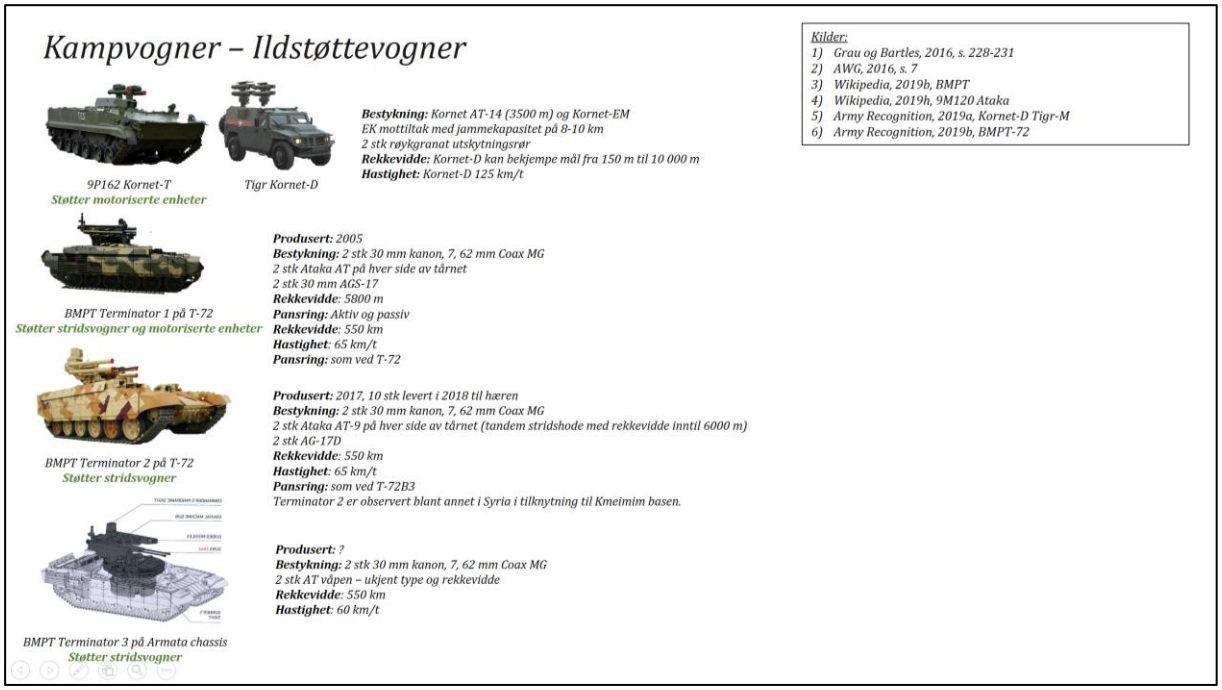
på stridsfeltet, og skape mer effektivt samvirke. I tillegg ser man flere vogner som får kraftigere kanoner og jammeresistente missiler (Wikipedia, 2019a). Totalt sett gir dette bedre beskyttelse, lengre rekkevidde og forbedret ildkraft. De nye vognene vil trolig observeres i økende grad de neste fem årene, men BMP-2 og 3 med BTR-82A vil fortsatt dominere i motoriserte enheter (IISS, 2019, s. 171). Se figur 4 for visualiseringen av utviklingslinjen for motoriserte vogner.



Figur 4. Illustrasjon av motoriserte vogner.

.

En forsterket trend er også at motoriserte enheter støttes av ildstøttevogner, som hjul- og beltegående missilutskytningsplattformer. Vognene er utstyrt med missiler med lang rekkevidde og ulike former for jammeresistens. Det er også observert at stridsvogner blir støttet av eksempelvis BMPT Terminator-3 (se figur 5), eller at T-72 blir støtter av T-90A vogner (Karber, 2015, s. 25). Rundt primærsysteme ser man et samvirke helt ned på sammensetningen av vogner i troppsformasjoner. Dette indikerer at beskyttelse og lokal ildkraft har blitt enda viktigere det siste tiåret, og at ildstøttevognene er tettere tilknyttet hovedsystemene på stridsfeltet.

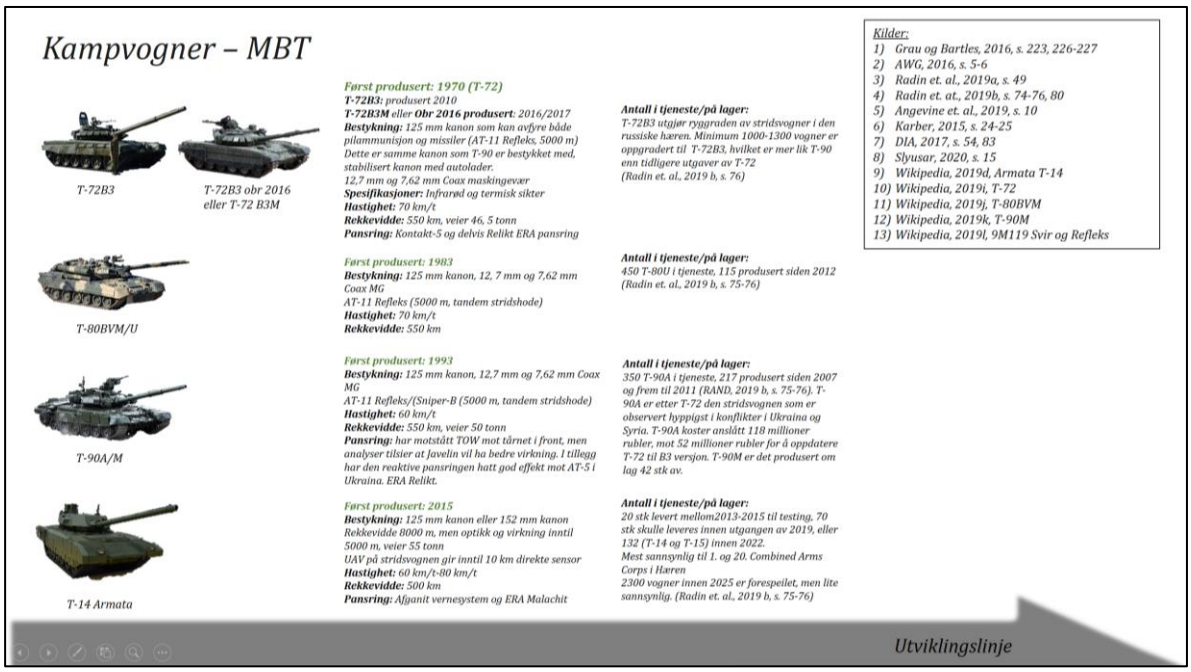


Figur 5. Illustrasjon av ildstøttevogner for motorisert infanteri og stridsvogner.

For stridsvogner er fortsatt T-72 den rådende plattformen i organisasjonen, etterfulgt av T-90A og T-80U/BVM (Radin et. al., 2019a, s. 49). Selv om T-90A og M i større grad har blitt innført, sammen med oppdateringer på T-80BVM, er moderniseringer på T-72B3M som så den største andelen av systemer komme ut av Våpenprogrammet frem til 2020 (Connolly og Boulègue, 2018, s. 8). Opptil 600 T-72 vogner vil være oppgraderte innen 2027 (Connolly og Boulègue, 2018, s. 8). Med de nye spesifikasjonene på T-72 nærmer den seg den teoretiske kapasiteten til T-90. I Øst-Ukraina har man imidlertid sett at mange T-72 vogner har blitt tatt ut, også oppdaterte vogner fra 2016. Dette nyanserer synet på hvor god pansring T-72 kan oppnå gjennom kun moderniseringsprosesser. T-90M har vist seg å ha en avgjørende effekt i kampene i Ukraina gjennom 2014 og 2015 (Karber, 2015, s. 25). I Ukraina har T-90 vognene hatt en rolle lenger bak på stridsfeltet, og med sin aktive pansring er det få til ingen stridsvogner av denne typen som har blitt tatt ut. I fem operasjoner av kompani størrelse frem til 2015 tok ukrainere dobbelt så mange tap, seks til én, der T-90 understøttet T-72 vognene (Karber, 2015, s. 26). Erfaringer fra den ukrainske hæren er også at trådstyrte missilvåpen som AT-5 ikke har hatt virkning mot pansringen på T-90 (Karber, 2015, s. 25). Dette medfører at russernes evne til å utvikle pansring med aktive og passive beskyttelsestiltak kan representere et skifte som fremtvinger prosedyreendringer. På grunn av økonomi og en krevende produksjonslinje for nye nye kampvognene, vil man trolig se et mindre antall

vogner ferdigstilt hvert år. Dette gjør at man trolig vil observere kombinasjoner av ulike vogner med kompletterende effekter også fremover i tid.

Armata T-14 er Russlands prestisjeprosjekt innenfor kampvogner. Armata T-14 stridsvogner ble underlagt avdelinger for testing allerede fra 2013, og det vil kunne bli innført 132 vogner innen 2022 (Elfving, 2020, s. 19). Flere kilder betviler imidlertid om russerne har de faktiske budsjettene og produksjonslinjen som kreves. Med den nye orienteringen for stridsvogner, ser man et fokus på bedre pansring og beskyttelse, kraftigere, langtrekkende og mer presise våpensystemer og mer integrasjon av informasjonssystemer, optikk og skytterteknologi (Elfving, 2020, s. 19). På Armata T-14 ser man på mulighetene for å øke kaliberet til 152 mm kanon, som også kan brukes til missiler (Elfving, 2020, s. 19). På tross av at vognene blir tyngre, ser det fortsatt ut som at mobilitet og rekkevidde klarer å opprettholdes. En annen trend som kan medføre endringer på stridsfeltet er utviklingen av dedikerte droner med utskytningsrampe på T-14 Armata (Grau og Bartles, 2016, s. 227). Dette gjør at vognene utvider sitt synsfelt fra om lag 5000 meter og opptil 10 000 meter. Stridsvognene kan med dette rekognosere motstanderens stillinger og fra skjul søke å påføre tap før vognene eksponeres og tar risiko. Teknologiske fremskritt preges i denne kategorien av en mer beskyttelse, ildkraft og interoperabilitet, som gjør stridsfeltet mer komplekst for en forsvarerer. Figur 6 viser stridsvognenes utviklingshorisont de neste fem årene.



Figur 6. Oversikt over stridsvogner og utvikling.

Implikasjoner – kampvogner

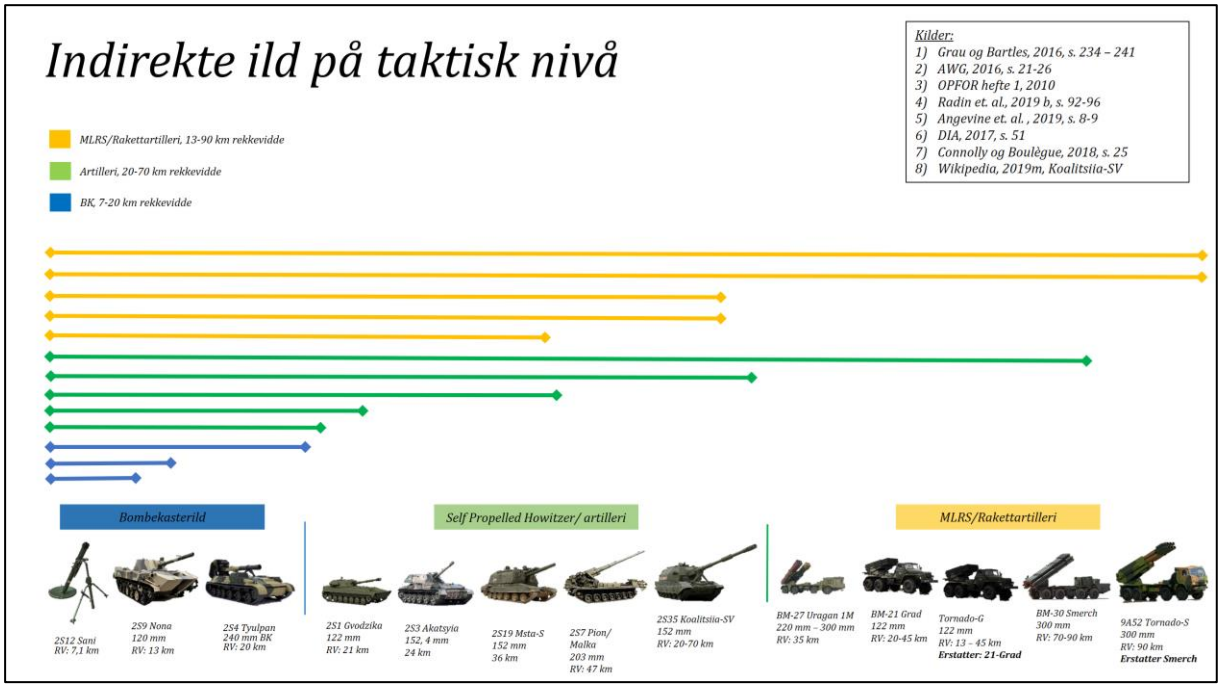
Med aktive og passive beskyttelsestiltak, stor ildkraft med rekkevidde og forbedret optikk og ledelsessystemer, er det grunn til å anta at russiske kampvogner samlet sett vil utgjøre en overlegen kapabilitet. For norsk teknologisk orientering kan dette tale for bedre pansring og beskyttelse, eller bedre rekkevidde og yteevne for ammunisjon på våre kampvogner. I tillegg kan det favorisere en større andel panserbrytende missiler oppsatt på vogner og for infanteriet. Utvikling av flere og lettere panserbrytende våpen med to stridshoder kan være nødvendig for å opprettholde effekten mot kampvogner i fremtiden (AWG, 2016, s. 29). Javelinsystemet har trolig ennå effekt, men vekten på dette systemet kan være et hinder for den mobilitet, samtidig som at rekkevidden er begrenset (effektivt inntil 2500 meter). Dermed kan fienden påvirke med sine våpensystemer lenge før han kommer innenfor engasjementsavstand. Erfaringer og utvikling i Ukraina tyder også på at bruken av miner med sprengstoff over 10 kg er svært aktuell for en forsvarer, da dette fortsatt viser til å ha god effekt (Slyusar, 2020, s. 29). I tillegg indikerer testing av metallskjermer på skroget og tårnet på vogner at effekten av RPGer, hulladninger og mini-IEDer kan avta med så mye som 60-70% (Slyusar, 2020, s. 61). Provisoriske løsninger som er laget for den ukrainske hæren har gitt betydelig effekt, som kan indikere at mindre kostbare løsninger også kan være med på å nulle ut teknologiske fremskritt, som ammunisjon.

Lavteknologiske tiltak kan også fremtvinges av utviklingen. Simuleringer og trening tilsier at treningsnivået mulig er bedre på nordiske kampvogner enn russiske - men dette er gitt at motstanderen *er innenfor rekkevidde*. Den generelle russiske satsingen på våpen som er avstandsleverte gjør at rekkevidde er og vil fortsette å være en viktig faktor på stridsfeltet (Thomas, 2019, s. 84). Dette gjør at norske styrker må iverksette tiltak for å overleve helt til fienden er på engasjementsavstand. Dette understreker viktigheten av kamuflerte og skjulte stillinger, samt skiftestillinger med dybde for norske hovedsystemer. Bakskråneforsvar og god dekning i front for vognene kan bli sentralt for at de skal overleve frem til striden mellom hovedmateriellet står. Kombinasjonen av stridsvogner, motoriserte vogner og ildstøttevogner på taktisk nivå vil trolig heve samvirket og ildkraften, som medfører at den russiske hæren vil bli en krevende motstander. Eget samvirke kan være essensielt for å stille fienden i flere dilemmaer, og på den måten øke egen sjanse for effekt.

2.2.2 Indirekte ild

Indirekte ild er et sentralt kapasitetsområde som representerer en avgjørende tapspåfører for Russland. Dette støttes av tall fra Ukraina, hvor artilleri har stått for for 75-80% av tapene i konflikten (Angevine et. al., 2019, s. 8; Slyusar, 2020, s. 6). Kategorien *Indirekte ild* består av Bombekasterild (BK) og artilleriild. BK inngår i et motorisert kompani, mens artilleri tilhører *missiltroppene og Artilleri,* og er dermed støtteressurser (DIA, 2017, s. 51*).* Disse troppene er igjen delt inn i tre separate avdelinger; missilenhetene, rakettartilleri og kombinerte artillerienheter. Missilenhetene opererer ballistiske missiler med kort rekkevidde, rakettartillerienhetene opererer enheter med rene MLRS batterier, mens de kombinerte enhetene besitter både tauet artilleri eller selvdrevet artilleri sammen med MLRS (DIA, 2017, s. 51). Tauet artilleri forsvinner i større grad fra mange avdelinger fordi de tar lengre tid å operere. I tillegg kan de russiske artillerisystemene avgi flatbaneild, med systemer som; 2S1 og 2S3. Dette bidrar til både egensikkerhet og forsterket ildkraft i de bakre områdene.

Figuren under viser en oversikt over kompleksiteten i antall systemer som kan defineres ned til det taktiske nivået, bredden i systemene og deres kompletterende art. Med en størrelsesordenen av systemer som også overlapper, viser dette også til en evne til å ivareta redundans, selv på det taktiske nivået. De nyeste systemene, under selvdrevet artilleri og BK viser også til grovere kalibre PGM, som 2S4 Tyulpan, Uragan-1M og 2S35 Koalitsiia-SV. Dette bidrar til at artilleriet langt på vei kan bruke bakkesystemer for å få tilsvarende effekt som bomber fra luften. Med de nye systemene Koalitsiia-SV og Tornado-G kan man også kombinere effekter av ulike ballistiske karakterer. Med teknologi kan denne ammunisjonen skytes fra ulike systemer og lokasjoner, men lande på bakken simultant med ulike kompletterende effekter. Utviklingen av kontrollsystemer som skaper interoperabilitet skaper med dette nye effekter på bakken.



Figur 7. Illstrasjon av indirekte ild på taktisk nivå.

De fleste av artilleriplattformene innenfor har en arvelinje tilbake til Sovjettiden, med unntak av nyere versjoner av 2S35 Koalitsiia-SV. Teknologien tilsier at det er ny presisjonsstyrt ammunisjon som står for den mest distinkte utviklingen. Dette skaper mer effektive lagdelte systemer med lengre rekkevidde, og korte operasjonstider før ilden lander på målet. Den største overordnede teknologiske utviklingen knyttet til indirekte ild er interoperabiliteten mellom sensorer og effektorer – kapabiliteten (Angevine et. al., 2019, s. 8). Det er UAVer, spesialstyrker, radarer og EK som fasiliteterer for mer nøyaktig måldata, slik at den massive ilden blir mer effektiv enn tidligere (Radin et. al., 2019b, s. 97). Dette medfører også at kostbar presisjonsild kan brukes til mål av høyere verdi. Fra Ukraina kan man også se at BM-21 Grad, BM-27 Uragan og BM-30 Smerch, altså MLRS, har stått for en økt dødelighet (Slyusar, 2020, s. 13; Karber, 2015, s. 12). Dette kan indikere at MLRS har blitt brukt mer på stridsfeltet i Øst-Ukraina enn vanlige artillerisystemer, men kilder fra konflikten sporer også denne effekten til større presisjon og hurtigere målfatning (Slyusar, 2020, s. 13). I tillegg har man eksempelvis i Donbass observert at Russland har brukt noen av sine beste radarer for presis kontrabeskytning på avstand, som: Zoopark-1, Leopard-T og Lyx-1 (Karber, 2015, s. 21).

Implikasjoner – indirekte ild

Den russiske hæren har et kvantitetsfortrinn i antall systemer, samt flere ulovlige ammunisjonstyper som har vist seg å være svært effektive på stridsfeltet (Karber og Thibeault, 2016, s. 62). Russland trenger heller ikke planlegge for å motvirke utilsiktet skade, hvilket gjør at tiden til målfatning og effekt går ned (Angevine et. al., 2019, s. 9). Dette gjør at kapasitetsgapet mellom den russiske og norske organisasjonen er så stort at dette tvinger frem lavteknologiske og teknologiske tiltak for å oppnå beskyttelse.

Beskyttelse kan oppnås i form av skjulte, forberedte og nedgravde stillinger i armert jern og betong, eller man kan oppnå beskyttelse gjennom prinsipper som mobilitet, spredning, kamuflasje (Karber, 2015, s. 21). Mindre enheter som utnytter spredning har eksempelvis vist seg å øke sine overlevelsesrater betydelig i Ukraina (Angevine et. al., 2019, s. 22; Karber, 2015, s. 20). I tillegg kan dette aktualisere tiltak som narrestillinger og oppblåsbart materiell med varmesignaturer for å tvinge sensorer til å reagere og skape informasjonsoverflod for fienden (Angevine et. al., 2019, s. 20). Tiltak kan også innebære trening i å detektere UAVer og opptre mer uforutsigbart. Taktisk opptreden vil trolig kreve spesifikk trening med feedback fra UAVer med termisk kapasitet og høyoppløselige videofeed. Å innlede trening med selv sivile enklere droner, vil trolig gi høy avkastning for avdelinger som er utrente på dette feltet. Dette kan også i stor grad påvirke kommandosentre og logistikkbaser, som gjør at alle avdelinger bør ha en svært høy bevissthet. Å operere under disse forholdene vil innebære at forsvareren må fortsette kampene på tross av høye tap (over 30%) og planlegge for en mer robust sanitets- og evakueringskjede. Toleransen for å ta tap bør også omfavne deler av stridsfeltet som historisk sett befinner seg lengre bak.

For fremtiden finnes det også teknologiske tiltak som omfatter å utstyre vogner og infanteri med elektroniske våpen (integrerte radarer) som kan jamme artilleriammunisjon på avstand for at ammunisjonen skal detonere for tidlig. Dette kan også utføres av rene EK avdelinger, avhengig av nærhet til de manøvrerende enhetene. Dette blir utviklet i dag spesielt av den ukrainske hæren mot 122 mm BM-21 Grad, samt 122 mm og 152 mm High Explosive ammunisjon (Slyusar, 2020, s. 14). I tillegg understreker Karber fra erfaringene i Øst-Ukraina at evnen til å kontrabeskyte russernes artilleri, og på den måten tvinge de til å flytte og rive opp deres massive beskytning, er særdeles viktig (Karber, 2015, s. 20). Behovet for et utstrakt nettverk av passive radarer med lav signatur kan være nødvendige i dette perspektivet. Et siste

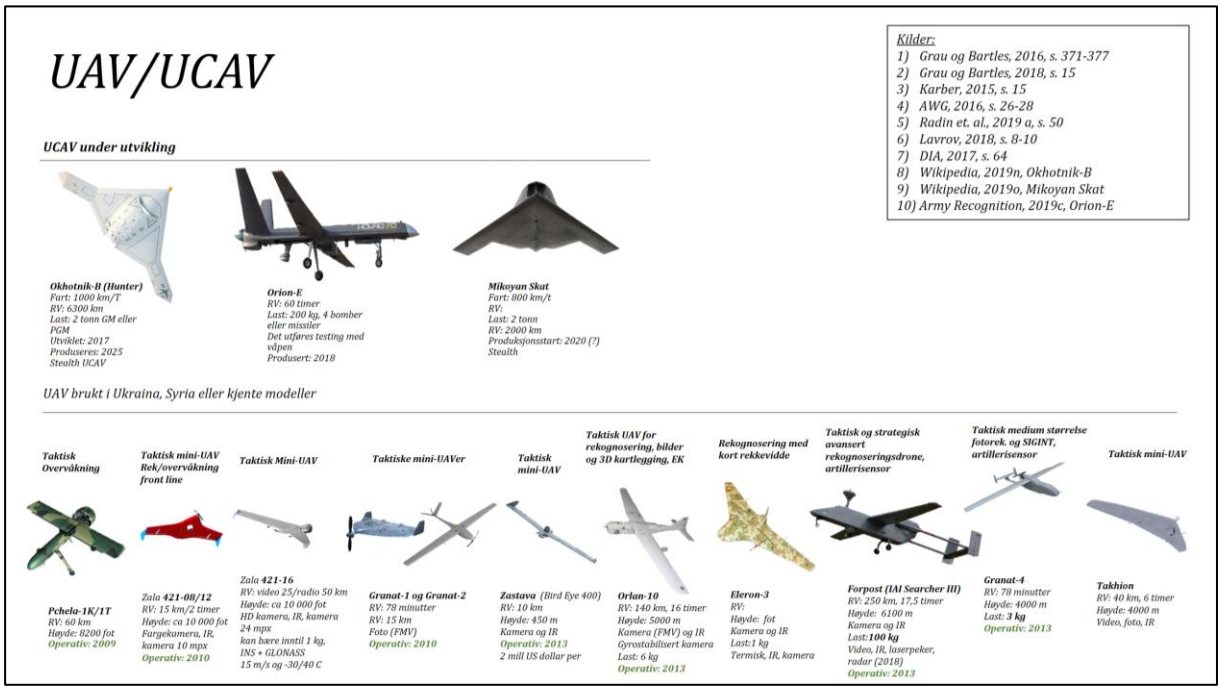
perspektiv som er verdt å merke seg er at etter over et tiår i Afghanistan og Irak har mange vestlige allierte gjort investeringer for å øke pansringen under vognene for å kunne motstå IEDer. Med en kovensjonell fiende, fordrer det trolig et større fokus på pansring og aktive tiltak på toppen av vognene mot artilleriild (Slyusar, 2020, s. 14). Dette illustrerer hvordan en konvensjonell teknologisk fiende skaper nye trusler på dagens slagmark.

2.2.3 UAVer

Autonom teknologi er en uttalt prioritert kapasitet for den russiske hæren. Den er også i høy grad sporbar gjennom bevilgninger, trening og øvelser, samt gjennom hyppig bruk i konflikter. Fra Russland opererte i Georgia i 2008 med én drone, er det mulig å observere en dramatisk økning i satsing og bruk av UAVer. I Ukraina alene har det blitt observert 13-14 typer UAVer, og i hæren fantes det allerede i 2017 over 2000 UAVer (AWG, 2016, s. 27; Karber, 2015, s. 12).

Ett primærområde for utviklingen av UAVer er det som kalles *recon-strike complex*, eller oppklarings- og målfatningsprosessen (Radin et. al., 2019b, s. 163; Grau og Bartles, 2018, s. 3). Etter vestlige normer kan dette sidestilles med *targeting*, en kapabilitet som utgjøres av sensorer, nettverk og effektorer. UAVer er det sentrale elementet i å identifisere mål, ta ut koordinater, sende tilbake til et C2 system, korrigere ild og gjøre en effektevaluering av ilden. I dag er UAVer tett integrert og danner sensorplattformen for samvirket mellom etterretning, indirekte ild, elektronisk krigføring og informasjonskonfrontasjon (påvirkningsoperasjoner). Kapabiliteten har blitt svært betydningsfull for hvordan Russland fører sin teknologiske strid. Dette bærer likhetstrekk med hvordan USA utnytter denne teknologien i Syria og Irak. I Ukraina har man sett en utvikling av systematikken i bruken av UAVer, som har medført at engasjementstidene har blitt kraftig redusert. Et fullt innskutt mål kan ta mellom 10-15 minutter, eller til og med mindre tid (AWG, 2016, s. 24).

En annen utvikling rundt UAVer er knyttet til å utstyre droner med EK kapasitet. Siden 2017 har flere UAVer hatt kapasitet til å innhente signaletterretning og andre til å jamme, og på denne måten oppnå kombinere effekter på stridsfeltet (AWG, 2016, s. 27). En forsvarer som ikke er klar over denne utviklingen vil kunne gjøre seg selv sårbar og undervurdere trusselen fra UAVer.



Figur 8. Illustrasjon av UAVer. UCAVer er fortsatt under utvikling i den russiske hæren.

I januar 2019 gjennomførte Russland også prøveflyvninger med deres første autonome kampflydrone *Okhotnik-B* (DIA, 2017, s. 64). I tillegg er også hvertfall tre andre droner under utprøving, som; Orion, Altius og Mikoyan Skat (Lavrov, 2018, s. 9). UCAVer og mer autonom teknologi er fortsatt et område i stor utvikling. Dette, med flere kilder vil kunne indikere at innen 2020 vil man med stor sannsynlighet kunne forvente at Russland har denne kapasiteten (Lavrov, 2018, s. 10).

Det er verdt å merke seg at Russland allerede har UAVer med lastekapasitet til å frakte ladninger eller lignende, eksempelvis Orlan-10 og Quadcopter. Nyere russiske taktikker tilsier at droner med lastekapasitet til fragmenterende granater blir brukt til å angripe bakre områder som ammunisjonslagre eller fuel depoter, og når personellet rykker ut for å slukke branner og lignende, blir de angrepet av «andre echelon» - det neste angrepet med droner (AWG, 2016, s. 27; Slyusar, 2020, s. 65). En annen trend er bruken av kamikaze-UAV, hvor UAVen er utstyrt med en ladning i flyets nese for å kræsjlande og utløse. Dette kan settes opp på både UAVer og quadcoptere, hvilket kan ha en relativt lav kostnad i fremtiden (Slyusar, 2020, s. 74-75). Mulighetene for å bruke autonom teknologi utstyrt med biologiske våpen, bærer også et potensial til å forme stridsfeltet. Her finnes det ikke registrerte data, men basert på Russlands

villighet til å bruke biologiske våpen, bør ikke dette avgrenses som en mulig teknologisk trussel – som eksisterer i dag (på tross av utfordringer knyttet til spredning og distinksjon). Siste eksempelet som kan benyttes her er forsøket på å forgifte Skripal og hans datter i England 2018 (UK Parliament, 2019).

Et annet viktig aspekt ved Russlands bruk av UAVer er at de ofte opererer i nettverk. Orlan-10 flyr ofte med 2 til 3 droner sammen, hvor den første rekognoserer på 1-1,5 km høyde, den andre brukes til elektronisk krigføring eller kompletterer bildet fra en høyere posisjon og den tredje kan fungere som et relé som overfører informasjonen som tas opp til et kontrollsenter (IDA, 2019, s. 8; Wikipedia, 2019s, Orlan-10). Dette er observert også i kombinasjon av et quadcopter på 8000 fot, mens UAVen fløy på ca. 2500 fot (Karber, 2015, s. 13). Disse teknikkene er dokumentert tilbake til 2014, hvilket innebærer at det kan antas å være videreutviklet siden da. Kina har allerede testet ut store dronesvermer på 200 UAV'er og inntil 1374 quadcoptere, hvilket tilsier at et så stort antall droner selv med små ladninger eller våpen kan utgjøre stor effekt mot mål (OE WATCH, 2018, s. 21). Dette bidrar til at UAVer bør anses som en teknologisk trussel med en stor bredde av virkningsområder, helt fra stridsfeltets front til bakerste mann. Det er svært viktig å merke seg at UAVer ikke bare er en sensor dedikert til overvåkning og målfatning for artilleriet. UAVer er også effektorer i form av EK midler, missiler og ulike ladninger.

Implikasjoner – UAVer

UAVer spiller en essensiell rolle i senere tids utviklede operasjonskonsepter i det russiske landdomenet. Derfor blir det også viktig for en forsvarer å kunne håndtere dette nettverket, både med teknologiske og lavteknologiske midler og metoder. Med utviklingen av UAV teknologi kan det bli viktig for en forsvarer å ha virkemidler til å reagere på denne trusselen, nettopp fordi én UAV kan ha integrert flere kapasiteter. En forsvarer kan settes opp med store radar- og EK installasjoner for å kjempe om dominans i det elektromagnetisike spekteret. Dette er trolig et større fortrinn for den geografisk tilknyttede forsvareren. I tillegg kan dronejammere (*Drone Defender*) bli mer aktuelle. Dette har vært effektivt, men er imidlertid kostnadskrevende å anskaffe langt ned i organisasjonen (AWG, 2016, s. 44). Med større behov for nettverk og streaming og flere antall UAVer, blir også Russland eksponert for hacking, som igjen kan oppgi hvor fienden befinner seg. For kampvogner og infanteri ser

andre nasjoner på tiltak rettet mot å nøytralisere UAVer gjennom radarer og missiler med mindre kaliber (Slyusar, 2020, s. 79). Å utvikle materiell med lavere signatur kan også være viktige grep, som: Nye antenner i kompositttmateriale, kamuflasjesett, lavere teltoppsett og lignende (Angevine et. al., 2019, s. 15).

Vår egen erfaring med droneaktivitet fra en motstander er forsvinnende liten fra Afghanistan og Irak, som gjør at dette er en ferdighet som må trenes opp. Basert på nyere taktikker kan man også hevde at behovet for å trene hele systemet forsterkes, også de som tradisjonelt sett har oppholdt seg lenger bak på stridsfeltet. Det beste lavteknologiske motmiddelet er trolig å ikke bli oppdaget, med kamuflasje og skjul (Masuhr, 2019, s. 2). Nedgravde stillinger, skjult stillingsgang og skiftestillinger kan være livsviktige tiltak. Utvikling av multispektral kamuflasjeduk ned på enkeltmannsnivå og moblitetsfremmende tiltak kan være helt nødvendige strakstiltak for å kjempe mot en konvensjonell aktør i dag (Army Warfare Branch, 2016, s. 18).

2.2.4 Eliteinfanteri og proxykrigere

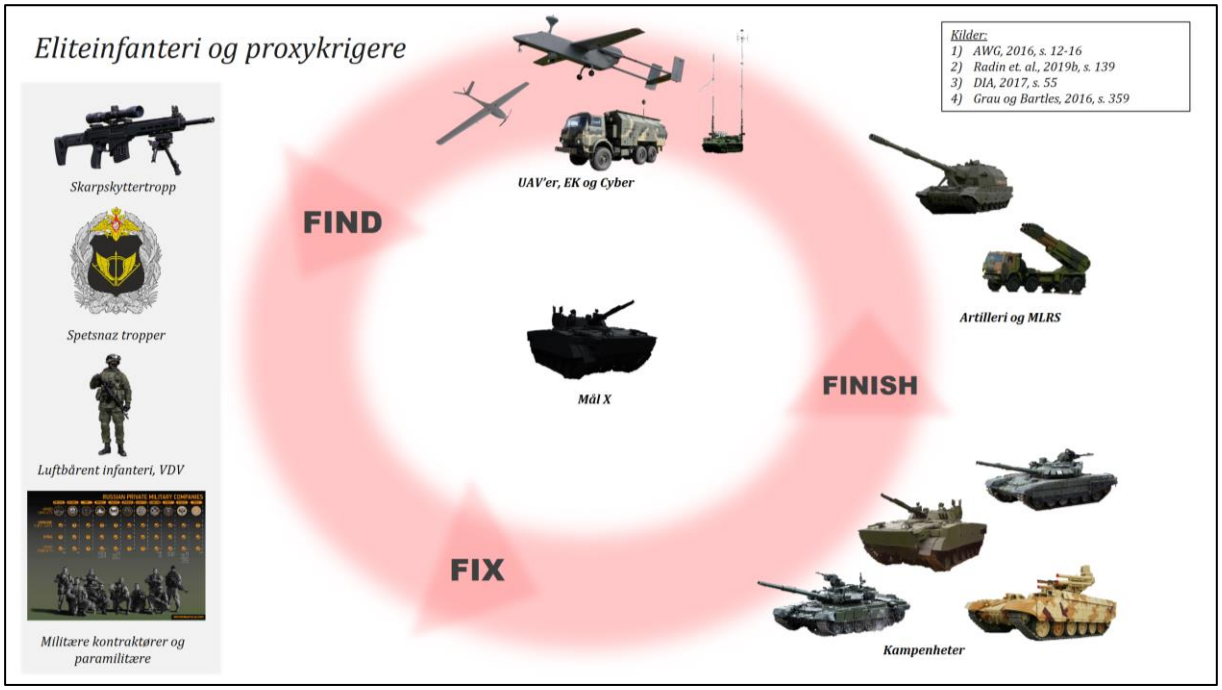
Deployerbart infanteri blir ifølge RAND definert som mer fleksible styrker med høy beredskap, trent for spesielle formål (Radin et. al., 2019b, s. 139). Under kategorien *eliteinfanteri og proxykrigere* tilfaller Spetsnaz, luftbårent infanteri (VDV), paramilitære styrker, kontraktører og skarpskyttere. Fra 2014 i Ukraina, Donbass, har Russland vist en stor villighet til å ta i bruk eliteinfanteri og spesialstyrker for å fasilitere for operasjoner under terskelen for væpnet angrep (DIA, 2017, s. 13, 55). Med dagens bevilgninger ser man også en fortsatt markant satsing innenfor disse styrkene, spesielt gjennom VDV og Spetsnaz (House, 2018, s. 15). Innen 2020, skal VDV og Spetsnaz øke med henholdsvis 60 og 100% (Connolly og Boulègue, 2019, s. 10). VDV ble fra 2016 oppført også med stridsvogner, og har tilsynelatende en større grad av profesjonelle soldater enn hva Spetsnaz har (DIA, 2017, s. 55). Dette understøtter en trend mot å utvikle selekterte og godt trente avdelinger med en høy grad av fleksibilitet og effektiv beredskap.

Fra kampene i Georgia og Ukraina kan en også observere hvordan militarisert befolkning i operasjonsområdet kan ta del av tidlige krigshandlinger, koblet med et innslag av private

militære kontraktører (AWG, 2016, s. 4). Det finnes om lag 10 aktører av ulike militære kontraktører i eller tilknyttet Russland som har operert i Syria, Ukraina eller begge. Wagner er en kontraktør som eksempelvis har deltatt i både Ukraina og Syria, som gir Russland økt fleksibilitet og strategisk mobilitet (Dick, 2019, s. 5). Russland har siden 2014 signert samarbeidsavtaler med om lag 20 afrikanske land, og Etterretningstjenesten anslår at bruken av private militære selskaper vil fortsette å øke som et foretrukket virkemiddel i utenrikspolitikken (Etterretningstjenesten, 2020, s. 36). Dette er med på å antyde at kompleksiteten i antall aktører på dypet har økt. På tross av at disse aktørene trolig vil kunne operere mer sømløst i tidligere sovjetstater enn Norge, vil elementer av fordekte styrker og proxykrigere representere en stor trussel på ulike kontinenter i fremtiden (DIA, 2017, s. 45).

Under kampene i Ukraina og Syria, fremstår det som at Spetsnaz også har blitt en viktig sensor for artilleriet (AWG, 2016, s. 12). Dette er også dokumentert at skarpskyttere, og til og med dedikerte skarpskyttertropper har blitt brukt til (AWG, 2016, s. 20). Dette samvirket oppnår man som et resultat av teknologisk utvikling, som binder sammen kontraktører, eliteinfanteri, spesialstyrker, skarpskyttere og andre sensorplattformer som UAVer og artilleri. Andre allierte har også identifisert et behov for å utvikle prosedyrer for å respondere på en mer robust skarpskyttertrussel. Dette er også basert på den moralske effekten skarpskyttere har hatt på sine motstandere, blant annet i Øst-Ukraina (Army Warfare Branch, 2016, s. 20). Ukrainske offiserer begynte å ta av distinksjoner og andre merker som kunne indikere deres grad eller posisjon (Army Warfare Branch, 2016, s. 20). Dette vil også kunne bidra til at en motstander må trene for denne trusselen, og at ledere i dag ikke alltid er tjent med å være langt fremme på stridsfeltet (Army Warfare Branch, 2016, s. 21).

Samvirket har også blitt registrert i forbindelse med utviklingen av mobile EK kapasiteter, hvilket bidrar til at styrker på dypet kan gjennomføre sabotasjeaksjoner uten den fysiske og direkte påvirkningen som man tidligere kunne forvente. På denne måten utgjør elitestyrker koblet med mer teknologi en mer potent trussel. Siden 2013 har generalstabsjefen Gerasimov vært tydelig på betingelsen for fremtidige operasjoner, hvilket er ett forent etterretnings- og informasjonsområde hvor styrkene kan samhandle i sanntid (Gerasimov, 2013, s. 2). Dette representerer noe av kompleksiteten knyttet til aktørbildet, hvilket utfordrer vestens evne til distinksjon og dermed bevare initiativet. Dette aktørbildet og samvirket er illustrert på figur 9.



Figur 9. Oversikt over eliteinfanteri og proxykrigere og hvordan disse integreres inn mot andre enheter.

Implikasjoner – Eliteinfanteri og proxykrigere

Enkelte kan hevde at med norsk tolkning av hybrid krigføring, tilfaller disse oppgavene Etterretningstjenesten, PST og politiet. Med den naturlige utfordringen knyttet til å oppdage disse truslene, er det også mange som påkaller tettere samarbeid mellom Forsvaret og politiet (Diesen, 2018, s. 46). Her kan det også hevdes at samarbeid og øving mellom Hæren, Heimevernet og kritisk infrastruktur er viktig for raskere å kunne reagere på sammensatte trusler. Det å utarbeide flere indikasjonsmetoder og raskere respons, vil trolig kunne bidra i dette bildet, også for styrker i landdomenet. Denne operasjonsmetoden styrker teoretisk sett angriperen eller aggressoren ved at man får tid til å befeste seg og utvikle sine trekk dersom en forsvarer ikke detekterer dette tidlig nok. Dette får konsekvenser for manøverkrigføringen ved at man blir tvunget til å bli reaktiv. Å utvikle kjennskap til taktikk og prosedyrer, og ha personell dedikert til å lokalisere disse i en tidlig fase, kan være verdt å konseptualisere for en eventuell motstander. Den komplekse sammensetningen av aktører med interoperabilitet fordrer trolig et større fokus på kontraoppklaring og bekjempelse av denne typen trusler. På tross av at man alltid vil ha styrker på dypet som driver oppklaring, kan det sannsynliggjøres at denne trusselen blir mer potent, i takt med utviklingen av teknologien.

2.2.5 Elektronisk krigføring

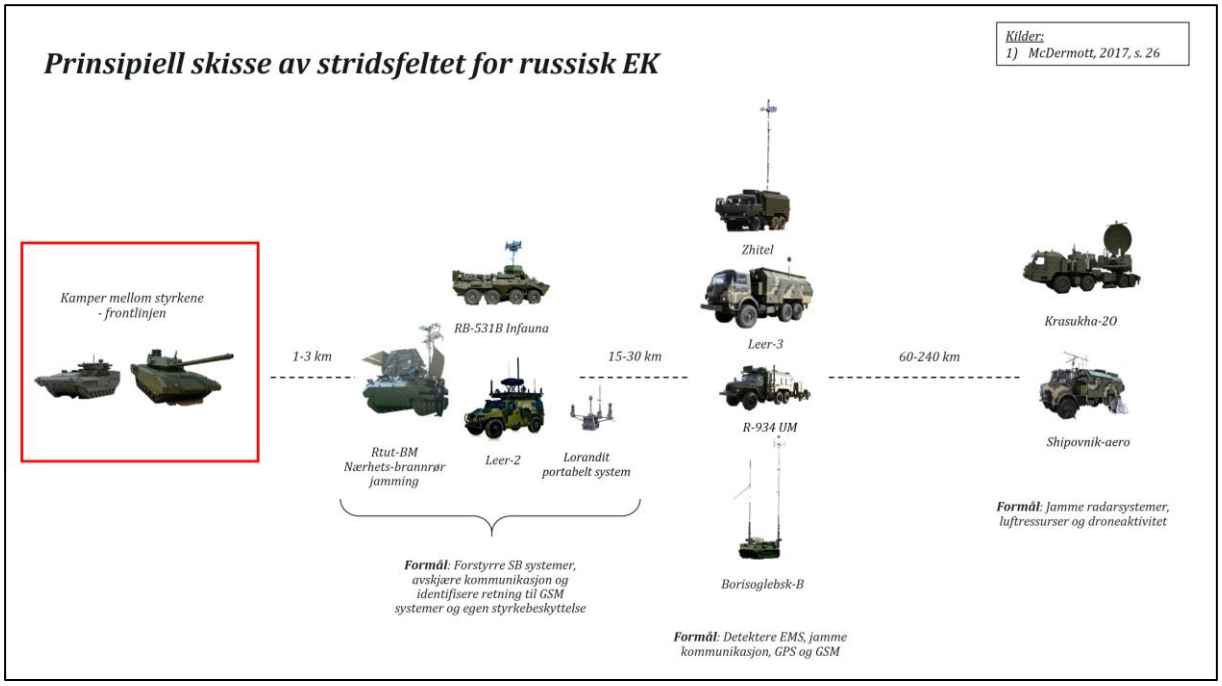
Elektronisk krigføring [EK] har vært et naturlig satsingsområde i Sovjettiden for å demme opp for vestens kapasisteter og økende teknologiske sårbarheter. De 10 siste årene kan man argumentere for at evnen til å føre EK operasjoner har økt ytterligere. (Kjellén, 2018, s. 37). Bare underlagt den russiske hæren finnes det fem EK brigader, hvorav fire tilhører hvert sitt militære distrikt, mens den siste svarer til *Joint Strategic Command*, og er en mobil brigade (Kjellén, 2018, s. 37). I tillegg har hver reformerte motoriserte brigade eller stridsvognsbrigade hvert sitt EK kompani. Siden EK troppene ble opprettet, eller reformert i 2009, har anskaffelsen av systemer økt kraftig. Også kompleksiteten og bredden i kapasitetene har beviselig økt (Kjellén, 2018, 42). Flere rapporter søker å nyansere det vestlige synet på russiske EK kapasiteter, fordi kapasitetene ikke er så offensivt rettet som inntrykket tilsier (Kjellén, 2018, s. 83). I tillegg har enkelte studier fastslått at en vestlig motstander vil bli totalt utslått av russernes overveldende kapabilitet i det elekromagnetiske spekteret. Denne konklusjonen ønsker andre å falsifisere, men hevde at slik som man må kjempe om luftrommet i dag, må man trolig også kjempe om å dominere i det elektromagnetiske rommet i fremtiden (McDermott, 2017, s. 28). For å få oversikt over systemer og kapasiteter systemene besitter, samt hvordan disse operer på det taktiske nivået, kan figur 10 gi et visuelt inntrykk.

Figur 10. EK systemer på taktisk nivå med oversikt over virkeområde og dokumentert bruk.

Russerne har trolig omtrent 14 operative systemer innenfor bakkestyrkene tilknyttet jammespekteret og kommando og kontroll enheter. I tillegg er det et titalls systemer som har vært på utprøving i hæren siden 2013. Systemene, som vist over, utstyrer landkreftene med evnen til å jamme en motstanders kommunikasjonslinjer, til å motvirke signaletterretning mot egne enheter, til å motvirke effekten av artilleri mot egne, til å spore og få posisjon på motstanderens enheter (ELINT), til å ta ut GPS og satelittkommunikasjon i perioder eller i avstander eller mate inn feil posisjoner og lignende (Kjellén, 2018, s. 45). I tillegg kan de samhandle tettere med artilleri ved å sende koordinater på motstanderen med å finne ut hvor signaturen fra enheter kommer fra. Her er det observert at samvirke mellom cyber og EK gjør det mulig å sende falske SMSer til mobiler eller mate inn feil informasjon i GPS systemer.

Utviklingen av kapasiteten indikerer at den russiske hæren prioriterer lettere systemer til sitt eliteinfanteri for å tracke motstanderens enheter og støtte med måldata på dypet med systemer som *Lorandit* og *Lesochek (*Kjellén, 2018, s. 46*)*. Nyere kampvogner utvikles for å kunne settes opp med *Palantin*, som kan jamme nærhetsbrannrører til artilleriammunisjon og dermed tilby forbedret egenbeskyttelse (Kjellén, 2018, s. 46) I tillegg utvikles flere offensive systemer med laserstråle, høybølgefrekvens og elektromagnetisk puls for å kunne ødelegge data og kommunikasjonsenheter (Kjellén, 2018, s. 22). På tross av at Russland trolig vil bruke tid på å produsere slike systemer, kan dette gi indikasjoner på hva man kan forvente i et femårs perspektiv.

Spesielt med det landsbaserte systemet Leer-3 har man i Ukraina sett evnen til å knytte EK og UAVer sammen. Samvirket bidrar både til å identifisere motstanderens styrker, gi posisjon på styrkene, transittere måldata til artillerisystemer og sende ut falske SMSer til enhetene på bakken (AWG, 2016, s. 18; McDermott, 2017, s. 22-23). Dette viser også en større samhandling mellom offensive midler, hvor elektronisk krigføring, cyber og påvirkningsoperasjoner blir tett integrert. Figur 11 forsøker å illustrere dette stridsfeltet og antall kompletterende systemer som virker innenfor det taktiske nivået (0-100 km).



Figur 11. Prinsipiell skisse av stridsfeltet for russisk EK.

Implikasjoner – EK

Kampen om det elektromagnetiske rommet vil utkjempes, og det er videre sannsynlig at egne styrker ikke vil være overlegne til enhver tid. Teknologisk sett fremmer dette behovet for å konkurrere med lik eller bedre kapasitet. Dette kan være store statiske radar- og EK-installasjoner som skaper et fortrinn for forsvareren. EK gir også muligheter for å satse på flere systemer som kan jamme innkommende missiler og artilleriammunisjon, for å redusere effekten av en del av fiendens hovedsystemer. I tillegg ligger det kanskje uante muligheter for fremtiden i å satse på offensive innsatsmidler innenfor EK.

Lavteknologisk sett betyr dette at forsvareren må kunne beherske å periodevis operere uten samband, blue force trackere eller GPSer (Angevine et. al., 2019, s 19). Dette aktualiserer tid til å trene basisferdigheter på alle nivåer. Dette krever også noe av lederskapet, da det fordrer at man har tillit langt ned i organisasjonen og kan opprettholde operasjonstempoet selv om informasjonsmiljøet er sterkt degradert. Dette krever reell tillit og initiativ på lavt nivå. Det kan videre kreve mer samtrening, bedre samvirke, mer lokal kjennskap til terreng. Det å sikre at organisasjonen kan fungere på tross av svikt i systemene er viktig for å ikke bli passive i striden (AWG, 2016, s. 42). Et nettverkssentrisk system har kanskje medført at man i vestlig

kultur har blitt mer avhengig av kontroll enn det som er sannsynlig å planlegge med i fremtiden, hvilket enheter bør ta innover seg (McDermott, 2017, s. 30).

Et annet aspekt er at enheter bør trenes opp mot «utslippskontroll» av ulike signaturer (Army Warfare Branch, 2017, s. 22; Angevine et. al., 2019, s. 20). Det å redusere signatur fra elektronikk i kritiske faser kan bli viktig for overlevelse. For patruljer krever dette eksempelvis at sambandstrafikk bør foregå minimum 200 m fra stilling eller observasjonspost for å i det minste sikre overlevelse mot artilleri. For å beherske utslippskontroll bør sannsynligvis også kunnskapsnivået på lavere nivåer økes. Mer forståelse betyr at man kan redusere egne svakheter på det teknologiske stridsfeltet.

2.2.6 Informasjonskonfrontasjon og cyber

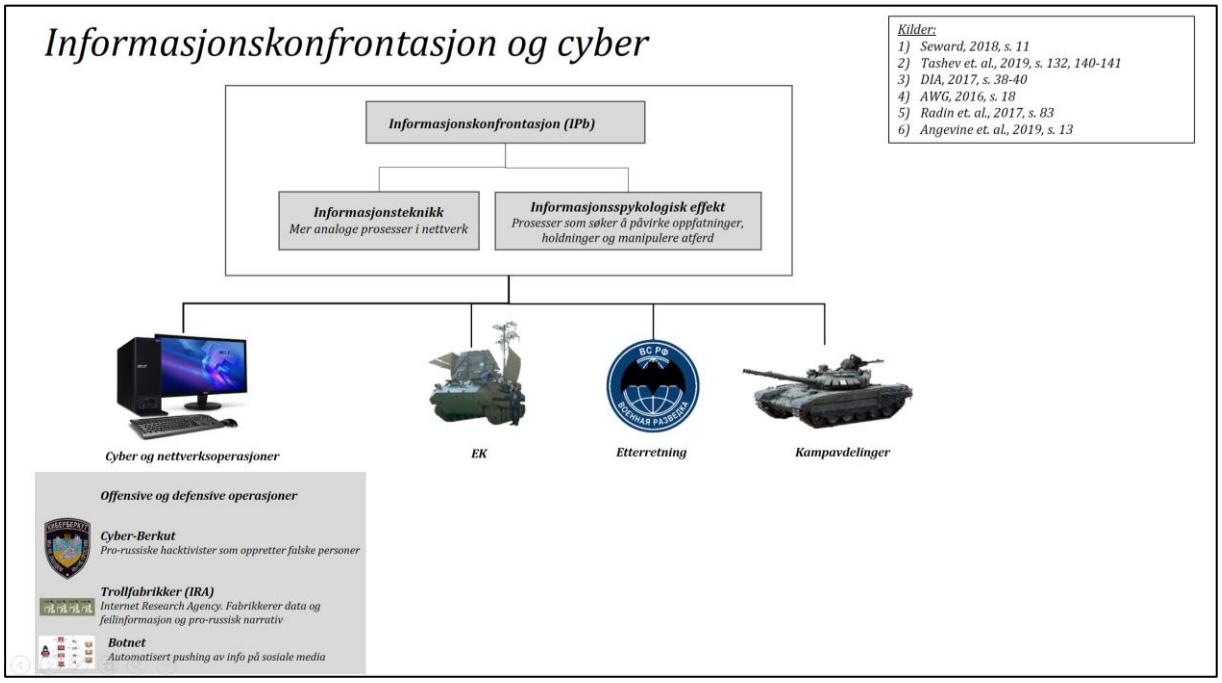
Russland har siden 2010 prioritert en styrking innenfor *informasjonskonfrontasjon,* eller det Vesten gjerne kaller påvirkningsoperasjoner (DIA, 2017, s. 38). Dette inkluderer diplomatiske, økonomiske, militære, politiske, kulturelle, sosiale og religiøse informasjonsarenaer (DIA, 2017, s. 38). Under informasjonskonfrontasjon sorterer russerne to metoder for å utøve påvirkning; Gjennom *informasjonsteknikk* og *informasjonsspykologisk* effekt (DIA, 2017, s. 38.). Den informasjonstekniske effekten henviser til den mer analoge prosessen i form av datanettverksoperasjoner gjennom angrep, forsvar og utnyttelse - det vi tradisjonelt sett forbinder med cyberoperasjoner. *Informasjonspsykologisk* effekt viser til påvirkning og manipulasjon av menneskers oppfatninger og atferd (DIA, 2017, s. 38). I lys av denne strategiske og doktrinelle tilnærmingen, bør cyber forstås som ett middel for å påvirke informasjonsmiljøet. Fra russisk side er det også vanskeligere å gjøre klare skiller mellom cyber, informasjonsoperasjoner, EK, etterretning. Alle disiplinene henger uløselig knyttet sammen, hvilket er viktig for å forstå hvordan det vil komme til uttrykk i fremtiden (Tashev et. al., 2019, s. 132). For å forstå informasjonskonfrontasjon og cyber ut ifra et tradisjonelt stridsfelt, kan det være hensiktsmessig å se på disse midlene som *åpningsilden* på slagmarken, hvor innslagene reduseres utover i konflikten. Først vil cyber med nettverksoperasjoner omtales, deretter sammenkoblingen av både cyber og informasjonskonfrontasjon.

For å forstå påvirkningen gjennom cyberoperasjoner, er det viktig å ha et forhold til ulike virkemidlene som har vært applisert fra Russlands side. Ett kjent virkemiddel er statssponsede hackergrupper, gjerne tilknyttet statens etterretningstjenester; GRU (den militære), FSB (den føderale), FSO (den føderale beskyttelsestjenesten) og den utenlandske etterretningstjenesten SVR (Kroghrud, 2019, s. 13). Grupper som *Cozy Bear, APT29* og *TheDukes* tilhører SVR, som har det primære ansvaret for Russlands utenlandsetterretning (Kroghrud, 2019, s. 35). *Cozy Bear* har eksempelvis blitt attribuert til en rekke angrep mellom 2014 og 2017, spesielt gjennom *phishing* mailer som lurer mottakerne til å trykke på vedlegg og linker med koding som gjør at gjerningsmennene får tilgang til informasjon og videre utnyttelser eller skadevare (TV2, 2017). I 2017 angrep Cozy Bear målrettet norske epostkontoer i APs Stortingsgruppe, Forsvaret, UD, Statens Strålevern og PST (TV2, 2017). *APT28, Fancybear og Sofacy* er tilknyttet GRU. GRU er den militære etterretningen som samler inn informasjon relatert til militær-politiske og militær-økonomiske spørsmål (Kroghrud, 2019, s. 35). APT28 ble eksempelvis godt kjent etter innblandingen i det amerikanske presidentvalget i 2016 (Kroghrud, 2019, s. 35). Det er grupper som er tilknyttet GRU som har vært kategorisert som de mest risikovillige, aggressive og utforskende aktørene innenfor cyberoperasjoner (Kroghrud, 2019, s. 36). Dette illustrerer at også personell lengre ned i hierarkiet i Forsvaret kan rammes av slike sofistikerte angrep.

Videre har Russland også benyttet *CyberBerkut*, eller oppdiktede personer og *trollfabrikker* som manipulerer og masseproduserer informasjon og forsøker å endre narrativer. *BOTer* som pusher informasjon på sosiale media har også blitt observert gjentakende helt siden hendelsen i Estland 2007 (DIA, 2017, s. 39; Kofman et. al., 2017, s. 83). Dette skaper et stort stimuli av informasjon for å påvirke befolkningers oppfatninger, og har vært identifisert eksempelvis under avstemningen om Brexit i England (UK Parliament, 2019). Disse angrepene kan også dedikeres til personell i samme grupper på sosiale medier og lignende, som gjør at forsvarspersonell også er utsatt for subtile budskap. På tross av den strategiske naturen til cyber og informasjonskonfrontasjon som virkemidler, kan man argumentere for at det i fremtiden kan få større effekt også på det taktiske nivået.

Man ser i Ukraina en tiltakende vilje til å gjennomføre mer individualiserte målrettede angrep på uniformert personell (AWG, 2016, s. 18). Cybers tilknytning til EK systemer, etterretning og informasjonsoperasjoner som en helhet, skaper et potensiale for å treffe mindre grupper.

Dette kan innebære kompromittende, sjenerende, uriktig eller kriminaliserende informasjon om den enkelte eller nære relasjoner, hvilket kan få en demoraliserende effekt. I registrerte tilfeller i Ukraina har det har blitt sendt SMSer til ledere og personell med falsk informasjon. Dette kan være meldinger med truende innhold eller utpressingspotensial for at soldatene ikke skal møte på jobb, eller imiterte meldinger fra nær familie som har blitt utsatt for sykdom eller skade som hindrer lederen å møte (Seward, 2018, s. 12; Angevine et. al., 2019, s. 13). Som et synkronisert virkemiddel kan dette frata en forsvarer handlekraft i en viktig fase.



Figur 12. Illustrasjon av informasjonskontroll og cyber, med samvirke.

I tillegg kan man se rene nettverksoperasjoner innenfor cyber som kan direkte få innvirkning på det taktiske nivået. Dette i form av bakdører som blir etablert i software som eksisterer i år eller måneder før angrepet og utnyttelsesfasen inntreffer. Dersom samvirkesystemer, ildledningssystem for artilleri og kommunikasjonsteknologi blir slått ut synkronisert med striden, representerer dette en risiko. Det ligger et skadepotensial i å legge inn uriktig informasjon eller manipulere systemene. Dette kan være krevende å oppdage, hvilket medfører at slik sofistikerte nettverksangrep kan få uante konsekvenser (Angevine et. al., 2019, s. 20).

Et annet aspekt som berører forsvareren er hvilket digitale fotavtrykk den enkelte soldat genererer med sine online verktøy. Dette er ikke unikt for vesten, og siden konflikten i Øst-Ukraina har dette også blitt satt på agendaen for russiske styrker. Attribusjon var innledningsvis krevende i Ukraina, men de senere årene har det oppstått egne nettsider av frivillige samfunn som spesialiserer seg på å dokumentere nærværet av russiske styrker og materiell i Ukraina, *informnapalm.com.* Russiske styrkers digitale fotavtrykk gjør det nå mulig med OSINT, analyser av åpne nettkilder å attribuere aggressjon i Øst-Ukraina i større grad (InformNapalm, 2019). Det samme kan eksemplifiseres da man i 2018 oppdaget at Strava, en nettbasert aktivitetsmonitor, la ut varmekart basert på treningsaktivitet på verdensbasis. Flere amerikanske baser i Midtøsten og Afrika ble offentliggjort, men også russernes tilstedeværelse i Syria, Kmeimimbasen i Latakia. Paralleller kan også trekkes til hvordan aktive stedstjenester genererer datapunkter gjennom mobilapplikasjoner. Dette kan være med på å understreke dagens behov militære styrker har for å identifisere eget digitalt fotavtrykk og være forut for utviklingen. Her kan man enkelt eksemplifisere med bruken av GPS klokker og mobilapper i militære leire for vaktsoldater. Alt utslipp kan bære et potensial for monitorering og derfor være en fare for at vi avgir for mye informasjon - uten å vite at vi gjør det.

Figur 13. Varmekart av aktiviet knyttet til russiske styrker i Latakia, Syria (Businessinsider.com, Strava heatmap, 2018).

Informasjonspsykologisk effekt kan også oppnås gjennom å fysisk presse eller påvirke menneskegrupper. Dette foregår både ved operasjoner i nærområdet, samt gjennom medier og presse. Det å vende befolkningen mot styrkene, redusere legitimiteten til statlige institusjoner

og skape motstand er kjente taktikker fra flere nasjoner i Russlands interessesfære. Det kan trekkes paralleller til Finnmark, hvor Norge også har pro-russisk befolkning, eller folkegrupper med tidligere russisk statsborgerskap. I 2016 hadde Norge 22 360 mennesker innvandret fra Russland mellom 1990 og 2016 (SSB, 2020). Flere argumenterer imidlertid for at psykologiske operasjoner har vist seg å være lite effektfullt, og dermed ikke utgjør den store risikoen mange frykter (Kofman & Rojansky, 2015, s. 5). Målrettet kringkasting og informasjon rettet mot befolkning som utviste sympati for den russiske saken i Ukraina ikke klarte å få støtte til separatistene (Kofman & Rojansky, 2015, s. 5). Dette førte til at Russland måtte bruke militære styrker for å påvirke kampene i Øst-Ukraina. Uavhengig kan informasjonspsykologisk effekt over tid trolig ha effekt, og bør være et virkemiddel man følger tett.

Implikasjoner – informasjonskonfrontasjon og cyber

Cyber og informasjonskonfrontasjon er i Norge gode eksempler på domener hvor den gjennomsnittlige soldat har lite innsyn og forståelse. For en forsvarende part er det viktig å være bevisst sitt digitale fotavtrykk og sine egne sårbarheter (AWG, 2016, s. 43). Utvikling på russisk side tilsier at man må øke informasjon og kunnskap, samt lede styrkene på dette området (Seward, 2018, s. 14). Også sivile bedrifter har erkjent at man ofte overinvesterer i tekniske tiltak for å møte digitale utfordringer, mens man underinvesterer i menneskene (PWC, 2017). Mange av angrepene hvor russerne har lyktes i å etablere bakdører i programvare skyldes det menneskelige feil. Dette understreker viktigheten av å utdanne og skape bevissthet i hele organisasjonen.

For at ledere skal settes i stand til å integrere dette i utdanning og trening må man konkretisere tekniske kapasiteter og gjøre det forståelig nok til at ledere på bakken kan motvirke effekten av dem. Det vil si at ledere bør utdannes innenfor cyber, etterretning, EK og påvirkningsoperasjoner, samt at det implementeres i trening og øving. Dette gjelder enheter fra nivået lag til bataljon i brigadesystemet. For den enkelte ligger det mye sikkerhet i å bevege seg fra en norsk «åpenhetskultur» til å utvikle en mer sunn skepsis mot teknologi og online aktiviteter. Det er mye som tyder på at det å avstå fra å ta med seg mobilen og GPS klokken ut i feltet ikke er nok for å møte på et teknologisk stridsfelt, fordi utnyttelsen skjer

hele tiden, og måneder og år fra konflikten oppstår. For en forsvarer virker det sentralt å anerkjenne at mennesket er i kjernen for påvirkning fra en motstander – i hele Totalforsvaret.

2.2.7 Kommando, kontroll og interoperabilitet

I Georgia 2008 fikk Russland erfare hvordan upresis artilleribeskytning og svikt i sambandssystemene påvirket deres effektivitet på stridsfeltet (Lavrov, 2018, s. 7). Siden 2008 har Russland lagt grunnlaget for å skape en kommunikasjons- og nettverksstruktur som inkorporerer hele statsapparatet for å møte visjonen mot en mer nettverkssentrisk organisasjon (Radin et. al., 2019a, s. 54). I 2017 alene ble 4000 systemer på strategisk og operasjonelt nivå anskaffet, 49 000 på taktisk nivå. Den senere tids satsing har medført at Russland nå kan bruke Forpost UAVen til operasjoner i Syria og strømme bildene i sanntid til både operasjonssenteret i Kmeimim i Latakia og i Moskva (Lavrov, 2018, s. 6). Det har vært antatt at russerne ligger langt bak i anskaffelsen av kommando og kontrollsystemer som kan understøtte slik interoperabilitet, men per i dag vil flere hevde at Russland er i ferd med å oppnå vestlig paritet på dette området (Radin et. al., 2019a, s. 79). Utviklingen i Russland påvirkes av dyr elektronikk, vestlige sanksjoner og høye kostnader, men likevel er Russland i ferd med å lykkes i å skape skape et omforent situasjonsbilde. Med automatiserte C2 systemer, som Andromeda-D og Strelets kan Russland langt på vei skape denne informasjonsutvekslingen i sanntid (Radin et. al., 2019a, s. 54).

Den nettverkssentriske utviklingen blir ledet av sambandstroppene (Grau og Bartles, 2016, s. 285). Etter testingen av et integrert og kryptert sambandssystem i 2010 (Yesu-TZ) anslo man at tiden det tok fra en ordre var ferdig til den nådde avdelingene – var en hel dag (Radin et. al., 2019b, s. 167; McDermott, 2011, s. 17). Nyere C2 systemer som Strelets i den russiske hæren kan samvirke med systemer med arvelinje fra Sovjet, samtidig som at det er integrert opp mot VDV, romstyrkene, luftforsvaret og det automatiserte C2 systemet Andromeda-D. Dette viser at utbedringene nå fasiliterer for den interoperabiliteten som kreveres for å oppnå nettverkssentrisk krigføring. Nyere systemer har også en rekke anti-EK tiltak, blue force trackere og kan settes opp ned til enkeltmann i den russiske hæren (Grau og Bartles, 2018, s. 15).

Dette utviklingsområdet er med på å heve kvalitet og kampkraft for de andre kapasitetsområdene i denne studien. Fordi teknologien skaper en interoperabilitet og samvirke som endrer krigens karakter. Integrasjonen gir kampenheter, eliteinfanteri, UAVer, indirekte ild, EK, cyber og informasjonskonfrontasjon de store effektene. Russland har kun forsøksvis testet de nyeste kapasitetene i Ukraina, Syria og under øvelser i Russland og Kina, samt i enkelte enheter i det vestre militærdistriktet, hvilket medfører at hele systemet samlet sett kan ha svakheter. I tillegg vil mer teknologi og nettverk også skape mer friksjon og sårbarheter, som vi selv kan kjenne igjen. Likevel gir de siste årenes utvikling grunnlag for å argumentere for at russerne har lyktes med å sammenkoble systemene og dermed tilføre en styrkemultiplikator. Her illustrert ved figur 14.

Figur 14. *Illustrasjon av viktige systemer for å oppnå interoperabilitet og en mer nettverkssentrisk organisasjon.*

Implikasjoner – kommando og kontroll

Samband, kommunikasjonsplattformer og båndbredde skaper en interoperabilitet på det taktiske nivået som trolig vil utfordre beslutningssløyfen til militære offiserer og endre tempoet på stridsfeltet i fremtiden. Dette krever psykologisk robusthet, samvirke, fellesoperasjoner og gode, realitiske planverk for å tilrøve seg initiativet igjen. For å kunne påvirke en teknologisk motstander og fremstille dilemmaer, krever dette trolig enten en

høyteknologisk tilnærming, en lavteknologisk og asymmetrisk tilnærming - eller innslag av begge. Trening av samvirke for Hærens ledere bør integreres tettere og på et lavere nivå. Ikke bare samvirke mellom manøverenheter og bombekaster- og artilleriild, men samvirke og forståelse mellom flere virkemidler i operasjonsmiljøet. I tillegg tvinges det frem at joint-perspektiver og kompetanse bør vektlegges fordi Hærens ledere alene ikke kan møte disse systemene med tempoet som ny teknologi tillater.

2.3 Oppsummering – en teknologisk motstander

Kapittel 2 har forsøkt å besvare forskningsspørsmålet: "*Hvilke teknologiske kapasiteter besitter Russland og hva vil kjennetegne en mer teknologisk strid?».*

Det første funnet er de syv kapasitetskategoriene, hvor studien kan spore en utvikling som påvirker hvordan teknologisk strid føres. Disse kategoriene er: kampvogner, indirekte ild, UAVer, Eliteinfanteri og proxykrigere, EK, cyber og informasjonskonfrontasjon, kommando, kontroll og interoperabilitet. Kapasitetsområdene utgjør fysiske og ikke-fysiske bestanddeler av operasjonsmiljøet på taktisk nivå, og svarer på hvilke teknologiske kapasiteter Russland besitter.

I forlengelsen av dette er verdt å trekke frem det neste funnet, nemlig at det gjennom studien kan sannsynliggjøres at Russland bør fremstilles som en teknologisk motstander. Den russiske hæren er både teknologisk konkurransedyktig og utfordrer vestlig og nordisk dominans innenfor flere kapasitetskategorier. Russiske styrker ligner i dag i svært stor grad de nettverkssentriske organisasjonene vi selv streber etter å være, selv om mye materiell fortsatt bærer preg å ha overlevd fra Sovjettiden. I tillegg har russisk orientering forsterket teknologisk utvikling på områder hvor vi har sårbarheter eller mangler kvantitet og utholdenhet. Denne asymmetrien i teknologisk utvikling er et viktig perspektiv å ivareta, fordi det er med på å utligne den militære maktbalansen. Dette medfører at det kan være formålstjenlig å både oppfatte og definere Russland som en teknologisk motstander.

Det tredje funnet er at det ikke først og fremst er revolusjonerende teknologi i seg selv, som kunstig intelligens, 3D- printing og robotmekanikk, nanoteknologi eller stordatabehandling

som i dag representerer de nye truslene på lavere nivå. Teknologiske trusler i Russland har oppstått som en følge av *evolusjonær teknologiutvikling*, gjennom modernisering og økonomisk pragmatiske utviklingsmodeller. Teknologien blir en styrkemultiplikator fordi den muliggjør en større grad av samvirke, stand-off, presisjon, beskyttelse og effekt når alt knyttes sammen. Sett i et mer strategisk perspektiv kan denne evolusjonen betraktes som så naturlig og ubetydelig at den kan bli oversett. På taktisk nivå kan den imidlertid skape en ny dynamikk som det er verdt å rette oppmerksomheten mot.

Det fjerde funnet er knyttet til hvilke implikasjoner dette får totalt sett. På taktisk nivå kan studien sannsynliggjøre at teknologien skaper et relativt høyere tempo og en større dødelighet på stridsfeltet. Dette påvirker alt fra plan- og beslutningsprosesser til prosedyrer på stridsteknisk nivå. Dette fordrer at en forsvarer må evne å knytte sammen virkemidler i tid og rom, både innenfor samvirke og fellesoperasjoner. Disse utfordringene krever trolig ikke bare teknologiske løsninger – men også lavteknologisk respons.

2.4 Nyanser ved russisk teknologiutvikling

Teknologien og de syv områdene for teknologiutvikling er i denne oppgaven i hovedsak sett på med perspektivet: Hva eksisterer i den russiske hæren i dag? Likvel er det områder som også avhenger av videre utvikling og budsjettbevilgninger (Armata, kamp-UAVer og offensive EK våpen). Her hersker det usikkerhet knyttet til fortsatte prioriteringer, som flere rapporter også påpeker (Radin et. al., 2019a, s. 67). Bortfall av råvarer, import av deler eller utilstrekkelig subsidiering av industri kan få konsekvenser eller føre til stagnasjon. Flere rapporter påpeker også den generelle økonomiske nedgangstiden i Russland, og sår tvil om Russlands fyllingsgrad av nytt materiell, hvilket også er et viktig perspektiv å ivareta.

Et annet moment er at oppgaven ikke evner å måle i hvor stor grad russisk organisasjon behersker nytt materiell, ny teknologi eller mer nettverkssentrisk binding mellom sensorer, beslutningstakere og effektorer. Utdanningsnivå, reell kompetanse, trening, øving og lederskap kan berøres, men kan ikke måles i parametre som gjør at vi kan nøyaktig analysere det. Dette er nyanser som bør fremkomme.

Det er også verdt å merke seg at ved alle utviklingsområdene i den russiske hæren, kan implikasjoner for en forsvarer utledes slik: å utvikle tilsvarende teknologi eller innretninger som overgår og nuller ut det mulige russiske fortrinnet. Dette ville både være kostnadskrevende og være basert på en urealistisk forutsetning, og dermed er implikasjonene i hovedsak rettet mot hva en militærmakt kan utbedre per i dag, uten store investeringer, budsjetter og innovativ utvikling. Dette er også utledet av hva andre stater har erfart siden 2008.

Gjennom fokus på ny teknologi og nye trusler kan det som er nytt og ukjent lett bli fortolket som mer dimensjonerende enn hva som faktisk er virkeligheten. Dette er en kognitiv skjevhet som bidrar til å vurdere fremtiden og det ukjente som mer truende, og teknologi spesielt som mer farlig enn hva som kan være tilfelle (Beadle, 2016, s. 71). Dette kan eksemplifiseres gjennom cyber som et nytt, teknisk og lite åpent domene. Truslene som oppstår i dette digitale rommet kan oppleves som svært kritiske og livstruende, på tross av at cyber med sin ikke-kinetiske natur historisk sett ikke har ført til en avgjørende seier på stridsfeltet i dag. Likevel er konsekvensene større ved å underestimere disse truslene og således et belegg for å risikere å portrettere truslene som mer dimensjonerende enn de er eller vil være.

Majoriteten av eksemplene som blir brukt for kapasitetsutvikling er dokumentert fra Georgia, Krim, Øst-Ukraina og Syria. Den uheldige effekten av dette er at ingen av disse konfliktene kan sammenstilles med en konflikt mellom to jevnbyrdige militærmakter. I vestlig kontekst blir eksempelvis ikke Ukraina sett på som en jevnbyrdig motstander, og konflikten i Øst-Ukraina kan også oppfattes som nærmere en proxykonflikt (Masuhr, 2019, s. 2). I konfliktene det refereres til har Russland hatt begrensede målsetninger, brukt begrensede midler og gjerne operert fordekt for å unngå at styrkene skal attribueres. Det vil si at det er vanskelig å estimere eksakt hvor kapasitetsutviklingen står og hvor stor redundans den russiske hæren har på de ulike nyutviklede systemene.

Oppgaven har videre skilt på indirekte ild på taktisk nivå inntil 100 km, mens over 100 km blir definert som operasjonelt til strategisk. Man kan hevde at indirekte ild over 100 km og Russlands ballistiske missiler har meget stor innvirkning på det taktiske nivået. Oppgaven ville imidlertid ikke blitt mulig å håndtere. Det samme gjelder luftvern og radarer, men som

man ikke kan spore den store teknologiske endringen i fra litteraturen som eksisterer i dag. Luft- og sjømakt har følgelig også stor innvirkning på det taktiske nivået i landstriden, og spesielt når man definerer Nord-Norge som det geografiske omdreiningspunktet for analysen. Det er en nødvendig avgrensning å ta disse bestanddelene ut av oppgaven, men det bør også fremgå at dette ikke er optimalt for å undersøke kompleksiteten i det en motstander møter på det teknologiske stridsfeltet.

3 Norske forestillinger om teknologisk strid

I dette kapittelet analyseres datamateriale som er innsamlet gjennom seks intervjuer med seks ulike militære ledere i Hæren. Spennet er fra kadetten ved Krigsskolen, via troppsjefer, stabsoffiserer, til kompanisjefen ute ved avdeling. Kapittelet vil vil sentreres rundt to spørsmål: Hvor oppdaterte er utvalget av militære ledere og hvordan vurderer de sin kompetanse om teknologisk strid.

3.1 Hvor oppdaterte er militære ledere?

For å undersøke hvor oppdaterte lederne faktisk er, benyttes følgende generelle parametre: I hvor stor grad intervjuobjektet evner å uttale seg om et kapasitetsområde. I hvor stor grad vedkommende evner å tilføre informajon, nyansere informasjon, stille spørsmål eller rette kritikk mot deler av informasjonen. I hvilken grad vedkommende evner å si noe om hvordan teknologien påvirker enheter på taktisk nivå, og om vedkommende har noen tanker om mulige metoder og midler i møte med utfordringene.

Det intervjuobjektene generelt viser til kunnskap om, er de tre utviklingsområdene kampvogner, indirekte ild og delvis UAVer. Først kartlegges områdene hvor de militære lederne utviser best innsikt og forståelse, og vi starter med kampvogner. I et utdrag kan vi observere at A1 svarer om russerne: «Det er ikke så mye nytt med kampsystemene. Det som er mer nytt, er satsingen på EMS [elektromagnetisk signatur]. De får også økt signatur. De er

generelt mye bedre enn oss på rekkevidde, men jeg tror fortsatt mobilitet er vårt beste kort da». Dette står i noe kontrast til hvordan lederen med mer erfaring svarer (A3):

> Svakheten med de [beskyttelsessystemene] er at det ikke dekker hele vogna. Enten så er det åpning på toppen eller bak, som gjør at de våpensystemene vi har fortsatt er effektive mot de aktive systemene, og samme med de reaktive systemene. De våpenene vi har klarer å rydde unna den reaktive pansringen. Det som allerede har fått konsekvens er tiltakene som gjør at man registrerer laser, som gjør at det er vanskeligere for infanteri å bedømme avstand riktig, og dermed også å sørge for treff. Det betyr egentlig prosedyreendringer, teknikkendring for folk som er på vogn, som gjør at man ikke kan bruke laseren like aktivt som tidligere.

Lederen med mer erfaring viser også evne til å se teknologien i en sammenheng og reflektere om implikasjonene på noe lengre sikt (A3):

> Med de nye systemene kan jo konsekvensene være at man ikke lenger er garantert treff med kinetiske våpen. Så med noen av systemene som ligger litt lenger frem i tid, da prater man om at man klarer å ta ut pilammunisjon, og da begynner vi å snakke en kapasitet [...].., konsekvensene er at vi er ikke garantert treff, eller garantert uttelling på treffet, som betyr mer ammunisjon. I utgangspunktet er dette ting som allerede er innarbeidet i prosedyrer og stridsteknikk. Hvis man ser utelukkende på rekkevidde, så har en motstander en fordel på oss. På PB [panserbrytende] siden har vi redusert rekkevidde, så selv om vi har betraktelig bedre teknologi og er mer treffsikre, så er rekkevidden svært begrenset [...]

Mer erfaring og tjeneste fra både troppsjefsnivået og bataljonstab bidrar til at intervjuobjektene også vurderer gyldigheten av informasjonen gitt i presentasjonen. Dette tyder på kognitiv refleksjon i tilnærmingen til ny informasjon. I tillegg nyanserer disse lederne svarene sine i større grad enn sine kollegaer med erfaring kun fra lavere nivå. Disse supplerer også med mer informasjon og detaljer enn hva som er gitt i presentasjonen, hvilket også indikerer at de besitter god og oppdatert kunnskap på området. Det som også gjenspeiles i svarene fra personellet med tjenesteerfaring fra staber, er at de i stor grad utleder

implikasjoner og gir flere mulige løsninger for å møte truslene. Dette belyses gjennom besvarelsen til A6 under spørsmålet knyttet til kampvogner og beskyttelsessystemer:

> Jeg leser jo dette litt som infanteriets renessanse. Det gjør at vi er tilbake til det som Taliban har gjort i Afghanistan. Vi er så teknologisk overlegne, men IEDer og veibomber treffer jo oss også. Jeg tror vi må sloss på en mer asymmetrisk og uforutsigbar måte. Vi må ikke havne inn i deres find-fix-finish loop, hvor de kan bruke kapasitetene mot oss. Vi må ikke være et mål.

Indirekte ild og UAVer er de andre kapasitetsområdene hvor de militære lederne generelt svarer utfyllende og nyansert, men også med delvis begrenset innsikt. Dette fremkommer blant annet gjennom hvordan A3 tilnærmer seg dette spørsmålet, her presentert ved et utdrag:

> Ja, det er kanskje en av de større utfordringene vi står overfor akkurat i dag. Motstanderen har blitt relativt dyktig innenfor recce-fire-complex [russisk målfatningsprosess]. Å lokalisere med sensorer og hurtig lede ild. Teknologien sitter jo vi på i dag også. Det er ikke sånn at fienden har enerett på å være i stand til dette. Vi har ikke muligheten til å gjøre det i samme omfang eller rekkevidde. Vi har ikke noen gode muligheter å kontre det på ved bruk av teknologi.

Flere respondenter påpeker at et økende samvirke og integrering mellom UAVer og artilleri reduserer tiden fra sensoren identifiserer et mål til den indirekte ilden treffer målet. Dette er det såkalte *recon-strike-complex* hos russerne, hvor målfatningstiden reduseres med de nye systemene. Intervjuobjektene understreker behovet for å rette oppmerksomheten mot prinsipper som kamuflasje, skjul, spredning, mobilitet, villedning og dronejamming for å møte sensorplattformen og dermed den indirekte ilden. Det å ikke bli oppdaget er et viktig ledd i å kunne føre striden på sine premisser. Intervjuobjektene vurderer det tilsynelatende slik at UAVer utgjør størst trussel på det kinetiske stridsfeltet som sensorer for artilleriet.

Dette medfører noe riktighet, men basert på russernes kvantitet på artilleriammunisjon kan det være en farlig slutning å utelukke ild mot sannsynlige mål, som også kan medføre store

personell- og materiellskader. Ett intervjuobjekt berører momenter også knyttet til rekkevidde på artilleriammunisjon og hvilke virkeområder som utvikles i den russiske organisasjonen. Dette er A2, som har lengre bakgrunn fra troppearten artilleri. Her fremstår det som sentralt med relevant bakgrunn for å forstå et avgrenset felt, også hvordan fienden bruker denne kapasiteten.

Intervjuobjektene forholder seg svært overfladisk til flere muligheter som ligger i UAV-teknologi. Først og fremst gjelder dette teknologiens potensial for å påvirke fiendens fortrinn ved oppklaring og etterretning. Videre gjelder det hvordan UAVer faktisk har blitt benyttet i ulike lagssjikt, også utstyrt med EK- kapasitet for å drive innhenting og jaming. I tillegg kommer hvordan kamikaze-UAVer og quadcoptere har blitt utstyrt med bomber og granater for å angripe styrker lengre bak på stridsfeltet. Dette er en taktisk bruk av teknologien man har sett i Øst-Ukraina, og som det kort blir redegjort for i presentasjonen (Vedlegg 2). I tiden intervjuene gjennomføres (koronasmitte og tiltak i Norge) kunne det også ha vært interessant å gjøre et tankeeksperiment rundt hvordan mer autonome droner som utstyres med biologiske våpen som virus og lignende, kunne skapt kaos og en stor effekt i et samfunn som en fase 0 i et krigsscenario.

Det er én respondent som trekker frem aspekter ved dette, men i sammenheng med spørsmålet knyttet til hvilke trusler vedkommende opplever som dimensjonerende på det teknologiske stridsfeltet. A6 trekker frem dette (før vedkommende får informasjonen fra presentasjonen av en teknologisk motstander): «Autonome systemer, og da mener jeg på en måte droner med våpen. Massive droner, myldring av droner som kan overvåke og engasjere et stort område autonomt. Egentlig alt som går på kombinasjonen av deteksjon og effekt». På spørsmålet om hvilke implikasjoner UAVer og indirekte ild kan få på taktisk nivå, svarer A6 videre at:

> Det medfører en økt bevissthet rundt at det ikke er noen bakre områder, alt er fronten. De flotte fine brigade KOene eksempelvis, der tror jeg bare vi må finne en annen løsning. Logistikken kan ha et fint og flott område i bakre hvor det er trygt, det eksisterer ikke. Alle som deltar i striden må operere som om de er i fronten. Alle må søke skjul, spredning og de samme prinsippene. Det er hoved take awayen.

I hovedsak indikerer denne isolerte analysen at intervjuobjektene har en begrenset forestillingsevne når det gjelder hvordan UAVer spesielt utnyttes til det fulle. Gjennom dette viser majoriteten av intervjuobjektene at de møter ny informasjon med kognitiv letthet, hvor de heller tar i bruk tidligere innlært kunnskap. Det vil si at det er mulig at de ikke vurderer dette som betydelig nok, ikke evner å utlede hvilke implikasjoner dette kan få eller ikke opplever informasjonen som gyldig. Det kan også oppstå fordi presentasjonen kan føre til informasjonsoverflod, hvilket gjør at de lederne må være mer selektive i hva som er verdt å ta med seg. I dette perspektivet er det også registrert at det kun er én av intervjuobjektene som synlig har notert kommentarer og trekker dette frem i beskrivelsen sin senere. Dette kan også føre til at lederene *må* overforenkle svært komplekse temaer for å kunne forholde seg til dem. I dette perspektivet kan det være rasjonelt for ledere knyttet til manøverenheter å fokusere på den største trusselen, nemlig UAVer som sensorer for artilleriet.

Denne overforenklingen, eller heuristikken er også gjenkjennbar der intervjuobjektene behandler kategorien eliteinfanteri og proxykrigere. Her gjengitt gjennom besvarelsene fra henholdsvis A3 og A5:

> Ja, det her er jo heller ikke noe nytt. Det som kan sies å være nytt er noe av kapasitene til disse enhetene. Vi vil alltid ha en fiende i forterrenget [les: dypet]. Og hvis man skal tenke utelukkende konvensjonelt, så er det bare sånn det er. Fienden vil alltid søke å lokalisere deg, finne ut hva du har tenkt til å gjøre. Det i seg selv er ikke nødvendigvis noe nytt. Den store forskjellen, om det er noen, er at motstanderen er i stand til å drive målbekjempning lenge før han er på plass, han er i stand til å gjennomføre begrensede direkte aksjoner for å lamme vår K2.

> Det er jo at.. I det kampelementene, nøkkelfunksjoner/ledere vil bli skutt og drept, lenge før kampelementene går inn. Man må belage seg på at alt man møter på kan være fiendtlige. Områder vi trener på i forbindelse med planverk og så videre er mest sannsynlig ikke sikre .. En kan møte på folk man ikke vet hvem er, de kan like gjerne snakke norsk. Den paramilitære dimensjonen vil nok være veldig vanskelig å forholde seg til.

På tross av lengre og relevant tjenestetid i stab, fremstår A3 noe motvillig til å erkjenne at spesialstyrker, skarpskyttertropper og paramilitære enheter på dypet, utstyrt med mer teknologi, utgjør en mer kompleks og kompetent trussel. Som respondenten påpeker selv, indikerer dette at trusselen vurderes fra et tradisjonelt konvensjonelt perspektiv, hvilket kan begrense evnen til å forestille seg denne typen trussel i neste konflikt. A5 behandler tilsynelatende også temaet fra et mer stridsteknisk perspektiv, som kan forklares med at vedkommende avtjener sine pliktår som troppsjef. I tillegg kan det tyde på at respondenten blir utsatt for kognitive skjevheter med overforenkling av mer komplekse problemstillinger.

Her kunne det vært interessant å utvide perspektivet på mulige formingsoperasjoner fienden kan utføre på dypet. Ikke bare fysiske sabotasjeaksjoner som rammer sivil infrastruktur, som eksempelvis strømleverandører, eller sambandssystemene til Forsvaret. Sabotasje knyttet til flyplasser, havner og knutepunkter i Nord-Norge, støttet av mer teknologi som tillater styrkene å opprettholde sine fordekte operasjoner, kunne ha vært interessante scenarioer. Type scenarioer hvor det er flere parallelle aksjoner hvor også Forsvaret må støtte. Eksempelvis mindre og mobile EK systemer som kan påvirke og delvis lamme systemer, samtidig som væpnede styrker jammer all kommunikasjon og fysisk overtar kontrollen på kritiske installasjoner. Lignende scenarioer er trolig ikke usannsynlige for militære ledere, men fremstår som utenkelige – eller utenfor forestillingen av stridsfeltet.

Dette leder til den andre delen av analysen. Den tar for seg hva militære ledere utviser mindre kunnskap om, og også mindre evne til å reflektere rundt. Spørsmålet intervjuobjektene blir stilt handler om integreringen av cyber, EK og informasjonskonfrontasjon, og hvordan dette vil virke inn på det taktiske nivået. Alle intervjuobjektene svarer på spørsmålet ved først og fremst å belyse perspektiver rundt elektronisk krigføring og implikasjonene av den. Forskjellene i svarene ligger i hvor utfyllende og nyanserte de er, her eksemplifisert gjennom A1: «Taktisk samvirke blir mer og mer aktuelt. EK i seg selv gir lite hvis du ikke kombinerer det med en kampplattform. De trenger hverandre for å utnytte maksimal effektivitet». Mindre tjenesteerfaring visualiseres her gjennom kortere besvarelser og mer bestemte uttrykksformer. Den elektroniske krigføringen med alle dens aspekter kan brukes både til å finne mål og til å ødelegge mål. Det kan være meget krevende, kanskje umulig, å gjemme seg for en fiende som besitter avansert EK-teknologi. Noen intervjuobjekter belyser dette (A2): «Vi må tilbake til

banale enkle ting som blir viktig da. Som basisteknikken i kamuflasje, det å sende på lav sendeeffekt, RTX, sambandsdisiplin, som igjen krever lang tid i trening. En rå tilnærming i å være grundig i alt man gjør for å kunne motstå det her». A3 understreker også viktigheten:

> På taktisk nivå så tror jeg vi er inne for en overraskelse, fordi vi er avhengige av den K2 [kommando og kontroll] vi har i dag. Motstanderen har mer enn nok kapasitet til å både redusere vår evne til K2, men bruker også EK i en offensiv setting, med å peile og bruke det inn i kjeden sin. Så konsekvenser på taktisk nivå er jo, sånn som i dag, at man ikke kan være avhengig av K2 systemer.

Videre presierer A3: «Selv om vi liker å si at vi driver med oppdragsbasert ledelse, så gjør vi det helt til sambandet forsvinner, så blir det kaos. Så der har vi nok en vei å gå. Hvis man skal tenke seg en liten stund inn i fremtiden, så er nok vårt beste alternativ å bli lavteknologisk». Perspektivet knyttet til hvordan det påvirker kommando og kontroll kan det trekkes paralleller til også hos A6:

> En ting jeg har vært veldig opptatt av [...] Det er det fysiske lederskapet. Du kan aldri jamme ut det at jeg som kompanisjef løper bort til troppsjefen og snakker face til face med en intensjon, målsetning og sluttilstand. Jeg ser at vi tillegger oss en måte å lede på hvor vi er opptatt av at sjefen skal være rolig, litt lenger bak og det skal være fint og flott på samband. Så vi trener på en måte som ikke er mulig å få til i praksis. Men jeg er veldig opptatt av det der, det Ingar Lund sier: Det å kontre ny teknologi med gammel teknologi. Det var en ting som jeg for eksempel gjorde da jeg kom inn i kompaniet. Bare sånn som at måten de opererte på da var jo helt sjanseløs i forhold til en dronekapasitet hos fienden. Det er en kapasitet som vi vet er der. Den har jeg selv ganske god innsikt i og har brukt det selv. Så det er en helt konkret ting jeg gjorde da jeg kom inn [...] Hvordan skal vi gruppere oss, hvordan skal vi sette opp baser for å motvirke dronekapasiteten. Det er veldig håndfast.

Gjennomgående indikerer analysen at lederne med erfaring fra bataljonstab og kompanisjef i større grad besitter informasjon om elektronisk krigføring. Videre vektlegger de også hvordan EK vil virke inn på de taktiske enhetene som opererer, og hvilke tiltak de kan søke å

gjennomføre for å redusere denne trusselen. Et interessant poeng i denne sammenhengen er at presentasjonen også gir informasjon om russernes evne til å eksempelvis jamme artilleriammunisjon. Dette er det bare respondenten med artilleribakgrunn (A2) som kommenterer i intervjuet. Dette kan også indikere at mer teknisk orienterte detaljer utelates underbevisst dersom de militære lederne ikke har erfaring, bakgrunn eller kunnskap om dette fra tidligere. Igjen kan dette overføres til en kognitiv lukkethet og en bereftelsestendens når det gjelder ny og mer ukjent informasjon.

Spørsmålsstillingen søkte å få de militære lederne til å uttale seg om samvirket mellom EK, cyber og informasjonskonfrontasjon og hvordan det kan komme til uttrykk på taktisk nivå. I analysen kommer det imidlertid frem at kun én bevisst omtaler cyber som fenomen. Her benytter A2 ulike eksempler på hvordan effekten av nettverksoperasjoner kan spre seg til enheter på bakken:

> Cyberdomenet, hva skjer om de er inne i systemene våre allerede. Da tenker jeg på sånn hacking. Blue force trackerne våre kan bli red force trackere dersom man gir det til fienden. Da har han kontroll på hele brigaden [....]... Den appen som kom i høst å lage et gammelt ansikt, når du lastet ned appen som fikk du tilgang til alle bildene dine på telefonen. Da har du et bredt OSINT grunnlag uten mye arbeid. At vi må være vare for sånne ting, er relevant. Skillet mellom ikke-taktisk og taktisk sjef sitt ansvar viskes ut.

Dette skiller seg ut også ved de andre kapasitetsområdene, ved at det ikke brytes ned til det taktiske nivået spesifikt, og at intervjuobjektet ikke trekker vurderingene videre til hvordan dette påvirker og hvordan man kan redusere disse truslene. De fem andre intervjuobjektene utelater å behandle temaet cyber, med unntak av A3 og A4, som henholdsvis påpeker at det prates lite om det, og at det kanskje treffer brigadenivået mer enn det taktiske nivået. Det er åpenbart at militære ledere kan svært lite om det tekniske domenet cyber, og har også liten forestillingsevne om hvordan trusler i cyberdomenet kan materialisere seg, samvirke og påvirke enhetene. Det er grunn til å anta at en fiende vil søke å utnytte dette kunnskapshullet.

Det siste temaet for spørsmålet var informasjonskonfrontasjon. Dette temaet ble heller ikke berørt i utstrakt grad av intervjuobjektene. En av respondentene har fersk erfaring fra grensen mot Russland i Øst-Finnmark. Vedkommende er den respondenten som i størst grad uttaler seg om effekten:

> Jeg tenker på påvirkningsoperasjoner. Å tippe en befolkning er nok større og mer aktuelt enn det vi tror, spesielt her oppe i Kirkenes. Sammenligner man Kirkenes med det som skjedde i Ukraina, så er det likhetstrekk. På innflytelse fra Russland. Vi ser at 75-års markeringen her oppe er så viktig for å vise at befolkningen her oppe er en del av Norge. Akkurat den var både Kongen og regjeringen tilstede på. Innflytelsen her oppe er nok større enn det man skulle tro. Butikkskilt på russisk. Mange ansatte er russiske. Den russiske ortodokse kirken blir brukt for å omvende folk i Kirkenes. Påvirkningsoperasjoner og EK, det ser man her oppe.

Det er viktig og relevant at respondenten har fersk erfaring fra grensen i Øst-Finnmark. Vedkommendes understreking av påvirkningsoperasjoner indikerer at bevisstheten om en aktuell trussel øker markant ved nærhet til og egen erfaring med trusselen. Det er nok selvsagt, men det har store implikasjoner for læring og bevissthetsøkning i andre deler av organisasjonen. Alle kan ikke ved selvsyn få økt bevissthet om det teknologiske stridsfeltet. Tvert imot vil bare et fåtall få slike erfaringer, og det vil være nødvendig å finne andre måter å lære opp organisasjonen på. Generelt indikerer analysen at fire av seks intervjuobjekter ikke uttaler seg om dette aspektet ved striden overhodet, og at to overfladisk peker på temaet, da relatert til befolkningen i Finnmark. Ut fra dette er det ikke urimelig å konkludere med at militære ledere på de nivåene som omfattes av denne undersøkelsen har begrenset forestillingsevne og trusseloppfatning av spesielt cyber og informasjonskonfrontasjon på det teknologiske stridsfeltet. De militære lederne utviser kognitiv letthet i måten de behandler et komplekst spørsmål på, og kognitiv lukkethet for de mer ukjente og tekniske aspektene ved striden.

3.1.1 Delkonklusjon

Kapasiteter og områder av den teknologiske striden som militære ledere allerede har kunnskap om, er blitt eksponert for og har trenet og øvd på, vurderer intervjuobjektene

generelt mer utfyllende, nyansert og praktisk. Dette er grovt sett: kampvogner, indirekte ild og delvis UAVer. Når det kommer til spørsmålene som dreier seg om de mer tekniske og tradisjonelt ikke-kinetiske domenene, som EK, cyber og informasjonskonfrontasjon, gjenspeiler svarene at det generelt er lav kompetanse og høyst begrenset evne til å forestille seg truslene og hvordan de kan påvirke de styrkene på bakken som lederne har ansvaret for, og selve utfallet av striden. Ny og mer teknisk informasjon blir tilsynelatende møtt med en kognitiv letthet og lukkethet, som begrenser evnen til å tenke utenfor boksen i situasjoner de militære lederne tidligere har fått skissert.

Dette kommenterer Anonym 4 i tilknytning til hvordan militære ledere skal holde seg oppdaterte: «I all den tid vi ikke har opplevd å møte en teknologisk likeverdig eller overlegen fiende, er vi nødt til å se til historien eller bruke fantasien (les: litteratur) for å øke forståelsen». Evnen til å bruke fantasien, utlede informasjon og tilpasse seg nye forutsetninger fremstår imidlertid som noe begrenset hos de militære lederne. Det er også relevant å trekke frem at de militære lederne viser en form for oppfatningsutholdenhet. Det vil si at de som utleder mest informasjon rundt UAVer, EK og påvirkningsoperasjoner også er de som delvis belyste disse forholdene før presentasjonen av en teknologisk motstander ble gitt. Dette underbygger og forsterker den registrerte tendensen hos respondentene til å validere sin egen kunnskap og innsikt i møte med ny informasjon. Flere intervjuobjekter blir utsatt for kognitive skjevheter knyttet til deres besvarelser. På dette feltet bruker flere av intervjuobjektene tidligere kunnskap som utgangspunkt for å fortolke også ny informasjon, som er menneskelig, men også en risiko for militære beslutningstakere.

3.2 Hvordan vurderer militære ledere egen kunnskap?

Hvordan vurderer så de militære lederne sin egen kunnskap og evne til nytenkning? Før dette spørsmålet besvares, er det viktig å etablere en forståelse av viktigheten militære ledere tillegger nettopp dette. Desto større betydning et kompetansefelt tillegges, desto mer engasjement og nysgjerrighet på feltet skulle det være å forvente. Intervjuobjektene i studien presiserer at det å forstå det teknologiske stridsfeltet er viktig til *særdeles viktig*. A1 påpeker at: «Det er viktig, og blir mer og mer viktig [...] Mye i dag handler om teknologisk forståelse og innsikt». A3 mener videre at: «Det er svært viktig å forstå teknologiens plass på

stridsfeltet. Det handler i første omgang om å kunne utnytte styrkene og begrense svakhetene ved egen teknologi, og omvendt for motstanderens teknologi». Intervjuobjektene fremstår som homogene i hvordan de vektlegger viktigheten av å forstå, og de må dermed tolkes dit hen at de er engasjerte og motiverte for å tilegne seg denne innsikten.

Videre ble intervjuobjektene spurt om hvor kompetente og oppdaterte de anså seg selv for å være. Flere av lederne svarte at de var oppdaterte, relativt oppdaterte eller oppdaterte i forhold til sine arbeidsoppgaver. Ett intervjuobjekt medga ved dette spørsmålet følgende (A6): «Ja, hvis jeg skal være helt ærlig, så skal jeg si at jeg er ikke helt oppdatert. Jeg sitter ikke med detaljkunnskap på sensorsystemer og radarer og sånne ting». I tillegg svarte A1 at vedkommende ikke hadde mye kunnskap. Det interessante ved disse besvarelsene er at respondentene generelt anser seg som over gjennomsnittet oppdaterte og kunnskapsrike. Respondenten som svarer at han ikke har den detaljkunnskapen som kanskje kreves, er også lederen med lengst tjenestetid, som i dag tjenestegjør som kompanisjef. En faktor med mulig forklaringskraft er at vedkommende er den eneste som har tjenesteerfaring utenfor Hæren. Faktorer som tjenestetid, alder og erfaring fra ulike grener, avdelinger og garnisoner farger svarene i ulik grad. Helhetlig sett indikerer dette spørsmålet at utvalget med bakgrunn utelukkende fra Hæren svarer homogent, og er i sitt selvbilde oppdaterte på teknologiske trusler.

Etter de innledende spørsmålene fikk hver respondent 15-20 minutter til å lese gjennom analysen av en teknologisk motstander. Det første interessante er at lederne med lavest antall år i tjenestetid også er de som bruker minst tid på å fordøye analysen (generell observasjon, ikke kvantifisert i antall minutter). Tre av de seks intervjuobjektene bruker ikke all tilgjengelig tid til å sette seg inn i presentasjonen, hvilket markerer et skille til de tre andre som tjenestegjør i bataljonstab og som kompanisjef. Ingen av lederne bruker lengre tid enn det som er tilmålt, eller kommenterer at det var for lite tid til å sette seg inn i mye informasjon. Dette er også relevant da flere av sidene i presentasjonen inneholder mye data og teknisk informasjon, som kunne være nytt for flere av intervjuobjektene.

De med lengst tjenestetid og erfaring fra bataljonstab svarer gjennomgående lengst i antall ord, mest nyansert og trekker i større grad inn nivåene over det taktiske, andre forsvarsgrener,

samt belyser taktisk samvirke og fellesoperasjoner. Disse utviser en større evne til å sette bestanddelene i sammenheng og til å belyse at taktisk sjef på bakken i dag må beherske og ha kompetanse over et vidt spekter av virkemidler. Dette kan trolig skrives på kontoen for at kompanisjefer og personell i stabsfunksjoner i mye større grad må ivareta samvirke og bidra til å planlegge operasjoner i bataljonen, i rammen av en større organisasjon.

Det at ledere med mindre fartstid bruker kortere tid på å sette seg inn i ny informasjon, kan indikere kognitiv lukkethet. Her kan man heller ikke utelukke et annet forhold, nemlig at undertegnede har en høyere militær grad enn de som tjenestegjør som kadett og troppsjefer. Dette kan bidra til ønsket om å fremstå som effektive i gjennomlesning og besvarelser. Kanskje også en direkte frykt for å fremstå som trege i møte en overordnet.

En form for forutinntatthet kan også registreres gjennom til A4: «Jeg hadde lyst til å prate om droner og artilleri. Det er en måte de har brukt det på i Ukraina og Krim, og en måte vi ikke bruker det på. Det er to forskjellige verdener å leve i at vi må ta innover oss den måten de bruker det på, for det er ganske effektivt». Flere av de militære lederne bekrefter etter å ha lest gjennom presentasjonen at de indirekte har validert informasjon de allerede hadde, og gjerne relatert til tjenestestillingen de har, hvor dette påvirker kunnskapsnivået.

Gjennom studien fremkommer det også forskjeller i hvor stor grad den militære lederen lar seg overraske av ny informasjon, eller anerkjenner at det var nytt. Generelt svarer fem av seks intervjuobjekter at det totalt sett ikke er noe nytt eller fullstendig ukjent. Denne forskjellen kan kontrasteres gjennom to besvarelser (A5):

> Definitivt. Den sliden der du forklarer hvor ting er på stridsfeltet. Det med, de verktøyene de har for å lede indirekte ild. Det er mer nytt. Det paramilitære er en del av den skissen, som vi bare har pratet om. Alle kapasitetene har vi gjerne sett før. Jeg er klokere nå på dette med måldata og hvor de er nå på det å kunne sende informasjon og måldata. Det spennet av UAVer var jeg heller ikke klar over.

A5 tjenestegjør i sitt første år som troppsjef og er tilsynelatende klar over egen uvitenhet, hvor den ligger og kan anerkjenne dette i intervjuet. I motsatt tilfelle kan man registrere ordlyden i hvordan gjennomsnittet svarer i møte med dette spørsmålet (A6):

> Hvis du ser veldig grovt på det, så var det ikke noe nytt. Jeg vet at vognene utduellerer våre vogner, at de har mye mer PV kapasiteter med mye lengre rekkevidde enn javelin. Jeg vet om deres UAV kapasiteter og indirekte ild med rekkevidde. Så er det at man må enda mer inn i de konkrete dataene da...

Det later ikke til at intervjuobjektet er klar over at vedkommende faktisk ikke har svart på hvordan cyber og informasjonskonfrontasjon utspiller seg eller har registrert informasjonen på disse feltene i presentasjonen. I tillegg belyser A6 at man må kjenne til detaljer og ha inngående kunnskap for å vurdere hvordan dette påvirker. Dette understreker respondenten ved flere anledninger, med intensjon om å påpeke at en sjef ikke må pålegge seg bindinger og begrensninger som ikke er nødvendige. I denne spesifikke sammenhengen hvor A6 påpeker detaljgrad, kan det leses som et rasjonale for at ledere ikke skal grave for dypt etter detaljer, for å unngå at planene blir for komplekse. Dette kan også bære en risiko ved at man underbevisst etablerer et grunnlag for at man ikke fullt ut skal forstå de teknologiske truslene. Generelt kan analysen spore en mangel på bevissthet og ydmykhet knyttet til egne svakheter på enkelte kapasitetsområder. Dette er fremtredende hos fem av de seks intervjuobjektene.

3.2.1 Delkonklusjon

Gjennom studien ser man gjennomgående at de militære lederne påpeker viktigheten av å være oppdaterte, at det er i stor grad troppsjefs og kompanisjefs ansvar, og at de opplever seg selv som oppdaterte. Likevel ser man at majoriteten ikke svarer på spørsmål som er knyttet til de mer tekniske og ikke-kinetiske aspektene ved den teknologiske striden, og ikke har utviklet noen bevissthet rundt dette. Dette sannsynliggjør funnet om at militære ledere generelt overvurderer sin egen forståelse for den teknologiske striden. I et fremtidsrettet perspektiv ligger det en stor risiko i at militære ledere ikke synes å være oppmerksomme på denne overkonfidensen og kognitive skjevheten. Videre kan man av analysen trekke ut tendensen til at yngre offiserer, eller offiserer med kortere tjenestegjøring i Hæren har en sterkere tilbøyelighet til å bruke mer bastante uttrykksformer og mindre nyanser i hvordan de

adresserer teknologiske trusler. Denne kognitive lukkingen kan også representere en risiko i møte med nye og uforutsette situasjoner. Dette kan bidra til at offiserer blir mindre tilpasningsdyktige og fleksible enn det operasjonsmiljøet kanskje krever. Dette blir også belyst av A6:

> Jeg ser jo at det er veldig mange som trener på den måten de gjorde før. Den måten de selv har lyst til å sloss på. «Jeg har lyst til å være manøverbataljonsjef i denne fine bataljonen, jeg skal rykke frem på den måten som jeg alltid har gjort». Og det er en divergens jeg ser... Sorry mac, det er ikke denne krigen som du nå skal sloss. Der tror jeg mange har litt å gå på.

Kognitive skjevheter hos militære ledere kan i møte med en teknologisk motstander gi fienden et større fortrinn på stridsfeltet. Dette er imidlertid ikke unikt for enkelte stater, og uttrykkes godt gjennom den amerikanske RAND-forskeren Carl Builder når han sier at man ser at de ulike grene har forskjellige personligheter (les:kulturer) som påvirker i hvor stor grad de er innovative. Gjennom hæren mener de å kunne se en personlighet som er fanget mellom behovet for å drive mekanisert strid etter andre verdenskrigs avstøpning, og behovet for å drive stabilitetsoperasjoner i en post-kald krig verden (Grissom, 2006, s. 14).

4 Et spørsmål om kultur?

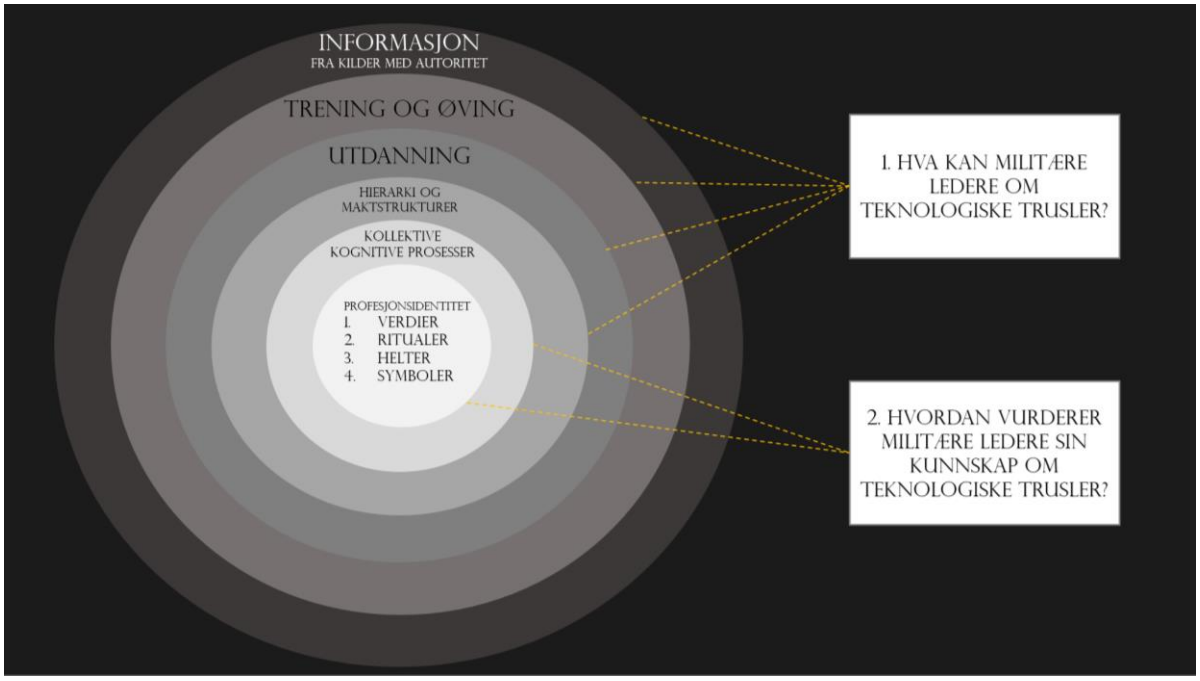
Hva kan forklaringen være på at den reelle kompetansen om teknologiske trusler er lav blant militære ledere? Og hvorfor overvurderer ledere i Hæren sin egen kompetanse og innsikt? Utover det åpenbare i at rammebetingelsene for å videreutvikle kompetanse kan være varierende i en hektisk hverdag, kan de reelle og dypereliggende årsakene være mange og sammensatte. I denne delen lanseres det noen mulige forklaringer (hypoteser) knyttet til hvert av disse to spørsmålene. Med utgangspunkt i til sammen seks hypoteser gjøres det et forsøk på å finne en hovedforklaring. Ved å identifisere årsakene kan det kanskje iverksettes tiltak for å utbedre kunnskapshull og kognitive fallgruver knyttet til den teknologiske striden. De seks hypotesene knyttes til de to hovedspørsmålene i dette kapittelet, fire til det første spørsmålet og to til det andre:

Hvorfor er den reelle kompetansen om teknologiske trusler lav på enkelte områder?

1. Skjermede miljøer
2. Lav grad av eksponering
3. Utdanning ute av takt
4. Hierarki og homogene grupper

Hvorfor overvurderer militære ledere i Hæren egen kompetanse og innsikt?

1. Kognitive prosesser
2. Profesjonsidentitet



Figur 15. Forklaringsmodell for de seks hypotesene som fremstilles for studien.

En annen måte å sortere disse seks hypotesene på er gjennom modellen over, figur 15. Bindingene mellom spørsmålene og forklaringsfaktorene er illustrert med gult og representerer de primære årsakene til situasjonen. Likevel vil eksempelvis verdier, symboler og helter også kunne forklare hvorfor militære ledere kan lite om teknologiske trusler. Derfor er det viktig å se på alle de seks faktorene som deler som samlet sett svarer på de to spørsmålene. Dette vil jeg se nærmere på mot slutten av kapittelet.

4.1 Skjermede miljøer

Den første hypotesen går ut på at tilflyten av informasjon er begrenset, og derfor skaper dårlige forutsetninger hos militære ledere til å være oppdaterte og kunnskapsrike. Denne hypotesen er mangefasettert. For å dykke dypere i den, kan det være hensiktsmessig å belyse hypotesen i form av flere faktorer, som: Skjerming, norsk organiseringsmodell og systemer for og kapasitet til informasjonsdeling.

En mulig forklaring på at militære ledere ikke forstår enkelte kapasitetsområder, samvirket og kompleksiteten, er tilgjengeligheten på informasjon og den norske organiseringsmodellen. Cyber, EK og etterretning og er områder som naturlig er preget av skjermingsverdig informasjon og hemmelighold. Avdelingene som forvalter disse områdene er også fysisk avskjermet fra andre avdelinger, hvilket kan føre til at utvekslingen av informasjon og forståelse er liten. Videre har det norske forsvaret tilsynelatende lagt ned PSYOPS, eller avdeling for psykologiske operasjoner. På den måten er påvirkningsoperasjoner for Hæren primært noe andre stater holder på med, som bidrar til at det blir vanskeligere å forstå hvordan andre bruker dette virkemiddelet. UAVer er også et eksempel på et kapasitetsområde der det er få innvidde med utdanning, det er en begrenset kapasitet og det er igjen få som tilegner seg informasjon og forståelse. Her kan organisatoriske forhold medvirke til at forståelsen hemmes. Dette understøttes av A6, som påpeker at den interne organiseringen i Forsvaret ikke ligger til rette for fullt ut å forstå dette området:

> På kompaninivået må du være mye mer forberedt på å bli utsatt for combined arms, hvor også EK og cyber er en integrert del av det. Hvis du ser her i Norge, så er vi ganske sånn domenedelt, både på kunnskap og hvordan vi kontrer det. Det er tilbake til det vi begynte med. Det blir veldig mye synsing om det.

Mangelen på informasjon som kan sammenstilles og frigis, med den norske delingen av cyber og EK, kan bidra til mindre kunnskap og helhetsoversikt. A3 legger tilsynelatende til grunn at ettersom at det gis lite informasjon, så definerer det hvilket fokus det får: «Psyops og cyber er vel ting som det i veldig liten grad prates om. Som en del av en operasjon så er ikke det noe vi har et tungt fokus på». Dette kan tolkes dithen at lite til inget informasjonstilfang om tekniske fagfelt gjør at det er svært vanskelig å skape forsåelse i de taktiske enhetene i Hæren, og

dermed få til en prioritering av dette.

Flere i studien påpeker også rollen Hærens Våpenskole (HVS) og Forsvarets Forskningsinstitutt (FFI) bør ha for å drive kunnskapsformidling. A3 vektlegger et moment i dette perspektivet: «[...] Man kan tenke seg at FFI har et ansvar for fremtidige teknologier, mens HVS har et ansvar for eksisterende teknologier. Det kan, og er i praksis, ofte fagområdene selv som deler informasjon». Det interessante med dette perspektivet er at de militære lederne nesten utelukkende fokuserer på lavteknologiske midler for å kontre en mer teknologisk orientert motstander. Utover lengre rekkevidde på artilleriammunisjon og evnen til å jamme fiendens kapasiteter, så er det enkeltmannsferdigheter og prosedyrer på tropps- og kompaninivå som blir gjengitt som effektive motmidler. Dette kan indikere at det er for svak tilknytning mellom de som utvikler og forsker på ny teknologi og de som skal omsette teknologien i praksis og utnytte de fordelene den kan gi.

Utfordringen ved at fagmiljøer selv sprer informasjon og oppdateringer, er at informasjonsbildet de sprer ikke blir sydd sammen til et større hele og distribuert på de forskjellige nivåene. A2 fremhever også Våpenskolens ansvar og hvilke utfordringer vedkommende ser med denne: «Det første som slår meg er jo Våpenskolen. De skal jo drive doktrineutvikling, og de gjør det jo også for oss, men er altfor underbemannet. Vi henger etter på spesielt reglementsiden». Tilgjengelighet på helhetlig informasjon og hvordan dette påvirker prosedyrer etterlyses altså i større grad fra spesielt personell som har gjennomført troppsjefstjeneste. Dette er en faktor som trolig har stor innvirkning på hvilken kompetanse og forståelse som skapes. Det kan tenkes at dersom teknologiske trusler blir for kompliserte og teknisk detaljerte til at det kan forstås, så er det HVS som må prosessere og operasjonalisere dette bildet til håndterlige og effektive prosedyrer. I fravær av dette, er det naturlig at militære ledere ser til løsninger de kan få til med det materiellet og personellet de har til rådighet.

A6 påpeker at det kan fremkalle negative konsekvenser når militære ledere ikke har nok detaljert informasjon til å trekke de riktige slutningene. Dette eksemplifiserer han med at det er stor forskjell på om fienden kan spore din sambandsbruk med mobiltelefon og radioer til en nøyaktighet på noen metre og flere hundre metre. Dersom taktiske sjefer ikke vet, er det fare for og helt åpenbart at de legger for store begrensinger på seg selv, for å ivareta en

sikkerhetsmargin. Respondenten understreker med dette viktigheten av å få nok detaljert informasjon og helhetsoversikt i bataljonene, slik at man kan utlede gode slutninger som ikke begrenser striden og mulige fortrinn. Det handler om å prosessere data og detaljer nedover i organisasjon med implikasjoner og oppdatering av prosedyrer. Kanskje trenger ikke Hærens ledere fatte de samme tiltakene i Sør-Varanger og Porsanger som på Huseby eller Rena. Men de må vite *hvorfor* konteksten tilsier at de gjør det forskjellig, uten å frata seg selv muligheter.

Dette kan ses som bottom-up innovasjon: Lederne på det taktiske nivået opplever trusler på nært hold som medfører et behov for å utvikle nye prosedyrer. De som sitter nærmest problemet tar tak i det og finner adekvate løsninger til riktig tid (Adamsky & Bjerga, 2012, s. 188). Utfordringen med dette er at dersom innovasjonen skjer på et lavt nivå, vil underenhetene i Hæren kunne utvikles i forskjellige retninger. I organiseringen av Hæren er derfor dette ansvaret plassert hos HVS. Våpenskolen bør være et toneangivende miljø for hvordan man møter ny teknologi med et top-down perspektiv.

I den virkelige verden er imidlertid utfordringen den at det ikke er HVS som sitter på informasjonen, selv om den altså bør utføre analysene og utforme tiltakene. Informasjonen kommer eksempelvis gjennom oppdateringer fra etterretningsapparatet, rapporter fra Cyberforsvaret og Nasjonal sikkerhetsmyndighet (NSM) – eller fra FFIs forskning på påvirkningsoperasjoner og hybride trusler. Ettersom fagmiljøene er adskilte, og fora for samarbeid og utveksling trolig ikke er etablert, kan det tenkes at ansvaret for å sy sammen et helhetlig bilde og utlede betydningen blir større for de miliære lederne i de forskjellige bataljonene. Gitt at ansvaret dermed implisitt øker på dette nivået, kan vi også få en økende risiko for at militære ledere vil vurdere og oppfatte trusler og påvirkning ulikt. Selv om dette samlet sett kan gi en større bredde i forståelser og løsninger, kan det også representere en fare for at Hærens enheter blir fragmenterte og mindre effektive i militære operasjoner. Dette problemet øker ved at den norske Hæren er relativt liten og helt avhengig av kraftsamling om både stridsidéer og gjennomføring av operasjonene.

Oppsummert påvirker trolig både skjerming og gradering av informasjon, norsk organisering og informasjonsdeling hvor oppdaterte militære ledere er om teknologiske trusler.

4.2 Lav grad av eksponering

Den andre hypotesen baserer seg på at lav eksponering for teknologiske trusler gir dårlig forberedte ledere. Flere eksempler gjennom intervjufasen har tydeliggjort at eksponering for teknologiske trusler kan bidra til å øke forståelsen. Med eksponering refereres det her spesielt til avdelingenes evne til å integrere teknologiske aspekter i trening og øving. Dette fremheves blant annet av hvordan kompanisjefen (A6) omsetter sin inngående og detaljerte kunnskap om EK, til en praksis i kompaniet hvor alle planer skal tilfredsstille et krav om enkelhet og lite koordinering.

> Det siste er jo signaletterretning, jamming og sånne ting. Det har jeg vært veldig fokusert på i forhold til å trene kompaniet. Vi skal aldri legge en plan som er avhengig av samband for å utføres. Det er alltid en faktor jeg har i planprosessen. Så jeg vil si at jeg er veldig opptatt av det, og jeg ser direkte effekter av at vi er opptatt av det, det er at planen blir enklere og den blir bedre.

Alle planer skal kunne gjennomføres uten samband og koordinering, og kompanisjefen understreker det fysiske lederskapet overfor sine underordnede. Videre refererer kompanisjefen (A6) også til Trident Juncture, hvor kompaniet skulle kjempe mot en spansk motorisert bataljon, og fikk erfare deres overveldende targetingprosesser på nært hold. Erfaringen respondenten tok med seg, var at planlagt mobilitet og oppholdende strid var et definitivt fortrinn mot en styrke med overlegen kvantitet og rekkevidde på indirekte ild.

> En viktig slutning som jeg tok med fra det var at tiden det tar fra vi engasjerer motstanderen til vi flytter oss må vi minimere. Vi kan ikke legge opp til at vi skal bli og sloss over tid. Da kommer vi til å bli lempet tung ild på og være ferdig... [...] Så det vi gjorde var at vi satt opp, ved den ene høyden som dominerte broen, der satt vi opp falske telt, skapte et inntrykk av at det var der vi var for å forme fienden slik at vi kunne komme inn asymmetrisk og stikke han i siden.

Det kan tolkes som at når lederen blir utsatt for konkret trening og øving mot en teknologisk motstander, ble tvunget til å planlegge for disse problemstillingene. Gjennom dette

eksempelet kan man utlede at enkelte ledere også vil lykkes i å omstille seg mot mer teknologiske trusler, men at det ligger en risiko å møte truslene for første gang i fullskala krig.

Troppsjefen som tjenestegjør på grensen til Russland i Øst-Finnmark (A5) reflekterte spesielt rundt påvirkningsoperasjoner og evnen til å forme befolkningen i Finnmark. Trolig fordi troppsjefen geografisk kjenner på trusselen og dermed blir eksponert. Evnen til å implementere teknologiske trusler i caseløsning, trening og øving kan synes å være viktig for å både skape forståelse, utfordre ledere til å tenke annerledes og til å skape motivasjon for å utvikle kompetansen. Cyber fremstår som det området som i minst grad blir integrert i trening og øving.

Eksponering for teknologiske trusler virker tilsynelatende ikke å være systematisert gjennom Hærens mange avdelinger, fra utdanning og gjennom tjeneste. Trolig gir det gode resultater direkte og indirekte når organisasjonen velger å utsette sine ledere for disse nye og relevante utfordringer (FFI, 2016, s. 38). Dette aktualiserer behovet for å se nytt på hvordan Hæren trener og øver.

4.3 Utdanning ute av takt

Den tredje hypotesen peker på at utdanningene er med på å skape grunnlaget for å forstå nye og ukjente problemstillinger. Med utdanningsløp som er ute av takt med utviklingen svekkes militære lederes evne til å forstå og motivasjonen for å øke egen kunnskap. Hypotesen vil derfor testes ved å se på emnebeskrivelser på henholdsvis Krigsskolen og Stabsskolen.

Flere av intervjuobjektene er oppmerksomme på hvilken rolle utdanning spiller i å forstå og utvikle bevissthet om teknologiske trusler. I intervjuene kommer dette til uttrykk gjennom spørsmålet om hvem som bærer ansvaret for å holde personellet oppdatert. Det henvises da spesielt til Krigsskolen og Stabsskolen av flere intervjuobjekter. I lys av dette er det interessant å se hvordan det legges til rette for denne forståelsen. Her gjennom Krigsskolen og den operative utdanningen, og ved Stabsskolen, for fulltidsstudentene.

4.3.1 Krigsskolen

Ved Krigsskolen kan man lese ut av studiemodellen og emnebeskrivelsen *Kontekst Landoperasjoner (OPS2201)* at kadettene ved operativkullet fra og med 2018 har et dedikert delemne til temaet militær teknologi og innovasjon (Forsvarets Høgskole, 2020). I henhold til de administrative rammene har delemnet 4 uker undervisningstid, hvor utvalgte læringsutbytter er disse:

> Etter fullført og bestått offisersutdanning skal kadettene ha kunnskap om og kunne oppdatere sin kunnskap om: 12. hvordan innovasjon og integrasjon av systemer og/eller teknologi skaper effekt i militære operasjoner, og kunne bidra til utvikling av ny anvendelse av teknologi i operasjoner.

Her skal kadettene blant annet kunne forklare muligheter og begrensninger ved teknologi, forklare betydningen av signaturer og andre sensorer, forklare dynamikken i teknologisk innovasjon og forklare hvilke konsekvenser dette kan ha for militære operasjoner. Emnebeskrivelsen og læringsutbyttene kan gi inntrykket av at dette er godt i tråd med behovet for kompetanse en militær leder i dag har. Det som videre er interessant, er at ett av intervjuobjektene i studien har gjennomført dette emnet. Det kunne derfor tenkes at kadetten ville være en av de som svarte mest utfyllende, nyansert, kritisk og oppdatert på spørsmålene i intervjuet. Det var imidlertid ikke tilfellet. Svarene var både kortere, med mindre innsikt og nyanser enn flere av intervjuobjektene. Dette etterlater et spørsmål om utdanningen evner å utfordre innsikt, forestillingsevne og nysgjerrighet tilstrekkelig.

4.3.2 Stabsskolen

Ved Stabsskolen kan det være utfordrende å finne emner som tydelig berører lederes forståelse av det teknologiske stridsfeltet, eller operasjonsmiljøet. Det må her sies at denne vurderingen er gjort ut fra analyser av studieplaner og andre dokumenter, og det må tas forbehold om at deltakende observasjon på emnene kanskje kunne nyansert bildet noe.

I emnet OPS4101, del 3, finner man et deltema som kan ha overføringsverdi i dette perspektivet (Forsvarets Høgskole, 2020). Del 3 tar for seg operasjonsmiljøet og dets innvirkning på militære styrkers muligheter og begrensninger. Dette omfatter historiske studier, i kombinasjon med globale trendanalyser, for å forstå hvordan dagens og morgendagens operasjonsmiljø påvirker militære styrker og militære operasjoner, inkludert ulike perspektiver på statlige og ikke-statlige aktørers motiver og strategier. I andre emner og grenvise fordypningsemner, er det krevende å se at emnene tar innover seg militære lederes behov for å forstå operasjonsmiljøet med vekt på de teknologiske aspektene. Ved master-deltidsstudiet med siste oppstart i 2017, var cyber tidligere en del av emnet *MILMA5530 Beredskap, krisehåndtering og asymmetriske trusler.* Dette virker imidlertid ikke å være en del av eller integrert i fulltidsutdanningen. Det er utfordrende å trekke ut nøyaktig hva alle emnene inneholder på et mer detaljert plan ut fra emnebeskrivelsene, eller hvordan andre emner evner å integrere disse perspektivene. Likevel ser det ut til at teknologiens rolle i operasjonsmiljøet og helhetlige perspektiver er relativt lite fremhevet i den videregående offisersutdanningen ved Forsvarets høgskole.

Denne lesningen av studieplaner og emnebeskrivelser gir grunnlag for å konkludere med at begge utdanningsløpene for offiserer og militære ledere i Hæren har lite fokus på perspektiver knyttet til teknologisk krigføring og utvikling.

4.4 Hierarki og homogene grupper

En tredje delforklaring på den lave kunnskapen om teknologiske trusler, er trolig sammensetningen av personell og den hierarkiske organiseringen av Hæren. Homogene og hierarkiske maktstrukturer bærer med seg noen utfordringer i møte med behovet for å tenke nytt og annerledes.

Hæren kjennetegnes av å være en homogen organisasjon der alle ledere gjennomgår nøyaktig den samme profesjonsutdanningen. I den grad det rekrutteres inn kompetanse utenfra, er det til støttefunksjoner utenfor selve stridsfeltet. Det er vel etablert i forskningen på svært homogent sammensatte organisasjoner (kjønn, bakgrunn, erfaring, alder og personlighetsprofil) at de ikke utmerker seg når det gjelder å finne alternative løsninger på

nye utfordringer (Beadle, 2016, s 19). På den andre siden kan det i homogene organisasjoner tas raskere beslutninger i kommandokjeden og føres et mer effektivt lederskap i strid, fordi idéene baserer seg på det samme grunnlaget. Menneskene tenker i utgangspunktet mer likt. Denne rekrutteringen og assimileringen inn i profesjonen utgjør også kvalitetssikringen for den militære makten som bærer voldsmonopolet på vegne av staten. I et slikt perspektiv gir dette god mening. Samtidig kan vi snu på det: Der det er lite mangfold er man i enda større grad avhengig av å skape et mangfold av idéer (Beadle, 2016, s 19). Her kan det virke som organisasjonen Hæren kan komme til kort, med general George S. Pattons ord: «If everybody is thinking alike, then somebody isn't thinking» (Business Insider, 2015). Mer likhet og konformitet bidrar til at militære ledere ikke trenger å lete etter nye løsninger på nye problemer, og representerer således en av de store truslene mot å møte en teknologisk motstander.

I tillegg er det vel kjent at hierarkier fort kan hemme informasjonsflyt, kreativitet og kritisk tenkning. I strenge hierarkier, som Hæren, er også organisasjonen mer utsatt for å bli dysfunksjonell dersom feil ledere bekler viktige stillinger (Beadle, 2016, s. 84). En illustrajon kan være det jeg nevnte ovenfor: Under gjennomføringen av denne studien brukte ledere med lavere grad enn forfatteren tilsynelatende kortere tid enn de mer erfarne på å prosessere informasjonen de fikk presentert. I en hierarkisk struktur kan denne tendensen tegne et farlig bilde av hvordan myndighetsforhold påvirker den rasjonelle og analytiske tankeprosessen. I tillegg er informasjonsformidling også avhengig av at sjefen oppfatter informasjonen som viktig nok til at den blir transittert videre nedover i hierarkiet, eller oppover (Posen, 1984, s. 224). Lederen i kommandokjeden kan altså bevisst og ubevisst selektere og skjerme informasjon og idéer. Mange forskere innenfor realismetradisjonen i internasjonal relasjoner påpeker at å adoptere nytt tankegods og bidra til utvikling krever at organisasjonen har visjonære ledere (Farrell og Terriff, 2010, s. 8). Dette understreker viktigheten av å utfordre lederne i organisasjonen til å holde seg oppdaterte og nysgjerrige for å møte fremtidige utfordringer og trusler.

Et siste perspektiv som påvirker hierarkiske og konservative organisasjoner, er at hæravdelinger naturlig er mindre preget av teknologi enn henholdsvis luft- og sjømakten. Dette kan bidra til å utvikle det Eliot Cohen refererer til som den «teknofobe» tendensen i *Technology and Warfare* (gjengitt av Beadle, 2016, s. 63). Denne kategorien personell har en

tendens til å degradere verdien av teknologi som faktor for militær suksess, hvilket oftere kan observeres i landdomenet (Beadle, 2016, s. 63). I FFIs rapport om *å forske på Forsvaret i fremtiden,* blir dette trukket frem som en risiko for gruppetenkning hvor man ikke vurderer fordeler og ulemper ved teknologi. Man kan med andre ord hevde at troen på lavteknologiske midler i møte med teknologiske trusler er en form for *ankring*, der dette «ankeret» vil hemme den militære lederen i ønsket om å se til andre, mer teknologiske løsninger på problemet.

Denne hypotesen belyser noen iboende utfordringer for hierarkiske, homogene og tradisjonsbundne organisasjoner. Disse aspektene påvirker trolig ledere i deres tro på teknologiske løsninger og dermed i deres forestilling av et teknologisk stridsfelt. d

4.5 Kognitive prosesser

Så, hvorfor overvurderer militære ledere egen kompetanse om teknologiske trusler? En av hypotesene handler om hvordan kognitive prosesser påvirker evnen til å forstå morgendagens utfordringer. I intervjuene observeres det en tendens til at den tradisjonelle og konvensjonelle virkelighetsoppfatningen applisert på mer komplekse teknologiske trusler. Intervjuene i studien indikerer at flere av respondentene ser på teknologiske maktmidler i lys av et tradisjonelt stridsfelt, der primært kinetiske effekter står i en kamp mot hverandre. Dette er for mange krigens ultimate uttrykksform, der kampen mellom viljene utkjempes. Likevel bør dette oppfattes som en kognitiv skjevhet hos militære ledere, der man utelukker eller undervurderer ny informasjon for å opprettholde oppfatninger om hvordan kriger skal utkjempes.

Dette kan illustreres i studien, hvor mange av de teknologiske virkemidlene kan operere som sensorer i en innledende fase, før de kinetiske innsatsmidlene tas i bruk. Dette er gyldig for UAVer, EK, cyber og informasjonskonfrontasjon. Denne fasen blir ofte tilskrevet den sivile instansen, politiet. Likevel, dersom militære ledere ikke forstår hvordan maktmidlene i denne fasen kan forme operasjoner, er det rom for å bli overrasket og handlingslammet – under *åpningsilden*. Det å applisere rammen for konvensjonell strid for å forstå det teknologiske operasjonsmiljøet kan bære med seg begrensninger. Dette belyser også delvis A2 i intervjuet:

> Jeg tror sjef Hæren har rett når han sier at neste krig vil komme overraskende på oss. Jeg tror ikke vi vil vite at vi er i krig før ganske langt uti det. Jeg tror den kommer til å starte i det teknologiske domenet, det vil være mye som er gjort, forhåndplantet i cyber før vi kommer til en fullskala krig med kinetiske midler. Det er nok mye vi ikke vet, og mye vi ikke vet at vi ikke vet.

Gjennomgående ved studien fremstår det som om militære ledere ikke er bevisste egne kognitive skjevheter og hvordan dette former deres oppfatninger og prosessering av informasjon. Det enkle tiltaket knyttet til dette kan være å øke bevisstheten, men kognitive prosesser er også nært relatert til profesjonsidentiteten. Derfor er det nødvendig å se disse som gjensidig påvirkende elementer.

4.6 Profesjonsidentitet

Den siste hypotesen fremholder at den sosiale identiteten i Hæren hindrer ledere i å fullt ut vurdere ny informasjon eller ta inn over seg nye konsepter. Under profesjonsidentitet kan man plassere både organisasjonens verdier, helter, symboler og ritualer (Hofstede, Hofstede og Minkov, 2010, s. 7-9). Identitet påvirker derfor lederens kontekstuelle utsyn – eller forståelseshorisont. Dette fremstår som viktige aspekter for å forstå hvordan intervjuobjektene svarer, og vil derfor redegjøres for her.

Idealer en offiser og leder i Hæren oppholder og streber etter kan trolig sammenfattes av den amerikanske statsviteren Samuel P. Huntington i 1957. Kompromissløshet, tydelighet, besluttsomhet, handlekraft, hardførhet, autoritet, viljestyrke og forutsigbarhet kan ses på som idealer organisasjonen er gjennomsyret av (Huntington, 1957, s. 59, 68-70,114). Idealene finner man igjen i spesielt symboler og helter. Hvilke helter organisasjonen dyrker frem som forbilder legger premisser for hvilke egenskaper og atributter ledere bør ha. I Hæren kan man finne igjen ledere som Napoeleon, Rommel, Patton – eller general Fleischer for norske forhold. Felles for de alle er at de har ledet styrker i ulike kriger og epoker, og at de

representerer idealene Huntington gjenga allerede i 1957.

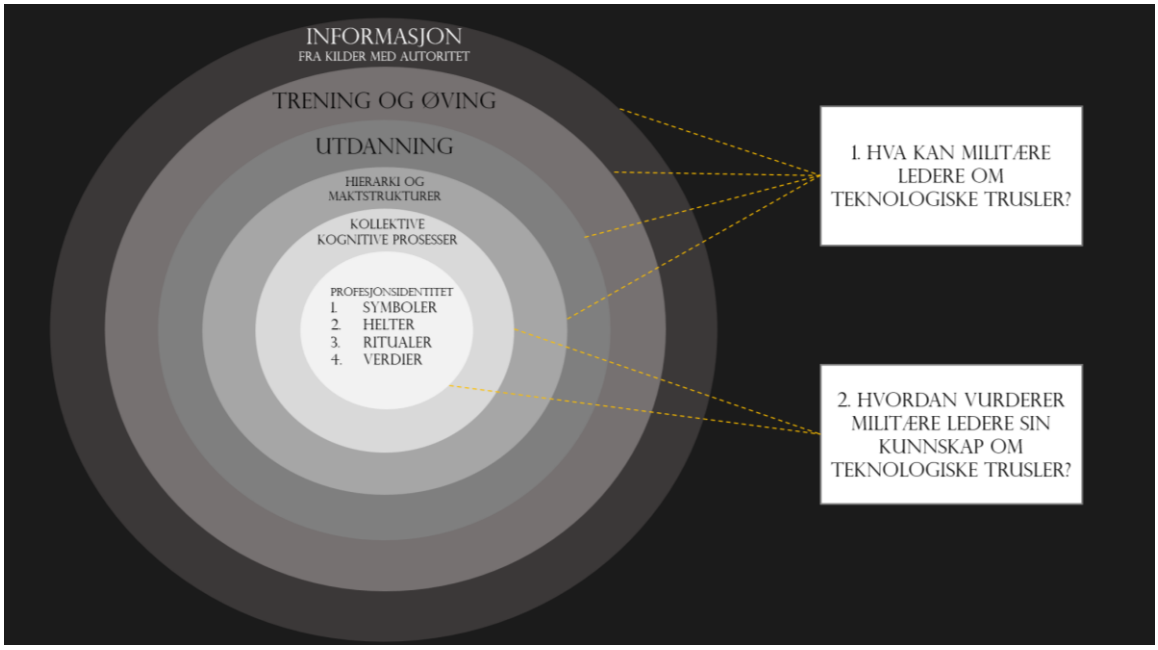
Idealer blir av Farrell og Terriff fremstilt også i boken «A Transformation Gap?» Boken omhandler utvikling og innovasjon i militære organisasjoner (Farrell og Terriff, 2010, s. 8). De hevder at hovedårsaken til at manøverkrigføringen som konsept ble akseptert av profesjonsutøverne på 1990-tallet, var at den fant klangbunn i det krigeridealet som dominerte organisasjonen (Farrell og Terriff, 2010, s. 9). Det er en åpenbar omvendt parallell til ny teknologi på stridsfeltet da mange av teknologikonseptene, og offiserenes rolle i dem, er svært fjernt fra det klassiske militære ideal, som også fremdeles lever i den norske hæren. Det vil kreve stor overbevisningskraft fra en leder i Hæren for å få avdelingen med på nye teknologiske løsninger som nedtoner kriger- og lederidealet de fleste i organisasjonen har «vokst opp» med. Ikke minst vil det kreve at lederen selv behersker slik teknologi og gjennom dette er en god ambassadør.

Offiseren med kommandomyndighet må ta beslutninger om liv og død, og evne å skape oppslutning om disse blant sine undergitte. I dette hviler det også et ansvar ved at offiseren ikke kan kommunisere usikkerhet, virke rådvill eller gi uttrykk for feil. Det er lite rom for tvilrådighet, og dermed forstås gjerne «oppfatningsutholdenhet» fremdeles som en positiv lederegenskap i Hæren. Det motsatte vil kunne oppfattes som et svakhetstegn. Urokkeligheten i oppfatninger og beslutninger virker å være helt sentralt i lederens selvbilde. Dette kan påvirke den sosiale identiteten til militære ledere, som gjør at det er utfordrende å la egne «svakheter», eller betenkeligheter skinne gjennom. På mange måter kan man hevde at dette selvbildet også utfordrer evnen til analytisk problemløsning og det å oppholde liknende «akademiske» idealer. Herunder evnen til å innta flere perspektiver, benytte metodiske formler for å utlede nye løsninger og nyansere virkeligheten. I tillegg kan dette tenkes å utfordre mer politisk orienterte idealer hvor evnen til å kjøpslå og inngå kompromisser kan være viktige. Disse egenskapene kan man imidlertid argumentere for at kun kravstilles til enkelte ledere og stabsoffiserer. Konklusjonen for hypotesen er at Hærens profesjonsidentitet, selvbilde og kognitive prosesser kan være trusler mot det å vurdere ny informasjon og nye trusler tilstrekkelig. I dette ligger det en fare for at lederen reagerer feil i et uløselig teknologisk dilemma på stridsfeltet.

4.7 Konklusjon – kulturens rolle

Hvordan kan så disse seks hypotesene henge sammen? Hypotesene som har blitt drøftet har vært knyttet til de to kjernespørsmålene – hva militære ledere kan om teknologiske trusler og hvordan de oppfatter egen kompetanse. Hypotesene har i kort omhandlet: Skjermede miljøer, lav grad av eksponering, utdanning ute av takt, hierarki og homogene grupper, kognitive prosesser og profesjonsidentitet. Hypotesene har i stort tatt for seg både et systemperspektiv og et individperspektiv – alt i rammen av *kultur*. Hypotesene konkluderes her med at militære lederes manglende evne til å forestille seg teknologisk strid best forstås gjennom linsen av organisasjonskultur (Kier, 1997, s. 28).

Organisasjonskultur kan forstås som et sett av felles normer, verdier og virkelighetsoppfatninger som utvikles i en organisasjon når medlemmene samhandler med hverandre og omgivelsene, og som kommer til uttrykk i medlemmenes handlinger og holdninger på jobben (Bang, 2013). Denne kulturen former både hva profesjonsutøverne tenker, hvilke preferanser de utvikler og hva de gjør (Kier, 1997, s. 69). Dette leder til hovedfunnet i oppgaven – at organisasjonskulturen i Hæren bidrar til at militære ledere i liten grad evner å forestille seg et teknologisk operasjonsmiljø som eksisterer i dag.



Figur 16. Forklaringsmodell for hvorfor et utvalg militære ledere kan lite om teknologisk strid og viser en tendens til å overvurdere egen kompetanse.

For å presentere forklaringer til de to spørsmålene har Hofstedes forståelse av kultur dannet grunnlaget for modellen, og den innerste ringen. Hofstede mener symboler og helter er de ytterste lagene i «løken» i hvordan kulturelle forskjeller manifisteres (for primært stater). Deretter følger ritualer, og innerst – verdier (Hofstede m. fl., 2010, s. 8). For å forstå alle lagene, har jeg imidlertid gjennom studien også lagt til flere lag.

Som fremstillingen antyder, vil det trolig være relativt enkelt å ta fatt på noen av de ytterste lagene gjennom å øke informasjonstilgang og samarbeid mellom miljøer, endre trening og rutiner eller legge inn ytterligere perspektiver i utdanningen. De tre innerste lagene vil derimot være vanskeligere og mer tidkrevende å utvikle, eller påvirke overhodet. Det vil si at dersom organisasjonen ønsker å endre militære lederes forestilling av teknologiske trusler og evne til nytenkning må sannsynligvis alle lagene i organisasjonskulturen utfordres. Dersom kun ny informasjon tilføres eller ytterligere forventningspress legges på våre offiserer og ledere vil det trolig skapes lite endring i organisasjonen. Studien ønsker med dette å kommunisere at tiltak ikke bør være rettet mot individperspektiv, men snarere - *systemperspektivet*. For å skape utvikling i Hæren, så vel som Forsvaret, anbefales det gjennom denne studien å utforme en helhetlig tilnærming til kultur med omfattende og samtidige tiltak. Dette anbefales det at Hæren gjør en egen studie for. Når krigens karakter endres må også organisasjonene være endringsvillige og nyskapende.

5 Konklusjon

Denne oppgaven har forsøkt å besvare tre forskningsspørsmål: Hvilke teknologiske kapasiteter besitter Russland i landdomenet og hva vil kjennetegne en mer teknologisk strid på landjorden? Hvilket kunnskapsnivå og forestillingsevne har et utvalg ledere i den norske hæren om en teknologisk motstander, og hva kan forklare ledernes kunnskapsnivå og forestillingsevne?

For best mulig å besvare disse spørsmålene, har oppgaven vært bygd opp rundt to hoveddeler. Den første har kartlagt og beskrevet russisk landmakt. Den har vist at moderne russisk landmakt i dag utgjør en formidabel teknologisk motstander, og at en eventuell strid på landjorden også vil være en teknologisk preget strid. Evolusjonspreget teknologisk utvikling

har medført et skifte på taktisk nivå. Viktige drivere i dette skiftet er lengre rekkevidde, mer beskyttelse, større presisjon og høyere tempo, samt nyvinninger innenfor UAV-teknologi, cyber og liknende. I sum har dette i stadig økende hastighet endret den russiske landmakten til en meget krevende motstander som evner å bruke et bredt spekter av kinetiske og ikke-kinetiske virkemidler på en integrert og helhetlig måte, slik at dette utgjør en betydelig trussel også på det taktiske nivå i en kamp på landjorden.

Oppgavens andre hoveddel har vendt blikket mot den norske hæren og lederne der, som kan risikere å møte en motstander som den russiske hær i strid. Hovedfokuset har vært en kvalitativ intervjuundersøkelse blant offiserer i den norske hæren, med utgangspunkt nettopp i mine funn knyttet til den russiske landmakten. Undersøkelsen har vist at militære ledere i Hæren har god kunnskap om teknologisk strid knyttet til kinetiske virkemidler og trusler i landdomenet. På dette området evner lederne å vurdere gyldigheten av informasjonen, tillegge ytterligere perspektiver, nyansere virkeligheten og utlede implikasjoner og tiltak i fremtiden. Med andre ord kan studien utlede at ledere i Hæren kan mye om den striden de «har kjempet før» og har trent for.

Når undersøkelsen blant lederne imidlertid tok for seg mer tekniske aspekter og ikke-kinetiske virkemidler integrert med kinetiske, kan de militære lederne lite. Samtidig er det et hovedfunn at overvekten av intervjuobjektene gjennomgående vurderer eget kunnskapsnivå høyere enn det i realiteten er. På dette området kan studien sannsynliggjøre at Hærens ledere rammes av kognitive skjevheter. Observasjonene er knyttet til en overkonfidens relatert til egen kompetanse, kognitiv lukking og letthet i møte med ny informasjon. Lederne er tilsynelatende ikke bevisste at de overvurderer seg selv, og mener generelt at de er relativt oppdaterte og kunnskapsrike om den teknologiske motstanderen. Dette leder til hovedfunnet: At et utvalg av ledere i Hæren har en begrenset forestillingsevne og forståelse når det gjelder det mer teknologisk orienterte operasjonsmiljøet der ikke-kinetiske virkemidler har en fremtredende rolle.

Oppgavens andre hoveddel gikk så over til å drøfte mulige forklaringer på dette funnet: Hva kan bidra til å forklare det relativt moderate kunnskapsnivået og respondentenes tendens til å overvurdere dette? Det sentrale og overgripende funnet i studien er at organisasjonskulturen

er den fremste årsaken til at Hærens militære ledere har en begrenset forståelse av det teknologiske operasjonsmiljøet vi i dag ser, og som vil møte norske hærstyrker ved en konfrontasjon med en motpart av den typen som den russiske hær i dag utgjør i våre nærområder. Fellestrekket ved alle de perspektivene og mulige forklaringene som er drøftet i denne delen av oppgaven, er at det er trekk ved Hærens organisasjonskultur som kan hemme de militære lederne i deres forståelse av teknologiske trusler og nytenkning. Med dette konkluderer studien med at visse elementer i Hærens organisasjonskultur utgjør et av de største hinderne for at Hæren vil møte forberedt på det teknologiske stridsfeltet.

Forkortelser

AGS	Automatisk granatutskytningssystem
APC	Armored Personnel Carrier
AT-5	Anti-Tank Missile, russisk betegnelse som Konkurs 9M113, AT-5 Spandrel i NATO
AT-9	Anti-Tank Missile, russisk betegnelse som 9M120 Ataka, mens NATO refererer til missilet som AT-9 Spiral-2
AT-11	Anti-Tank Missile, brukes som ammunisjon på T-90 stridsvogn, kalles AT-11 Sniper i NATO
AT-14	Anti-Tank Missile, Kornet eller AT-14 Spriggan i NATO
BK	Bombekaster
BMPT	Tank Support Fighting Vehicle, Ildstøttevogn primært for stridsvogn
BTG	Battalion Tactical Group, bataljonstridsgruppe på norsk
C2	Kommando og kontroll (brukt med engelsk forkortelse)
CSS	Combat Service Support, logistikkelement eller avdeling
CV-90	Norsk stormpanservogn
EK	Elektronisk krigføring
ELINT	Elektronisk etterretning
EMS	Elektromagnetisk signatur
FMV	Full Motion Video
GLONASS	Russisk globalt satelittnavigasjonssystem, *Globalnaja navigatsionnaja sputnikovaja sistema*
GM	Guided Missile
GSM	Digitalt Mobiltelefonsystem
IFV	Infantry Fighting Vehicle
IPb	Russisk informasjonskonfrontasjon, kalt informasjonsoperasjoner eller påvirkningsoperasjoner
IR	Infrarød

LEO-2	Norsk stridsvogn
LTK-S/V	Lett Terreng Kjøretæy, Sommer eller Vinter
MBT	Main Battle Tank, stridsvogn i norsk terminologi
MLRS	Multiple Launch Rocket System, fortkortelsen eller rakettartilleri brukes gjerne på norsk
MUAS	UAV underlagt enheter i hærens bataljoner
OP	Observasjonspost
PB	Panserbrytende
PGM	Precision Guided Missiles
PV	Panservern, utstyrt med anti-tank missiler/våpen
RV	Rekkevidde
SIGINT	Signaletterretning
UAV	Unmanned Aerial Vehicle
UCAV	Unmanned Combat Aerial Vehicle

Litteraturliste

Adamsky, D. & Bjerga, K. I. (2012). *Contemporary Military Innovation. Between anticipation and adaption*, ISBN-13: 978-0415523363. London & New York: Routledge

Angevine, R. (Red.), Warden, J., Keller, R., Frye, C. (2019). *Learning Lessons from the Ukraine Conflict, Document NS D-10367/Log: H 18-000503.* Alexandria, VA: The Institute for Defense Analyses

Army Recognition (2019a). *Kornet-D Tigr-M, pansret AT kjøretøy.* Hentet 13. September 2019 fra *https://www.armyrecognition.com/russia_russian_missile_system_vehicle_uk/kornet-d_anti-tank_missile_carrier_4x4_vehicle_tigr-m_gaz-233116_technical_data_sheet_pictures_video_0105153.html*

Army Recognition (2019b). *BMPT-72.* Hentet 13. September 2019 fra https://www.armyrecognition.com/72_terminator_2_tank_support_armoured_fighting_vehicle_technical_data_sheet_specifications.html

Army Recognition (2019c). *Orion-E UCAV,* Posted On Wednesday, 21 November 2018 15:00. Hentet 19. oktober 2019 fra https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/russian_kronstadt_group_details_orion-e_uav.html

Army Warfare Branch (2016). *Insights to «Training Smarter» Against a Hybrid Adversary,* Edition 1, March 2016. London: Army Warfare Branch.

AWG. (2016). *Russian New Generation Warfare Handbook,* Version 1: Dec. 2016.

Fort Meade, MD: Asymmetric Warfare Group.

Bang, H. (2013). *Organisasjonskultur – en begrepsavklaring,* 5. april 2013. Hentet 31. mars 2020 fra https://psykologtidsskriftet.no/fagartikkel/2013/04/organisasjonskultur-en-begrepsavklaring

Beadle, A. (2016). *Å forske på Forsvaret i fremtiden – muligheter, begrensninger og kognitive fallgruver, FFI-rapport 2016/01810.* Kjeller: Forsvarets Forskningsinstitutt.

Business Finland. (2019). *Digibarometri 2019.* Helsinki: The Finnish Software and E-business Association.

Business Insider. (2015). *11 Quotes that show the great leadership of General George Patton,* December 21, 2015, 7:33 pm. Hentet 26. mai 2019 fra https://www.businessinsider.com/11-quotes-that-show-the-great-leadership-of-general-george-patton-2015-11?r=US&IR=T.

Business Insider. (2018). *Here are some of the biggest reveals from a fitness-tracker data map that may have compromised top-secret US military bases around the world.* Hentet 19. januar, 2020, fra *https://www.businessinsider.com/strava-heatmap-most-revealing-images-2018-1?r=US&IR=T*

Connolly, R., og Boulègue, M. (2018). *Russia's New State Armament Programme – Implications for the Russian Armed Forces and Military Capabilites to 2027, May 2018.* London: Chatham House, The Royal Institure of International Affairs, Russia and Eurasia Programme.

Dick, C. (2019). *Russian Forces Posture Towards the West,* Research Paper, April 2019. London: Chatham House, The Royal Institure of International Affairs.

Masuhr, N. *(*2019*). Lessons of the war in Ukraine for Western Military Strategy,* nr. 242, April 2019, DOI: 10.3929/ethz-b-000335676. Zürich: Center for Security Studies, Analyses in Security Policy.

DIA. (2017). *Russia Military Power – Building a Military to Support Great Power Aspirations.* Washington: Defence Intelligence Agency.

Diesen, S. (2018). *Lavintensivt hybridangrep på Norge i en fremtidig konflikt, FFI-rapport 2018/00080.* Kjeller: Forsvarets Forskningsinstitutt.

Dyndal, G. (2019). *Et militær-teknologisk kappløpp er på gang.* Hentet 12. august, 2019, fra *https://transitmag.no/2019/01/29/et-militaer-teknologisk-kapplop-er-pa-gang/*

Elfving, J. (2020) *Russian tanks – facts and fiction. Symposium om stridskjøretøy, 28. januar 2020.* Kjeller: FFI.

OE WATCH (2018). *Foreign News & Perspectives of the Operational Environment, China Sets New Records for Aerial, Naval Drone Swarms,* Vol. 8/Utg. 7/July 2018, s. 21. Fort Levenworth, KA: US Army Training and Doctrine Command.

FFI. (2016). *Viten – teknologien Forsvaret trenger*, utg. 2, 2016. Kjeller: Forsvarets Forskningsinstitutt.

FFOD (2019). *Forsvarets Fellesoperative Doktrine.* Oslo: Forsvarets Høgskole, Forsvarets Stabsskole.

Forsvarsdepartementet. (2020). *Vilje til beredskap – evne til forsvar. Langtidsplan for forsvarssektoren* (Prop. 62 S, 2019-2020). Oslo: FD.

Forsvarets Høgskole (2020a). *Emnebeskrivelse OPS2201.* Hentet 3. februar 2020 fra https://utdanning.forsvaret.no/nb/emne/OPS2201/745.

Forsvarets Høgskole (2020b). *Emnebeskrivelse OPS4101*. Hentet 3. februar 2020 fra https://utdanning.forsvaret.no/nb/emne/OPS4101/469.

Etterretningstjenesten. (2020). *Fokus 2020. Etterretningstjenestens vurderinger av aktuelle sikkerhetsutfordringer.* Lutvann: Etterretningstjenesten.

Gerasimov, V. (2013). *The Value of Science in Prediction,* Military-Industrial Kurier, February 27, 2013. Hentet 21. oktober 2019 fra https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjD-ILckdLpAhWnyqYKHQvpAVEQFjABegQIBBAB&url=https%3A%2F%2Fjmc.msu.edu%2F50th%2Fdownload%2F21-conflict.pdf&usg=AOvVaw3RLq8p7Bs8Ri9uMesSPaLv

Grau, L. og Bartles, C. (2016). *The Russian Way of War – Force Structure, Tactics, and Modernization of the Ground Force.* Fort Levenworth, KA: Foreign Military Studies Office.

Grau, L. og Bartles, C. (2018). *The Russian Reconnaissance Fire Complex Comes of Age, May 2018.* Fort Levenworth, KA: Foreign Military Studies Office.

Grissom, A. (2006). *The future of military innovation studies.* Hentet 2. april 2020, fra https://www.tandfonline.com/doi/full/10.1080/01402390600901067 Washington: Journal of Strategic Studies.

Hofstede, G, Hofstede, J. & Minkov, M. (2010). *Cultures and Organizations. Software of the mind*, ISBN: 978-0-07-177015-6. McGraw-Hill eBooks.

Huntington, S. (1957). *The Soldier and the State:The Theory and Politics of Civil-Military Relations.* Cambridge: Harvard University Press.

InformNapalm. (2019). *Om InformNapalm.* Hentet 21. oktober 2019 fra https://informnapalm.org/no/om-oss/

Harris, C. og Kagan, F. (2018). *Russia's Military Posture – Ground Forces Order of Battle,* March 2018. Washington: Institute for the Study of War.

Hæren (2010). *OPFOR, hefte 1.* Rena: Hærens Våpenskole.

IISS (2019). *The Military Balance, Chapter Five: Russia and Eurasia,* s. 166-221. Hentet 30. oktober 2019 fra https://doi.org/10.1080/04597222.2019.1561031

Jacobsen, D. I. (2018). *Hvordan gjennomføre undersøkelser? Innføring i sammfunnsvitenskapelig metode*, 3. utg. Oslo: Cappelen Damm.

Karber, P. (2015). *«Lessons Learned» from the Russo-Ukrainian War,* Draft, 8 July, 2015. Hentet 16. januar 2020, fra *https://www.researchgate.net/publication/316122469_Karber_RUS-UKR_War_Lessons_Learned*

Karber, P. og Thibeault, J. (2016). *Russia's New Generation Warfare*, Army, June 2016, s. 60-64. Arlington, VA: The Magazine of the Association of the United States Army.

Kjellén, J. (2018). *Russian Electronic Warfare. The role of Electronic Warfare in the Russian Armed Forces*, FOI-R--4625—SE. Stockholm: Totalförsvarets forskningsinstitut.

Kofman, M. (2018). *From Hammer to Rapier: Russian Military Transformation in Perspective*, Changing Character of War Centre, Russia Brief, Issue 1, January 2018. Oxford: University of Oxford, Pembroke College.

Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., Tkacheva, O., Oberholtzer, J. (2017). *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, ISBN:978-0-8330-9606-7). Santa Monica, CA: RAND Corporation.

Kofman, M. og Rojansky, M. (2015). *A Closer Look at Russia's «Hybrid War»*, nr. 7, april 2015. Washington: Kennan Institute, Wilson Center.

Kier, E. (1997). *Imagining War – French and British Military Doctrine Between the Wars*. New Jersey: Princeton University Press.

Kroghrud, P. (2019). *Russisk cybersabotasje – forsmak på fremtidens cyberkrig*? Bergen: Universitetet i Bergen, Masteroppgave.

Lavrov, A. (2018). *Russian Military Reforms from Georgia to Syri*a, november 2018. Washington: Center for Strategic & International Studies.

McDermott, R. (2011). *Russian Perspective on Network-Centric Warfare: The Key Aim of Serdyukov's Reform*. Fort Levenworth: KA: Foreign Military Studies Office

McDermott, R. (2017). *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*, september 2017. Tallinn: International Centre for Defence and Security [ICDS].

McDermott, R. (2019). *Russian Military Introduces New Automated Command-and-Control Systems*. Hentet 19. Oktober 2019 fra

https://jamestown.org/program/russian-military-introduces-new-automated-command-and-control-systems//

Persson, G. (Red.), Hedenskog, J., Malmlöf, T., Norberg, J., Oxenstierna, S., Roffey, R., Pallin, C., Westerlund, F**. (**2016). *Rysk militär förmåga i ett tioårsperspektiv – 2016,* FOI-R—4367—SE, desember 2016. Stockholm: Totalförsvarets forskningsinstitut.

Posen, B. (1984). *The Sources of Military Doctrine: France, Brittain and Germany Between the World Wars.* Ithica & London: Cornell University Press.

PWC (2017). *Digitale bjørnestreker - Alvorlige cyberangrep og trusler mot datasikkerhet har blitt en del av et norsk trusselbilde,* oppdatert 13. februar 2017. Hentet 12. april 2020, fra https://blogg.pwc.no/styringogkontroll/digitale-bj%C3%B8rnestreker-alvorlige-cyberangrep-og-trusler-mot-datasikkerhet-har-blitt-en-del-et-norsk-trusselbilde

Radin, A., Davis, L., Geist, E., Han, E., Massicot, D., Povlock, M., Reach, C, Boston, S., Charap, S., Mackenzie, W., Migacheva, K., Johnston, T., Long, A. (2019a). *The Future of The Russian Military – Russia's Ground Combat. Capabilities and Implications for US-Russia Competition,* RAND-RR3099. Santa Monica, CA: RAND Corporation.

Radin, A., Davis, L., Geist, E., Han, E., Massicot, D., Povlock, M., Reach, C, Boston, S., Charap, S., Mackenzie, W., Migacheva, K., Johnston, T., Long, A. (2019b). *The Future of The Russian Military – Russia's Ground Combat. Capabilities and Implications for US-Russia Competition. Appendixes, RAND-RR3099.* Santa Monica, CA: RAND Corporation.

Schmuel, S. (2017). *Multi-Domain Operations: Air-Land Battle, Once More, With Feeling.* Hentet 18. mai, 2020, fra

https://warontherocks.com/2017/06/multi-domain-battle-airland-battle-once-more-with-feeling/

Seward, S. (2018). *Cyberwarfare in the Tactical Battlespace: An Intelligence's Officer's Perspective*, Infantry, april-juni 2018. Hentet 19. januar, 2020 fra https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjYwez63o_nAhUKp4sKHZr5BsQQFjAAegQIAhAB&url=https%3A%2F%2Fwww.benning.army.mil%2Finfantry%2Fmagazine%2Fissues%2F2018%2FAPR-JUN%2FPDF%2F7)Seward-Cyber.pdf&usg=AOvVaw2tLUnTykqv-UNrkKOGQEbm

Skjelland, E. (Red.), Glærum, S., Beadle, A., Endregard, M., Guttelvik, M., Hennum, A., Kvalvik, S., Køber, P, Mørkved, T., Olsen, K. E., Sendstad, C., Voldhaug, J. E., Åtland, K. (2019). *Hvordan styrke forsvaret av Norge? Et innspill til ny langtidsplan (2021-2024),* FFI-rapport 2019/00328. Kjeller: Forsvarets Forskningsinstitutt.

Slyusar, V. (2020). *Eastern Ukraine: Lessons learned from land operations in the context of armoured vehicles,* Symposium om stridskjøretøy, 28. januar 2020. Kjeller: FFI.

Statistisk Sentralbyrå (2020). *Fakta om innvandring.* Hentet 20. april 2020 fra https://www.ssb.no/innvandring-og-innvandrere/faktaside/innvandring

Store Norske Leksikon (2020). *Kognitiv psykologi.* Hentet 17. april 2020 fra https://snl.no/kognitiv_psykologi

Tashev, B., Purcell, M., McLaughlin, B.(2019). *Russia's Information Warfare. Exploring the Cognitive Dimension*, MCU Journal, Vol. 10, nr. 2, 2019s. s. 129-147. Quantico, VA: Marine Corps University Press.

Farrell, T. og Terriff, T. (2010). *A Transformation Gap? American Innovations and European Military Change.* California: Stanford Security Studies.

Thomas, T. (2019). *Russian Forecasts of Future War,* Military Review, May-June 2019, s. 84-93. Fort Levenworth, KS: The Army University Press.

TV2. (2017). *PST bekrefter: Russiske hackere har angrepet Forsvaret, UD, Ap, Statens Strålevern og PST, oppdatert 03.02.2017.* Hentet 12. april 2020 fra https://www.tv2.no/a/8903847/.

UK Parliament. (2019). *Disinformation and 'fake news': Final Report, 6 Foreign influence in political campaigns,* 18 February 2019. Hentet 11.april, 2020, fra https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179109.htm#footnote-079.

Werkheiser, E. (2020). *Ideas for the Operational Environment – Multi-Domain Operations, 11 March 2020*, forelesning om Multi-Domain i rammen av emnet Complex Operations. Oslo: Krigsskolen.

Wikipedia. (2019a). *Kurganets-25*. Hentet 13. september 2019 fra https://en.wikipedia.org/wiki/Kurganets-25

Wikipedia. (2019b). *BMPT Ildstøttevogn*. Hentet 13. september 2019 fra https://en.wikipedia.org/wiki/BMPT_Terminator

Wikipedia. (2019c). *Bumerang, K-16 og K-17*. Hentet 13. september 2019 fra https://no.wikipedia.org/wiki/VPK-7829_Bumerang

Wikipedia. (2019d). *Armata T-14*. Hentet 13. september 2019 fra https://no.wikipedia.org/wiki/T-14_Armata

Wikipedia. (2019, e). *BMP-2 og 3.* Hentet 13. september 2019 fra

https://no.wikipedia.org/wiki/BMP-3

Wikipedia. (2019f). *BTR-80.* Hentet 13. september 2019 fra https://no.wikipedia.org/wiki/BTR-80

Wikipedia. (2019g). *Armata T-15.* Hentet 13. september 2019 fra https://no.wikipedia.org/wiki/T-15_Armata

Wikipedia. (2019h). *9M120 Ataka AT-9.* Hentet 13. september 2019 fra *https://en.wikipedia.org/wiki/9M120_Ataka*

Wikipedia. (2019i). *T-72*. Hentet 13. september 2019 fra https://no.wikipedia.org/wiki/T-72

Wikipedia. (2019j). *T-80BVM.* Hentet 13. september 2019 fra https://en.wikipedia.org/wiki/T-80

Wikipedia. (2019k).*T-90M.* Hentet 13. september 2019 fra https://en.wikipedia.org/wiki/T-90

Wikipedia. (2019l). *9M119 Svir, 9M119M Refleks*. Hentet 13. september 2019 fra https://en.wikipedia.org/wiki/9M119_Svir/Refleks

Wikipedia. (2019m). Koalitsiia-SV. Hentet 13. september 2019 fra https://en.wikipedia.org/wiki/2S35_Koalitsiya-SV

Wikipedia. (2019n). *Okhotnik-B.* Hentet 19. oktober 2019 fra https://en.wikipedia.org/wiki/Sukhoi_S-70_Okhotnik-B

Wikipedia. (2019o). *Mikoyan Skat.* Hentet 19. oktober 2019 fra

https://en.wikipedia.org/wiki/Mikoyan_Skat

Wikipedia. (2019p). *R-168 Akveduk.* Hentet 19. oktober 2019 fra https://nn.wikipedia.org/wiki/R-168_Akveduk

Wikipedia. (2019q). *Panserbataljonen.* Hentet 7. desember 2019 fra https://no.wikipedia.org/wiki/Panserbataljonen

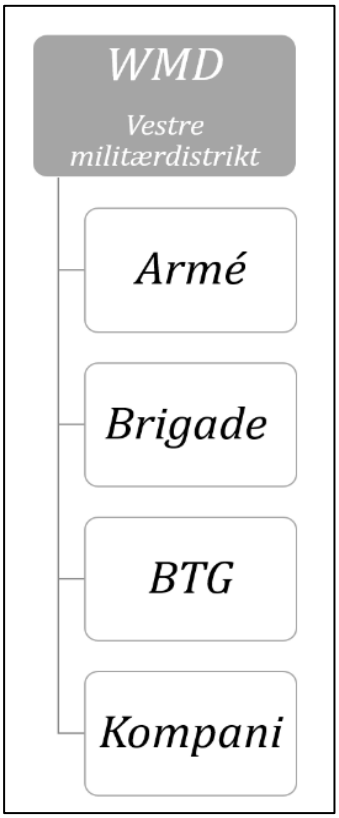
Wikipedia. (2019r). *Telemark bataljon.* Hentet 7. desember 2019 fra https://no.wikipedia.org/wiki/Telemark_bataljon

Wikipedia. (2019s). *Orlan-10.* Hentet 13. september 2019 fra https://no.wikipedia.org/wiki/Orlan-10

Wikipedia. **(**2020a). *Stridsvognsbevæpning*. Hentet 24. mai 2020 fra https://no.wikipedia.org/wiki/Stridsvognsbev%C3%A6pning

Wikipedia. **(**2020b). *Pilammunisjon*. Hentet 24. mai 2020 fra https://no.wikipedia.org/wiki/Pilammunisjon

Vedlegg 1 – Et kompani i en russisk BTG



Figur 1.

Det vestre militærdistriktet spenner seg fra Ukraina i sør, gjennom de baltiske statene, Finland og Norge i nord (Persson et. al., 2016, s. 79). Kjernen av militærdistriktet utgjøres av 1. stridsvognsarmé, 20. armé, 6. armé, styrker fra det 11. armékorps i Kaliningrad, samt styrker stasjonert i Moldova i form av et fredsbevaringsoppdrag[1] (Harris og Kagan, 2018, s. 12). Ugrupperingen av av russiske styrker var i 2018; Tre motoriserte infanteribrigader, ett motorisert infanteriregiment og tre luftbårne regimenter i nærheten av de baltiske statene. I tillegg til nærvær av luftbårne styrker, er det også en betydelig tilstedeværelse av Spetsnaz i tilknytning til 20. armé (Harris og Kagan, 2018, s. 14). Det vestre militærdistriktet er med sin nærhet til Moskva og randstatene i vest et prioritert distrikt. Dette kan underbygges av både bemanning av personell, antall enheter og materiellet som finnes i avdelingene (Persson et. al., 2016, s. 79).

Russisk BTG er en forsterket bataljonsstridsgruppe satt opp med enten motoriserte eller mekaniserte styrker (DIA, 2017, s. 52). Bataljonstridssgruppene skal i stor grad være selvforsynte for operasjoner av kortere varighet, og den foretrukne organiseringen der Russland har vært i ulike former for væpnede kamper. Dette vil si at bataljonstridsgruppen har eksempelvis har egen BK enhet, artilleri, motorisert PV tropp og logistikkelement. Derfor er BTGen et godt rammeverk for å forstå et teknologisk konvensjonelt kompani (Harris og Kagan, 2018, s 14).

En BTG består så av fire kompanier med kampenheter. Det ene kompaniet som studien tar utgangspunkt er organisert med fire tropper, hvorav tre tropper er oppsatt med BMP-2 og 3, og én tropp er kryssunderlagt med stridsvogn, i kombinasjoner av primært T-72B3/T-72B3 obr 2016 og T-90A/M (Grau og Bartles, 2016, s- 119; DIA, 2018, s. 51; Radin et. al., 2019a,

s. 70). Det vil si at kompaniet disponerer både motoriserte kampenheter og stridsvogner i det samme kompaniet. Støtteressurser vil organisk tilhøre bataljonsnivået ett nivå opp, mens det for studiens del illustreres sammen med kompaniet for å forstå kompleksitet og samvirke på lavere nivå. Eksempelvis vil de luftbårne troppene [VDV] og Spetsnaz føres kommando over av henholdsvis luftstyrkene og spesialstyrkekomponenten. Ressurser som; VDV, motoriserte panservernvåpen, elektronisk krigføringstropp, UAV tropp, skarpskyttertropp og Spetsnaz har vært helt essensielle for Russlands operasjoner i Georgia, på Krim, i Ukraina og Syria. Da spesielt dokumentert fra kampene i Donbassregionen i Ukraina og Syria (AWG, 2016, s. 21; Lavrov, 2018, s. 8; DIA, 2018, s. 13).

I en tenkt situasjon hvor alle eller deler av ressursene vil virke, vil kompaniet være *Main Effort* i BTGen. Dette vil si at kompaniet løser *det* viktigste, eller et av de viktigste oppdragene i bataljonen, som gjør at ressursene blir underlagt eller at kompaniet har prioritet på deres støtte innenfor et gitt tidsrom. En annen grunnforståelse er at de russiske landstyrkene analyseres ut fra å være en aggressor eller angripende part. Analysen tar utgangspunkt i et Finnmarksscenario lagt til grunn av FFI, men geografiske forhold vil ikke stå som sentrale for dette kapittelet. For å forestille seg hvordan det teknologiske stridsfeltet kan se ut, er denne forståelsen sentral.

Vedlegg 2 – Presentasjon av rammer for intervju og funn i kapittel 2

Figur 1. Skjelland et. al., 2019, s. 16, fra «Hvordan styrke forsvaret av Norge? Et innspill til ny langtidsplan (2021-2024)», FFI-rapport 2019/00328.

Geografiske forhold og norsk ambisjon

Under arbeidet med Forsvarssjefens fagmilitære råd i 2014/2015 og Landmaktutredningen i 2016/2017 ble det viet betydelig tid og ressurser til analyser, krigsspill og simuleringer av to handlemåter mot et strategisk overfall. Den ene handlemåten tok utgangspunkt i operasjonell nektelse (beskrevet ovenfor), og den andre søkte å realisere et framskutt forsvar av Finnmark – en kontrollambisjon:

Kontroll i Finnmark: *Her er ambisjonen å forsvare og holde Finnmark med egne styrker inntil allierte forsterkninger kommer Norge til unnsetning. Dette gjøres med tunge, mekaniserte landstyrker som gjennom oppholdende strid og deretter en stansoperasjon, søker å holde kontroll over hele eller deler av Finnmark.*

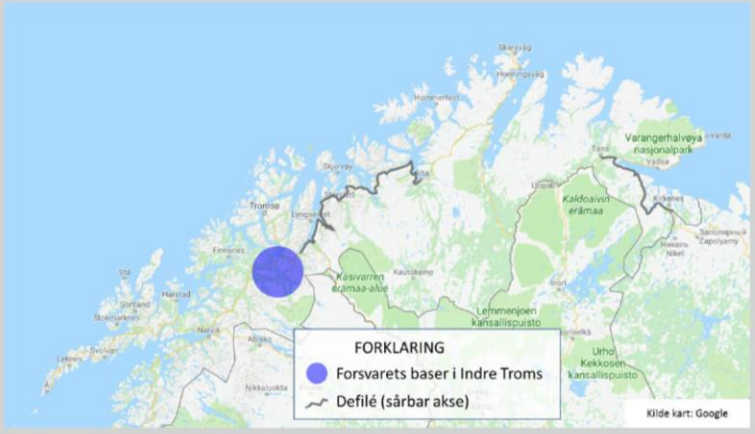
Figur 2. Skjelland et. al., 2019, s. 48-50, fra «Hvordan styrke forsvaret av Norge? Et innspill til ny langtidsplan (2021-2024)», FFI-rapport 2019/00328.

Boks 5.1 – Geografien

En aktør som skal gjennomføre militære operasjoner i Finnmark, må ta hensyn til to ulike defiléer[119], markert i kartet under. I vest finner vi *Lyngendefiléet*, som er betegnelsen vi benytter for veistrekningen fra Indre Troms gjennom Lyngenområdet og til Alta. I øst har vi veistrekningen fra grensen mot Russland til Tana bru.

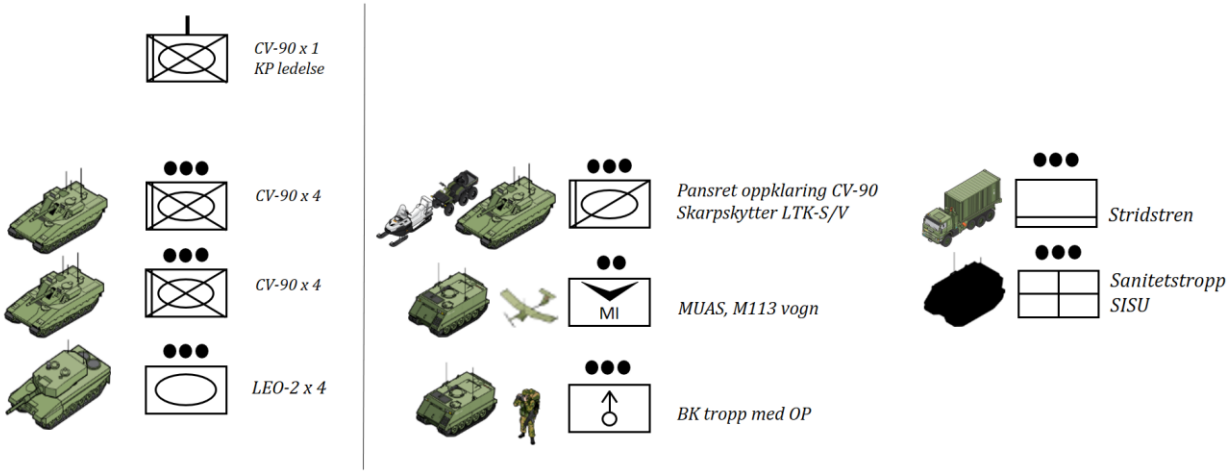
For en aktør som er avhengig av å fremføre forsterkninger eller forsyninger langs vei til Finnmark, kan disse defiléene utgjøre en sårbarhet. Samtidig kan de benyttes til forsvarsformål for en aktør som ønsker å kontrollere og forsvare Finnmark.

Den norske handlemåten i den innledende fasen av et strategisk overfallsscenario, som ble beskrevet i boks 3.1 (kapittel 3), innebærer blant annet at landstyrkene oppretter en robust terskel i Lyngenområdet. Alternative konseptuelle løsninger vil utnytte geografien i Finnmark på ulike måter, og dette kommer vi tilbake til i kapittel 6.



Kilder:
1) *Wikipedia, 2019q, Panserbataljonen*
2) *Wikipedia, 2019r, Telemark bataljon*

Norsk mekanisert kompani – generisk organisering med støtteressurser



Kapasitetsområde 1 – Utviklingstrekk ved russiske kampvogner

Utvikling av russiske stridsvogner:
- *Bedre pansring, mer aktiv og passiv pansring*
- *Kanoner som kan avfyre både HEAT, AFPDS ammunisjon og missiler*
- *Grovere kaliber (Armata, 152 mm)*
- *Bedre optikk, skyttersystemer, termisk og IR*
- *Lang rekkevidde på kanon og missilsystemer*
- *Nattsikte (T-90A, T-72 obr 2016)*
- *Oppdaterte C2 systemer med evne til å utveksle måldata med artilleriet (Strelets)*
- *Automatiske ladesystemer*
- *Ubemannede tårnsystemer*
- *UAV på stridsvogn med 10 km rekkevidde (Armata)*
- *Lavere signatur med utforming og kamuflasjemaling*

Svakheter per 2020:
- *Lite moderne sikte for vognkommandør på majoriteten av vognene*
- *Oppbygning av vognen gir dårligere odds for overlevelse ved et treff (endret til Armata-skroget)*
- *APFSDS prosjektilet er antatt dårligere enn tilsvarende vestlig prosjektil*
- *Dårligere treningsstandard eller utnyttelse av systemene enn vestlige (?)*
- *Armata er tiltenkt å bli lettere, men foreløpig kan tyngre plattformer tenkes å redusere mobilitet til en viss grad*

Generelle utviklingstrekk:
- *Opererer oftere i en kombinasjon av kompletterende vogner, både innad i stridsvognsformasjoner, men også kombinert med andre kampvogner (APC, IFV og ildstøttevogner)*
- *T-90M og nyere kampvogner vil ha høy evne til overlevelse på stridsfelt (erfaringer fra Ukraina)*
- *Grovere kaliber 125 til 152 mm kanon*
- *Kanoner som kan avfyre ulike typer ammunisjon*
- *Bedre pansring på vogner mot artilleriild, IEDer og missiler*
- *Bedre kommunikasjonssystemer som understøtter hurtig utveksling av informasjon med andre systemer, som UAV'er og artilleri*
- *Informasjonsutveksling med tropper i forterrenget, som Spetsnaz, VDV og skarpskyttere*
- *UAV direkte underlagt enkelte vogner*

To prinsipper synes å stå sentralt i utviklingen av russiske kampvogner, nemlig: Beskyttelse og ildkraft.
Disse faktorene bidrar til at kampvognene oppnår beskyttelse ved at de kan oppklare og forme fienden med mer presis ild før de iverksetter manøveren, og utnytte systemer de har overlegen kapasitet og kvantitet på. De oppnår lengre rekkevidde og beskyttelse igjen ved å kombinere tropper med ildstøttevogner med missiler, hvilket bidrar til muligheten til å engasjere fienden med både artilleri og missiler før han kommer innenfor engasjementsavstand. Grovere kaliber og større bruksområde for kanonen bidrar også til større effekt for hovedsystemene.

Personellreformene etter 2008, bruk av profesjonelle soldater, mer trening og øvelser, samt kamperfaring fra Syria blant de fleste aktuelle enheter bidrar også til at treningsstandarden kan forventes å tilsvare eller være nært opptil vestlig nivå i WMD (vestlige militærdistrikt). Fire Control systemene og automatiserte prosesser i tårnet fasiliterer for å hurtig kunne engasjere mål. Med utvikling som foregår av automatisert måloppdagelse (AI) vil også treningsnivået på et vogncrew i et 5-10 års perspektiv kunne viskes ut mellom russiske styrker og en motstander.

Det er færre vogner i den russiske hæren sammenlignet med Sovjettiden, og eksempelvis om lag 3000 aktive stridsvogner i organisasjonen. 1498 av disse blir attribuert til det vestlige militærdistrikt. Selv om ikke alle disse vognene ville ha kommet i spill ved en væpnet konflikt, representerer dette en komparativ kvantitetsmessig overlegenhet med en norsk organisasjon.

Utviklingen av Armata har medført at anskaffelsen er svært kostbar, og man estimerer derfor at antallet vogner vil bli lavt. Imidlertid ser man at ut av kampvognprosjektet kommer det nyvinninger og tekniske løsninger som andre plattformer blir oppdatert med, hvilket bidrar til rimelige oppdateringer.

Kapasitetsområde 2 – Utviklingstrekk ved russisk indirekte ild

Generelle utviklingstrekk:

- *I Øst-Ukraina ser man mellom 2014 til og med 2017 at artilleritroppene står for opptil 75% av alle tapene i konflikten, da spesielt knyttet til MLRS*
  - *På tross av at dette ikke kan overføres totalt til andre forhold og geografi, kan dette være med på å danne et bilde av det teknologiske stridsfeltet*
- *Overlegenhet gjennom kvantiteten opprettholdes i stor grad som fra Sovjettiden, men flere systemer med komplementære effekter får et tettere samvirke*
- *Større kaliber (240-300 mm) gjør at artilleri kan langt på vei få tilsvarende effekter som ved bruk av flybomber*
- *Både artilleri og MLRS blir raskere å operere og relokalisere for å unngå kontrabeskytning av motstanderens artilleri (selv om mye av artilleriet i Ukraina eksempelvis blir tatt ut av artilleri, mens BM-21 Grad MLRS ikke er ett av de nyeste og raskeste systemene)*
- *MLRS har lang rekkevidde på systemene, hvilket medfører at en motstander med begrenset rekkevidde eller ammunisjon vil kunne forbekjempes og formes før man kan engasjere selv med artilleri (hvilket fordrer samvirke med andre systemer i et fellesoperativt perspektiv)*
- *Tiden til målfatning har blitt kraftig redusert de siste 6 årene, på bakgrunn av effektorene har blitt tettere bundet sammen med sensorene, som: UAV'er, eliteinfanteri og EK i forterrenget*
- *Koblingen opp mot flere sensorer bidrar til at ilden blir mer presis, og at dyrere presisjonsammunisjon kan brukes til mer høyverdige mål*
- *På bakgrunn av at Russland ikke forholder seg til konvensjoner på samme måte som vestlige allierte, muliggjøres bruken av flere typer ammunisjon med mindre human karakter*
  - *Dette muliggjør også en kortere beslutningsprosess knyttet til hvilke mål som skal engasjeres og hvordan, og gjør at målfatningsmodellen blir preget av tempo*

I utviklingen av indirekte ild kan tilsynelatende ildkraft, interoperabilitet og mobilitet virke å stå sentralt. Mengden systemer bærer likhetstrekk fra Sovjettiden, som i seg selv representerer en betydelig trussel og en potensielt demoraliserende effekt for en motstander. Teknologien står her for et betydelig skifte i prosedyrer fordi den legger til rette for et samvirke mellom sensorer og effektorer med et høyt tempo.

Kapasitetsområde 3 – Utviklingstrekk ved russiske UAVer

Generelle utviklingstrekk:

- *Bruken av UAV'er har økt kraftig siden Georgia konflikten i 2008, og i dag finnes det eksempelvis 13-14 systemer i bruk og til uttesting i Øst-Ukraina*
- *Targetingprosessen ved bruk av UAV'er er redusert til 10-15 minutter*
- *UAVene er utstyrt med både rekognoserings- og oppklaringsfunksjoner med bilde og videokapasitet, lysforsterkersett og termiske kameraer, men også elektronisk krigføringskapasitet*
- *Flere typer UAV'er er kjent for å operere i nettverk eller sverm, der de flyr i ulike høydesjikt med ulike funksjoner, hvilket sørger for presis målfatning og redundans på systemene*
- *Billigere UAV teknologi gjør at man kan anskaffe mange systemer, og også at hyllesystemer er vanskeligere å attribuere til én bestemt aktør for en tidsperiode*
- *UAV'er med lastekapasitet til bomber og kamikaze-UAV'er med lav signatur gjør at statiske installasjoner, depoter og bakre områder også kan bli mer utsatt for angrep*
- *Nettverk, båndbredde og målfatningssystem gjør at UAV'er har blitt svært betydningsfulle på det teknologiske stridsfeltet*

Komplementære UAV systemer på stridsfeltet skaper en ny dynamikk, som tidligere har vært forbeholdt de teknologisk overlegne militærmaktene. UAV'er øker effekten av ildkraften, og samtidig beskyttelse for hovedsystemene og utvikler evnen til å oppklare og innhente etterretning. Med UAV'er som innehar evnen til å jamme eller drive signaletterretning, øker også trusselen, både kinetisk og ikke-kinetisk.

Kapasitetsområde 4 – Utviklingstrekk ved russisk eliteinfanteri og proxykrigere

Generelle utviklingstrekk:

- *Bruken av styrker som opererer fordekt og under terskelen for væpnet konflikt er en godt dokumentert operasjonsprosedyre siden 2014*
- *Bruken av Spetsnaz, VDV og skarpskyttere i større enheter på dypet kan utnyttes i større grad på grunn av kommunikasjons- og nettverksstruktur som muliggjør hurtig utveksling av informasjon i sanntid (Strelets)*
- *Eliteinfanteri kan koblet med UAV'er bidra til å redusere tiden til motstanderens enheter blir engasjert av artilleri (spesielt koblet mot BM-21 Grad MLRS)*
- *VDV og Spetsnaz har blitt utstyrt med mer mobile EK innretninger, hvilket muliggjør fordekt og lokal jamming av signaler, samt signaletterretning i forterrenget*
- *Kompletterende styrker med avansert samband og nettverk bidrar trolig til større redundans på denne type oppklaringskapasitet*
- *Spetsnaz vil vokse til 100% av sin størrelse, og VDV med 60%, hvilket synliggjør et økende behov for rask deployerbart, mobilt og godt trening infanteri*

Utviklingen av mobilt eliteinfanteri preges av prinsippene for mobilitet, etterretning og beskyttelse for hovedsystemene i kampavdelingene. Et viktig skifte fra tidligere er at Spetsnaz, VDV og skarpskyttere har Strelets systemet og kan drive målfatning direkte med artilleritroppene. Med utviklingen av sambandssystemer og teknologi, vil trolig dette eliteinfanteriet kunne virke tettere integrert med også kampavdelingene og således oppnå større synergieffekter. Uten interoperabilitet og integrasjon av systemer, ville trolig eliteinfanteriet ha en forstyrrende effekt på en motstander, men med tettere og bedre synkronisert samvirke kan man forvente mer presis og tidsriktig bruk av artilleri og missiler på stridsfeltet. Antallet og graden av kompletterende styrker vil også kunne få en demoraliserende effekt på en motstander, da disse av natur vil søke å overraske en fiende og skape et fortrinn på stridsfeltet.

Utviklingsområde 5 – Utviklingstrekk ved russisk EK

Generelle utviklingstrekk:

- *EK har historisk vært et kapasitetsområde hvor Russland har investert mye for å møte vestens overlegne teknologiske makt og sårbarheter, og dette har tilsynelatende vedvart*
- *Landstridskreftene har om lag 14 systemer for å drive EK på det taktiske nivået, i tillegg til 10 systemer som har vært til testing og utprøving siden 2013*
- *Systemene er primært rettet inn mot å beskytte egne systemer og dominans i det elektromagnetiske rommet, og er ikke så offensivt rettet som man ofte kan få inntrykket av i vesten*
- *EK opererer ikke bare som adskilte systemer, men man ser mer integrasjon og lettere systemer i flere enheter forbeholdt bakkestyrkene, som:*
    - *Jammesystem på kampvogner for å detonere nærhetsbrannrør fra artilleri for tidlig*
    - *Jammesystem og signaletterretning hos eliteinfanteri*
    - *Jammesystemer og signaletterretning på vogner og hjulgående kjøretøy*
    - *Jamming og innhentingskapasitet i UAV'er*
- *Evnen til å slå ut GPS, GSM, sambandssystemer og kunne mate inn feil informasjon i systemer (spoofing etc.) påvirker en motstander på måter som gjør at man ikke nødvendigvis kan feste lit til teknologi på samme måte som ved operasjonsområder der man har dominans i det elektromagnetiske spektrum*

Elektronisk krigføring er et middel for å møte vestens tradisjonelle teknologiske overtak, men også sårbarhet, og vil trolig vedvare i fremtiden. Dette vil bidra til å øke støyen og friksjonen på stridsfeltet, og hindre en part i å etablere full situasjonsforståelse. Dette vil påvirke operasjonsmiljøet i stor grad, og fordrer en god forståelse for de taktiske styrkene av hva signatur er og hvordan dette har innvirkning på striden.

Utviklingsområde 6 – Utviklingstrekk ved russisk informasjonskonfrontasjon og cyber

Generelle utviklingstrekk på taktisk nivå:

- *En tettere samordning av aktivitetene som foregår under informasjonskonfrontasjon (IPb)*
- *Mer nettbasert aktivitet skaper sårbarheter og gjør det lettere å finne informasjon som kan diskreditere viktig personell eller frata ledere legitimitet i deres roller*
- *Jamming, signaletterretning og cyber i nettverk gjør at GSM og sekundærsamband er svært enkelt å identifisere og sende meldinger tilbake til*
    - *Under strid kan dette ha en svært demoraliserende effekt (på tross av at GSM og smarttelefoner i stort er forbudt i operasjoner)*
- *Imiterte meldinger til eller fra nær familie kan bidra til å demoralisere militær personell på taktisk nivå*
- *Digitale fotavtrykk er økende, som kan avgi informasjon om svakheter i forsvarssystemet*
- *Feil informasjon kan mates inn i systemene som monitorerer stridsfeltet, og på den måten redusere tempoet i operasjoner og øke kontrollbehovet for taktiske sjefer*

Fra 2014 kan man spore en tiltakende vilje og evne til å målrettet angripe enkeltpersoner og nær familie i militærmakten, med imiterte tekstmeldinger, truende meldinger eller meldinger direkte til personell på bakken etter de har blitt utsatt for artilleriangrep. Ledere har også blitt utsatt for hacking og innhenting av kompromitterende informasjon som kan svekke deres legitimitet . Effekten av informasjonskonfrontasjon på det taktiske nivået har et potensial for å øke i fremtiden.

Utviklingsområde 7 – Utviklingstrekk ved russisk kommando, kontroll og interoperabilitet

Generelle utviklingstrekk:

- *Mange av kapasitetsområdene i studien bærer isolert sett ikke preg av revolusjonerende teknologi, brytningsteknologi eller har kommet dithen at kunstig intelligens eller robotmekanikk har overtatt noen vesentlig rolle på det teknologiske stridsfeltet*
    - *Brytningen representeres først og fremst gjennom kommunikasjonsteknologi og nettverksstruktur som tillater den russiske hæren å operere med et omforent situasjonsbilde distribuert i sanntid – en nettverkssentrisk tilnærming*
    - *Fordeler som tidligere vestlige allierte var i besittelse av har også innhentet andre stater i det teknologi har blitt billigere og mer allmenn*
- *Den russiske hæren er nære ved å ha etablert en nettverkssentrisk struktur, og således kvalitetsmessig nær paritet med en konvensjonell militærmakt i Vesten*
- *Strelets, systemet som kan utveksle måldata i sanntid i mellom spetsnaz, VDV, hæren og luftforsvaret kan til dels overgå integreringen av ulike plattformer, komparativt med en vestlig styrke*
- *Det siste tiårets satsing og budsjetter til C4ISR har gitt resultater, hvilket medfører at den russiske hæren også vil korte inn sin beslutnings- og handlingssyklus på det teknologiske stridsfeltet*
    - *Per i dag er det spesielt sammenknytningen av UAV'er og menneskelige sensorer på dypet med effektorer som indirekte ild som utgjør et spesielt skifte i operasjonsprosedyrer og tempo på stridsfeltet*

Vedlegg 3 – Utvalg av intervjuobjekter

Utvalg av intervjuobjekter

Utvalgskriterier

Det er valgt ut seks intervjuobjekter til denne studien. Alle intervjuobjektene skal ha gjennomført Krigsskolen, med unntak av ett intervjuobjekt. Hensikten er å kunne kartlegge og analysere funn hos et utvalg militære ledere i Hæren med kommandomyndighet. Altså, offiserer og ledere i Hæren. Utvalget for studien er trukket ut på bakgrunn av en personellsammensetning mellom primært troppsjefs- og kompanisjefsnivået. I tillegg vil ett av intervjuobjektene representere kadettmassen, før vedkommende blir troppsjef i Hæren. Intervjuobjektene er representative for flere tjenestesteder i den norske hæren, fra avdelinger i nord til avdelinger i sør. Aldersspennet varierer fra 22 til 37 år. Det er ikke kjønnsbalanse i studien, med bare ett kvinnelig intervjuobjekt. Uavhengig av dette ble det forsøkt å inkludere flere kvinnelige ledere, uten hell. Studien er anonymisert, og derfor vil opplysninger om intervjuobjektene begrenses.

Oversikt intervjuobjekter

A1: Intervjuobjektet er kadett ved Krigsskolen og har tidligere gjennomført sin førstegangstjeneste i HMKG, Garden. Vedkommende har med dette bakgrunn fra troppearten infanteri.

A2: Intervjuobjektet har gjennomført troppsjefstjeneste, vært nestkommanderende i et «kompani» og gjennomført stabstjeneste i en bataljon. Vedkommende har erfaring fra troppearten artilleri.

A3: Intervjuobjektet har gjennomført troppsjefstjeneste, vært nestkommanderende i et kompani og gjennomfører stabstjeneste. Vedkommende har bakgrunn fra troppearten infanteri. Intervjuobjektet har vært deployert til utenlandstjeneste flere kontingenter.

A4: Intervjuobjektet har gjennomført troppsjefstjeneste. Vedkommende har erfaring fra artilleri og patruljetjeneste.

A5: Intervjuobjektet gjennomfører sine pliktår etter Krigsskolen, som troppsjef. Vedkommende har erfaring fra infanteri og jegertjeneste.

A6: Intervjuobjektet tjenestegjør som kompanisjef. Vedkommende har erfaring også fra stabstjeneste og utenlandstjeneste i flere omganger. A6 har bakgrunn fra infanteri og patruljetjeneste.

Vedlegg 4 – Informasjonsskriv

Vil du delta i forskningsprosjektet

«Hvordan rustes militære ledere til å møte på det teknologiske stridsfeltet?»

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke hvordan militære ledere er i stand til å møte en teknologisk aktør i fremtidens landstrid. I dette skrivet gir jeg deg informasjon om målet for prosjektet og hva deltakelse vil innebære for deg.

Formål
Formålet med studien er å undersøke hvordan teknologi og nye trusler former hvordan militære ledere tenker og planlegger. Basert på hvordan Hæren har operert de siste 10 årene i både Afghanistan og Irak, har norske offiserer møtt kapasitetsmessig underlegne fiender. Dette vil trolig ikke være realiteten om kun kort tid. Teknologi blir mer tilgjengelig, billigere og mer anvendelig. Er dagens militære ledere mentalt rustet for å møte en teknologisk aktør. Et taktisk scenario vil være med på å gi svar på hvordan militære ledere i form av planleggingsprosesser tar hensyn til denne typen aktør. Deretter vil dybdeintervjuer i Hærens ledelse undersøke om dette gir de samme indikasjonene elelr svarene.

Innledningsvis vil masteroppgaven svare på hvordan en teknologisk motstander vil se ut, både kapasitetsmessig, men også i form av taktikk og prosedyrer. Deretter vil et scenario legges til grunn med påfølgende intervjuer med et utvalg av 4-5 personer for å svare på hvordan denne fienden tas høyde for i operasjonsplanleggingen. Avslutningsvis vil det gjennomføres dybdeintervjuer med personell i Hærens ledelse for å undersøke hvordan utdanningen tilrettelegger for å utvikle ledere til å møte teknologiske aktører.

Opplysningene som hentes inn vil kun nyttes til dette formålet, og vil etter innlevering avsluttende studie bli slettet. I masteroppgaven vil alt personell anonymiseres.

Hvem er ansvarlig for forskningsprosjektet?
Masteroppgaven skrives som en del av master deltidsstudiet ved Forsvarets Høgskole. Undertegnede, Rine Veberg er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
Utvalg 1 er trukket ut på bakgrunn av en personellsammensetning mellom troppsjefs- og kompanisjefsnivået. Minst 1 vil tjenestegjøre som troppsjef, minst 1 har gjennomført Stabsskolen og 1 avtjener eller har avtjent kompanisjefstjeneste. Alle har gjennomført Hærens Krigsskole. 4-5 personer vil benyttes for å svare på et scenario hvor en teknologisk aktør fremstilles, og en del av plan- og beslutningsprosessen brukes som verktøy for å analysere fienden og en taktisk løsning.

Hva innebærer det for deg å delta?
Det vil gjennomføres individuelle semi-strukturerte intervjuer for begge utvalg. Det vil benyttes båndopptaker for å få med alle taktiske detaljer, uttrykk og ordvalg. Intervjuet vil foregå på arbeidsplassen til den enkelte, eller ved Krigsskolen. Koordinering vil foregå primært på mail og tekstmelding. Tekstmelding og telefon vil benyttes nærmere tidspunktet for møtet. Samtykket må signeres elektronisk før/i forbindelse med møtet for å delta i studien.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykke tilbake uten å oppgi noen grunn. Alle opplysninger om deg vil da bli anonymisert. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Det er kun undertegnede og veileder som har tilgang til opplysningene som blir gitt
- Informasjonen i masteroppgaven vil bli anonymisert
- Alt datamateriale vil lagres personlig ugradert PC, som tilhører Forsvaret
- Datamaterialet vil slettes etter sensur av masteroppgaven

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Prosjektet skal etter planen avsluttes i løpet av mai 2020. Datamaterialet med personellopplysningene vil da slettes.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg,
- få utlevert en kopi av dine personopplysninger (dataportabilitet), og
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

Med vennlig hilsen

Rine Veberg

Vedlegg 5 – Samtykkeerklæring

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet «*Teknologi og nye trusler*» og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i et intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, juni 2020.

_____

(Signert av prosjektdeltaker, sted, dato)

Vedlegg 6 – Intervjuguide

Intervjuguide – Utvalg 1

«Hvordan rustes militære ledere til å møte på det teknologiske stridsfeltet?»

Introduksjon til intervju

Oppgaven har innledningsvis kartlagt en relevant teknologisk motstander og mulige implikasjoner dette kan få. Deretter gjennomføres intervjuer med ledere på det taktiske\ nivået for å undersøke militære lederes forestillingsevne rundt det neste teknologiske stridsfeltet. Du er valgt ut fordi du har ekspertkompetanse innenfor landdomenet og er utdannet eller i ferd med å bli utdannet ved Krigsskolen eller Stabsskolen. Utvalget er representativt hva gjelder kjønn, erfaring og tjenestested. Intervjuet er delt i 3 deler, hvor den første delen tar for seg generelle spørsmål om kunnskap og kompetanse. Del 2 er mer spesifikk på motstanderens kapabiliteter, og retter spørsmål for vurdering og analyse mot lederen. Spørsmål 3 er en kort avslutning rettet mot en oppsummering eller ytterligere kommentarer.

Intervjuguide

Del 1

Spørsmål 1
Hvor viktig opplever du at det har vært for deg å forstå det teknologiske stridsfeltet?

Spørsmål 2
Hvor oppdatert er du på hvordan det teknologiske stridsfeltet ser ut eller vil virke inn på det taktiske nivået?

Spørsmål 3
Hvem bærer ansvaret for å holde personellet oppdatert?

Spørsmål 4
Hvor henter du informasjon eller hvilke kilder bruker du for å øke din forståelse av operasjonsmiljøet generelt?

Spørsmål 5
Opplever du operasjonsspesifikk informasjon tilstrekkelig til å holde seg oppdatert på en teknologisk motstander?

Spørsmål 6
Dersom du vil trekke frem kapasiteter eller utviklingsområder som representerer trusler for moderne militærmakter i dag, hva ville du vektlegge?

Del 2

Kapittel 2 i oppgaven kan oppsummeres i disse vedleggene. Analysen leder til 7 kapasitetsområder hvor Russland har gjort tiltak for å oppnå utvikling og en mer nettverkssentrisk organisasjon, som representerer et skifte fra hvordan vi eksempelvis har operert mot aktører i Afghanistan og Irak. Du vil nå få 15 minutter til å få oversikt over disse funnene, samt en generisk norsk bataljon med støtteressurser. Deretter vil du kunne bruke FFIs Finnmarksscenario for å sette dette i en geografisk kontekst. Videre vil du få spørsmål innenfor de 7 kategoriene, eller kapasitetsområdene hvor du vil kunne vurdere relativ kampkraft mellom russisk og norsk organisasjon. Med en gitt motstander, hvilke prinsipper ville du eksempelvis vektlagt som forsvarer og taktisk sjef for din enhet.

Spørsmål 1
Med bedre beskyttelsessystemer, som aktiv og passiv pansring på stridsvogner og mekaniserte vogner, hvilke implikasjoner vurderer du at dette får for en motstander?

Spørsmål 2
Et forterreng preget av eliteinfanteri og andre skjulte styrker – hva kan dette medføre for en motstander av dette?

Spørsmål 3
En motstander med overlegen kvantitet og redundans på UAV'er og indirekte ild (spesielt MLRS), samt et økt tempo i targetingprosessen, hvordan påvirker dette en motstander? Hvilke prinsipper ville du ha vektlagt i møte med dette?

Spørsmål 4
Med sammenkobling av komplekse systemer for EK, cyber og informasjonskonfrontasjon på taktisk nivå – hvilken trussel representerer dette for din taktiske enhet?

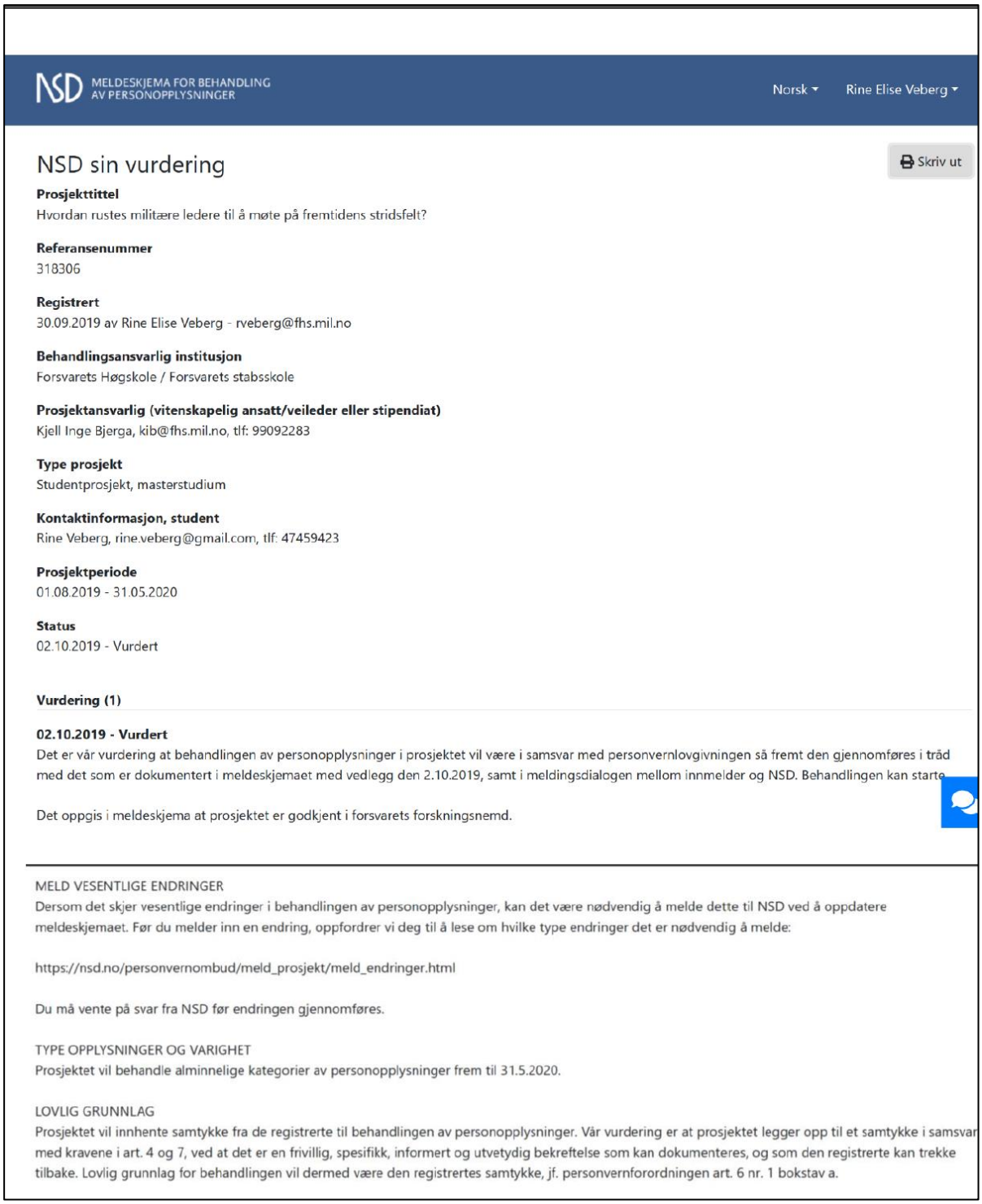
Del 3

Spørsmål 1
Opplever du at din kjennskap til en teknologisk motstander er endret etter intervjuet?

Spørsmål 2
Har du noen kommentarer eller betraktninger rundt det teknologiske stridsfeltet som du opplevde at spørsmålene ikke dekket?

Avslutning på intervjuet
Tusen takk for at du har satt av tiden til å bidra i denne studien. Forhåpentligvis bidrar du ikke bare til denne konkrete oppgaven, men også til å stimulere nye tanker rundt hvordan Hæren møter den teknologiske striden. Takk!

Vedlegg 7 – Godkjenning NSD



NSD MELDESKJEMA FOR BEHANDLING AV PERSONOPPLYSNINGER

Norsk ▾ Rine Elise Veberg ▾

NSD sin vurdering

Skriv ut

Prosjekttittel
Hvordan rustes militære ledere til å møte på fremtidens stridsfelt?

Referansenummer
318306

Registrert
30.09.2019 av Rine Elise Veberg - rveberg@fhs.mil.no

Behandlingsansvarlig institusjon
Forsvarets Høgskole / Forsvarets stabsskole

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)
Kjell Inge Bjerga, kib@fhs.mil.no, tlf: 99092283

Type prosjekt
Studentprosjekt, masterstudium

Kontaktinformasjon, student
Rine Veberg, rine.veberg@gmail.com, tlf: 47459423

Prosjektperiode
01.08.2019 - 31.05.2020

Status
02.10.2019 - Vurdert

Vurdering (1)

02.10.2019 - Vurdert
Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 2.10.2019, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte

Det oppgis i meldeskjema at prosjektet er godkjent i forsvarets forskningsnemd.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde:

https://nsd.no/personvernombud/meld_prosjekt/meld_endringer.html

Du må vente på svar fra NSD før endringen gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 31.5.2020.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).

NSD vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET
NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Tlf. Personverntjenester: 55 58 21 17 (tast 1)

Vedlegg 8 – Godkjenning Forsvarets Forskningsnemd

FORSVARET
Forsvarets høgskole

Vår saksbehandler
Borghild Boye, bboye@mil.no
+4723 09 57 55, 0510 5755
FHS/STAB/UTD FOU

Vår dato 2020-04-20
Vår referanse 2020/014094-002/FORSVARET/ 919

Tidligere dato
Tidligere referanse

Til
Rine Veberg
.
..

Kopi til

Tillatelse til å innhente opplysninger i og om Forsvaret til forskningsformål

1 Bakgrunn

Forsvarets høgskole (FHS) har mottatt din søknad av 30. september 2019 om tillatelse til å innhente opplysninger i og om Forsvaret til forskningsformål. På grunn av en misforståelse ble ikke den fullstendige søknaden mottatt for behandling i forskningsnemnda før 2. april 2020.

Prosjektet det skal samles data til er en masteroppgave, og følgende problemstilling er oppgitt: Teknologi og nye trusler. «Hvordan rustes militære ledere til å møte på fremtidens stridsfelt?» Det er gjennomført intervju med personell i Forsvaret.

2 Drøfting

Vurdering av søknader om tillatelse til å innhente informasjon i og om Forsvaret til forskningsformål er regulert av *Bestemmelse om utlevering av personopplysninger til forskning og gjennomføring av spørreundersøkelser*, fastsatt av sjef HR-avdelingen i Forsvarsstaben 1. mai 2018.

I henhold til punkt 2.3 og 2.4 i denne bestemmelsen er det en forskningsnemnd oppnevnt av sjef FHS som behandler søknader om tillatelse til datainnsamling i Forsvaret. Kriterier og rettsgrunnlag som skal legges til grunn for vurderingen er omtalt i punkt 4.1 og 4.2.

Forskningsnemnda har vurdert din søknad som tilfredsstillende i henhold til gjeldende krav.

3 Vedtak

Søknad om tillatelse til å innhente opplysninger i og om Forsvaret til forskningsformål innvilges. Tillatelsen gjelder til prosjektslutt 31. mai 2020.

4 Vilkår for tillatelsen

Det er kun gitt tillatelse til innhenting av det datamaterialet som fremgår av søknaden. Data hentet fra Forsvaret skal ikke benyttes til andre formål enn den aktuelle masteroppgaven. Ved prosjektslutt skal alle data hentet fra Forsvaret slettes. Det skal sendes sluttmelding til FHS vedlagt masteroppgaven. Sluttmelding sendes til datautlevering@fhs.mil.no

Sven G. Holtsmark
professor
leder av forskningsnemnda

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