FORSVARET
Forsvarets høgskole

Militære operasjoner i cyberdomenet

Hvordan påvirker cyberdomenet utøvelsen av operasjonskunst?

Steffen Molvær Rummelhoff

Masteroppgave

Forsvarets høgskole

Vår 2021

Forord

Valg av tema for min masteroppgave kom ganske tilfeldig til meg. Gjennom det første studieåret ved FHS var jeg innstilt på å skrive om ledelse og lederteam i Forsvaret. Endring av tema var en prosess som pågikk gjennom sommerferien 2020, når jeg fikk skoleåret litt på avstand og nye tanker oppstod. Det at jeg valgte å skrive om cyberdomenet og operasjonskunst ble ganske tilfeldig, men i ettertid er jeg svært godt fornøyd med at jeg valgte å endre tema og retning på oppgaven. Jeg har tilegnet meg ny kunnskap og forståelse om svært akutelle tema, som vil være nyttig fremover i min karriere.

Arbeid med masteroppgave er en modningsprosess. Selv om jeg har skrevet oppgaven er det mange gode venner og kolleger som har hjulpet meg med innspill, gjennom faglige diskusjoner og generelle råd og vink helt frem til innlevering. Til dere alle, tusen takk. Men det viktigste for meg gjennom denne prosessen har vært mine to veiledere.

Veiledning kan sikkert gjøres på ulike måter. Tilnærmingen mine veiledere har valgt har etter min mening vært helt perfekt. De har fra første stund vært støttende. De har utfordret meg faglig og metodisk, samtidig har begge vist stor grad av fleksibilitet og tilgjengelighet. Jeg har ikke blitt servert løsninger, men heller blitt utfordret til å tenke annerledes og nytt der det har trengtes. Denne måten å veilede på har i seg selv bidratt til utvikling og i så måte vært en god inspirasjon og motivasjon for min del gjennom hele masterarbeidet. Derfor går en stor takk til Stein Hatlem Forsdahl og Stig Tore Aannø.

Steffen Molvær Rummelhoff
Oslo, Mai 2021

Sammendrag

Operasjonskunst handler om å omsette strategiske føringer og direktiver til taktiske handlinger. Operasjonskunsten har til hensikt å koordinere og synkronisere militære fellesoperasjoner for å nå strategiske målsettinger. Det handler om å utnytte kunnskap, praksis og kognitive egenskaper som er med på å muliggjøre avgjørelse og derigjennom gjennomføringen av suksessfulle militære operasjoner. Planlegging, gjennomføring og ledelse av militære operasjoner er kjernen i den militære profesjon, hvor operasjonskunsten spiller en avgjørende rolle.

I 2016 anerkjente NATO cyberdomenet som et eget krigføringsdomene, på lik linje med land, sjø, luft og rom. Denne studien søker å beskrive og forklare hvordan cyberdomenet påvirker utøvelsen av operasjonskunst. Dette gjøres gjennom å analysere cyberdomenets påvirkning på de åtte fellesfunksjonene: manøver, kommando og kontroll, ild, etterretning, informasjon, styrkebeskyttelse, understøttelse og sivil-militært samarbeid.

Studien viser at cyberdomenet utfordrer oppfatningen av tid, rom og styrker, da domenet er globalt gjennom dets utstrekning og rekkevidde. Det tradisjonelle operasjonsmiljøet har på denne måten ekspandert og tilført krigføringen ytterligere en faktor, som medfører økt kompleksitet, slik erkjennelsen også var når operasjonskunsten som militærteori oppstod.

Som en relativt ny arena for krigføring utfordrer cyberdomenet også måten vi må tilnærme oss krigføringen på. Det muliggjør økt grad av asymmetri og utfordrer oppfatningen av konfliktspekteret, for når er vi i krig i cyberdomenet?

Effektene cyberoperasjoner skaper er alltid fysiske. Likevel utfordrer cyberdomenet den tradisjonelle tilnæringen til forståelse og utnyttelse av militær makt. Bruken og utnyttelsen av cyberdomenet gir uante muligheter, samtidig som det medfører økt risiko og sårbarheter. Skillet mellom det sivile og militære blir mer utydelig gjennom det digitale rom. Cyberdomenet har derfor endret krigens karakter og påvirker på denne måten også utøvelsen av operasjonskunsten.

Nøkkelord: Cyberdomenet, cyberoperasjoner, operasjonskunst, operasjonsmiljø og fellesfunksjoner

Summary

Operational art is the employment of tactical actions based on strategic guidance and directions. The purpose of operational art is to coordinate and syncronise joint operations in order to reach strategic ends and objectives. It contains the creative application of knowledge, practice and cognitive abilities, which enables success in military operations. Operational art holds an decisive role in the military planning process and during the execution of military operations.

In 2016, NATO recognised cyberspace as an operational domain, joining land, air, sea and space. This study seeks to describe and explain how cyberspace influences the conduct of operational art, by analysing the eight joint functions: Manoeuver, fires, command and control, intelligence, information, sustainment, force protection and civil-military cooperation.

The study shows that cyberspace challenge the perception of time, space and force contribution. As a global domain, through its prevalence and reach, cyberspace separates itself from the physical domains. The operational environment has further expanded with cyberspace, which adds more complexity to the conduct of military operations. The same recognition was done when operational art as a theory were presented.

Cyberspace, as a relative new operational domain, challenges the traditional understanding of war. Cyberspace further enables asymmetric means and capabilities. It challenges our perception of the spectrum of conflict. Because, when are we at war in cyberspace?

The effects of cyberspace are always physical. However, it does not only challenge the traditional understanding of war, but it also challenges the utilisation of military power. Cyberspace presents both new opportunities, risks and vulnerabilities to military operations. Cyberspace further obscures the division between the civilian and military area of operation. Cyberspace has changed the character of war, which influences the conduct of operational art.

Keywords: Cyberspace, cyber operations, operational art, operational environment and joint functions

Innholdsfortegnelse

Figurer

1 Innledning

«From the moment a rock was first used as a hammer, society has been driven by technology. Today's great leap forward is not physical, but it is digital» (Stoltenberg, 2018).

1.1 Aktualisering

Digitaliseringen verden de senere år har stått overfor har gitt oss uante muligheter. Det forenkler livene våre og gir oss muligheten til å være langt mer effektive enn tidligere. Mennesker kan nå kommunisere og interagere på måter som før ikke var mulig. Måten samfunnet utnytter seg av cyberdomenet på omtales i Forsvarets fellesoperative doktrine (FFOD, 2019) som en forutsetning for økonomisk utvikling, fremtidig velferd og stabilitet (Forsvarsstaben, 2019, s. 26). Norge er intet unntak og er nå et av de mest digitaliserte samfunnene i verden (Forsvarsdepartementet & Justis-og_beredskapsdepartementet, 2018, s. 28). Som betyr en stor tilknytning til- og avhengighet av cyberdomenet.

Men, digitaliseringen gjør oss samtidig også meget sårbare. Digitaliseringen har åpnet en helt ny arena for aktører som har til hensikt å ramme en annen part, en motstander eller en fiende. Gevinstene kan være økonomisk motiverte, eller det kan være et ønske om å tilegne seg kjennskap og kunnskap om noe eller noen. Det kan også være et ønske om å spre eller manipulere informasjon som på kortere eller lengre sikt vil bidra til at en uærlig eller destruktiv hensikt oppnås. Arild Bergh ved Forsvarets forskningsinstitutt sier at «siden 2014 ha man sett en markant økning i staters koordinerte bruk av sosiale medier for å forsøke å påvirke andre staters befolkning» (Bergh, 2020, s. 7). Dette bidrar til at demokratier og samfunn settes under press. Som vi har sett i maktkampen mellom Russland og vesten, hvor sosiale medier nyttes i utstrakt grad for å desinformere, villede og skape usikkerhet. Valget i USA 2016 er en ting, men i den siste tiden oppleves det en økning i cyberangrep fra statlige aktører mot andre lands statlige institusjoner, som Russlands angrep på stortinget høsten 2020 (Stortinget, 2020).

Rekkevidden og omfanget av de digitale verdikjedene[1] cyberdomenet utgjør er med på å utfordre alles sikkerhet. Lysneutvalget (2020) sier at sårbarhetene henger sammen med graden av sammenkoblinger. Altså i hvor stor grad et system er avhengige av andre eller ikke. Samtidig peker de på at systemenes kompleksitet også påvirker graden av sårbarhet. Jo mer komplekst et system er, desto mer uoversiktlig

[1] «En digital verdikjede er en struktur av leveranser mellom virksomheter, hvor hver leveranse enten er en digital tjeneste, software eller hardware» (DSB, 2020, s. 10).

kan det være, som igjen er med på øke risikoen for sårbarheter (DSB, 2020, s. 12). Dette gjelder innenfor alle etater og samfunnssektorer.

Digitaliseringen av krigføringen er ikke noe nytt. På lik linje med at det sivile samfunn er avhengige av det digitale rom[2] er Forsvaret det samme. Fra tidenes morgen har teknologisk utvikling og krigføring fulgt hverandre tett. Teknologi og krigføring har på denne måten drevet samfunnsutviklingen fremover (Conti & Raymond, 2017). Utvikling skaper og gir nye muligheter som må utnyttes til egen fordel. Samtidig gjør tempoet i denne utviklingen at det oppleves svært utfordrende og kan gjøre det vanskelig å forstå omfanget og betydningen av cyberdomenet. Operasjonsmiljøet er på denne måten i konstant endring og utvikling. Cyberdomenet er derfor med på å endre krigens karakter, noe militære sjefer og profesjonsutøver må ta inn over seg.

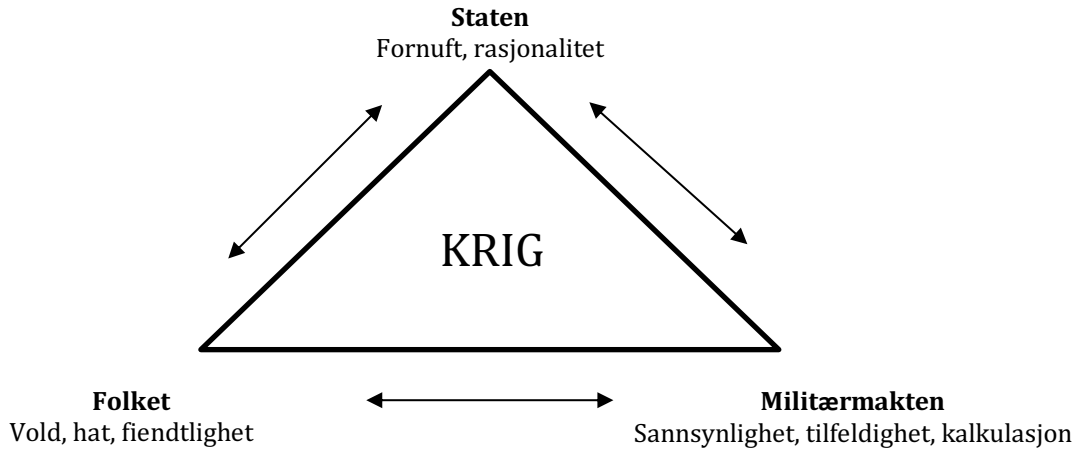
Som det til nå er det yngste og mest ukjente krigføringsdomenet utfordrer cyberdomenet hele samfunn på uante måter. Denne utfordringen må tas på største alvor og krever både nytenkning og tilpasning. Derfor var det svært gledelig å se at Sønstebyprisen[3] 2021 gikk til Cyberforsvarerene[4]. Dette er et synlig bevis på og anerkjennelse av viktigheten denne innsatsen har, samtidig som den er med på å aktualisere utfordringene vi står overfor. Cyberforsvarerne består av statlige, militære og private institusjoner som alle har til hensikt å beskytte Norge og norske interesser mot trusler i det digitale rom, i cyberdomenet. Det at prisen går til både militære og sivile aktører viser samtidig omfanget av domenet og dets utbredelse og spenn.

1.2 Krigføringens karakter

Krig har alltid vært og vil trolig også i fremtiden fortsatt forbindes med vold, lemlestelse, lidelse og død. Teknologisk utvikling kan sies å ha mye av skylden i dette. Likevel er det mennesker som står bak all brutaliteten. I følge Clausewitz var det menneskets behov for å sloss mer effektivt som drev utviklingen av krigføringen. Samtidig sier han at grunnlaget for hvorfor man går til krig (dens natur), fortsatt forblir det samme, uavhengig av krigføringens utvikling (Clausewitz, 1984, s. 127).
Krigens natur er ifølge Clausewitz konstant og består av en treenighet (figur 1); vold, hat og fiendtlighet; Sannsynlighet og tilfeldighet; Fornuft og rasjonalitet. Disse fenomenene knytter han

[2] FDs cyberretningslinjer (2014) omtaler det *digitale rom* som et synonym til cyberdomenet (Forsvarsdepartementet, 2014, s. 5)
[3] I henhold til statuttene kan Sønstebyprisen deles ut til: «(…) den person eller organisasjon som i handling har fremstått som en modig forsvarer av de grunnleggende verdier i vårt demokrati, herunder holdt forsvarsviljen levende og bidratt til at vårt forsvar trygger landets frihet og uavhengighet.» (Sønstebyfondet, 2021).
[4] Forsvarets Høgskoler FHS/Cyberingeniørskolen, Etterretningstjenesten, KRIPOS NC3, Telenor Norge, Næringslivets Sikkerhetsråd, Politiets Sikkerhetstjeneste PST, NTNU, Nasjonal Sikkerhetsmyndighet, Norsk Senter for Informasjonssikring – NorSIS, CSS og NORMA CYBER (Sønstebyfondet, 2021).

videre opp mot folket, militærmakten og staten (Clausewitz, 1976, s. 89). Alle er faktorer som vil påvirke krigers karakter (det foranderlige). For selv om det i hans tese antydes at krig i sin reneste form handler om å ødelegge sin motstander og utslette ham ved bruk av vold, fortsetter Clausewitz i sin anti-tese og syntese med å si at treenighetens fenomener vil påvirke hverandre og vil leve i en slags symbiose. Derigjennom fremheves fornuften og rasjonaliteten, representert gjennom staten. Fordi det er målsettingene med krigen som er det essensielle. Ikke i hvor stor grad en stat eller et folk klarer å ramme sin[e] motstander[e]. Det er i denne sammenhengen hans utsagn om at krig er en fortsettelse av politikken med andre midler må forstås. For der politikken setter målene, er militærmakten midlet for å nå de[t] politiske mål (Clausewitz, 1976). Dette forstås som politikkens primat og krigsmaktens autonomi.



Figur 1: Clausewitz´treenighet

Krigens karakter er et resultat av krigens natur. Det er politiske målsettinger som avgjør graden av militærmaktens voldsanvendelse. Både før, under og etter Clausewitz sin tid er det det fysiske stridsfeltet som i stor grad har vært grunnlag for det meste av krigføringen. Kriger blir utkjempet på landjorden, i luften eller på havet. Synergieffekten av å kombinere de tre fysiske domene har vist seg å gi uante muligheter. Ut over 1800- og 1900 tallet ekspanderte operasjonsmiljøet og endret dermed krigens karakter ytterligere.

På 1920-tallet i Sovjetunionen kom erkjennelsen av at krigføringen ikke lenger var det den en gang var. Krigen var blitt større, mer omfattende og det handlet ikke lengre kun om å vinne slaget for å vinne krigen. Til forskjell fra tidligere hvor det dreide seg om å beherske taktikken, ha kjennskap til våpen og utstyr, hadde den sovjetiske offiseren Aleksandr A. Svechin gjennom erfaringer fra 1.Verdenskrig og tidligere, sett at krigføringens økende kompleksitet hadde behov for en mer helhetlig tilnærming og forklaring (Svechin, 1927, s. 69). For å vinne krigen og ikke bare slagene måtte man

forholde seg til planlegging, gjennomføring og ledelse av operasjoner på en mer helhetlig måte hvor staten og strategien hadde en sentral rolle.
Operasjonskunst, som Svechin kalte det, handler om å omgjøre politiske og strategiske mål og føringer til taktiske handlinger og oppgaver (Forsvarsstaben, 2019, s. 243). Fra tidligere av fantes det ikke et nivå mellom politikken og de taktiske enhetene på slagmarken. Behovet for det operasjonelle nivået ble dermed identifisert og etablert.
Utfordringene krigens karakter presenterte måtte møtes med kognitive prosesser hvor striden ble utkjempet i hodet og på kartet i like stor grad som på slagmarken. Planlegging av operasjoner ble ikke bare synliggjort som mer omfattende, men behovet for dens omfang ble også belyst. I likhet med teknologiske revolusjoner og nyvinninger begynte mennesker å tenke annerledes om hvordan militære operasjoner måtte planlegges, gjennomføres og ledes. Det britiske Forsvarsdepartementet sier at konflikters utvikling må læres gjennom historien, tilpasses nåtiden for så å kunne forutsi fremtiden, noe som betyr at forståelsen av operasjonsmiljøet er avgjørende (MoD, 2016, s. 18). For å forstå krigens karakter stilles det derfor også store krav til å forstå konflikten[e] i seg selv.

1.3 Problemstilling

Cyberdomenet ble først under NATO Warsaw Sunmmit 2016 anerkjent som et krigføringsdomene, på lik linje med land, sjø, luft og rom (NATO, 2017b).

Cyberdomenet er trolig mer aktuelt nå enn noen gang. Det er et område som fenger og som skaper interesse, men også et område det kan være vanskelig å forstå.
For er vi virkelig klar over i hvilken grad vi som enkeltmennesker og del av verdenssamfunnet er blitt og har gjort oss avhengige av teknologi?
Er vi klar over mulighetene, begrensninger og utfordringene dette medfører?
For militære operasjoner betyr cyberdomenet et langt mer komplekst og utvidet operasjonsmiljø. Det er med på å utfordre skille mellom strategi og taktikk, mellom det politiske, militærstrategiske, operasjonelle og taktiske nivå. Dette medfører videre at planlegging, gjennomføring og ledelse av militære operasjoner også blir mer krevende. Som en konsekvens av dette vil cyberdomenet påvirke utøvelsen av operasjonskunsten. Oppgavens problemstilling er derfor:

- ***Hvordan påvirker cyberdomenet utøvelsen av operasjonskunst?***

1.4 Oppgavens oppbygning

I andre kapittel presenteres oppgavens teoretiske tilnærming. Først beskrives og forklares operasjonskunsten, hvordan den har utviklet seg og dens relevans i dag. Deretter presenteres cyberdomenet og hvordan det forstås som krigføringsdomene.
I oppgavens tredje kapittel presenteres studiens metode. Her vil oppgavens hensikt, metodevalg og forskningens kvalitet redegjøres for og drøftes.
I oppgavens fjerde kapittel drøftes cyberdomenets påvirkning på operasjonskunsten med bakgrunn i de åtte fellesfunksjonene: Manøver, ild, kommando og kontroll, etterretning, informasjon, understøttelse, beskyttelse og sivilt-militært samarbeid[5]. Til slutt vil jeg oppsummere og konkludere med hvordan cyberdomenet påvirker utøvelsen av operasjonskunst.

1.5 Analyse og avgrensning

Det kan argumenteres for at militærteorien legger grunnlag for utviklingen av militære doktriner, som igjen gir retning for militærstrategien. Summen av dette gir fundamentet for hvordan vi gjennomfører militære operasjoner. Fordi militærteorien sier noe om hvordan vi skal tenke om krig, hva det er og hvordan den kan forstås. Doktrinene skal på sin side redegjøre for og beskrive prinsipper og gi retningslinjer for hvordan militære styrker skal anvendes for å nå militærstrategiske målsettinger (Forsvarsstaben, 2019, s. 13). Målsettingen nås gjennom at politiske og strategiske føringer omsettes til taktiske handlinger.

Styrende doktriner og dokumenter i NATO og Norge er valgt for å beskrive og forklare hvordan cyberdomenet kan forstås og påvirker hvordan militære operasjoner planlegges, gjennomføres og ledes. Oppgavens problemstilling besvares videre ved å drøfte de åtte militære fellesfunksjonene, som i seg er kapabiliteter og aktiviteter som gjelder for alle fellesoperasjoner (Forsvarsstaben, 2019, s. 136; NATO, 2019a, s. 1-21). Fellesfunksjonene velges som drøftingsfaktorer fordi de er førende for militær planlegging, gjennomføring og ledelse av operasjoner og dermed må ses i sammenheng med utøvelse av operasjonskunsten. Samtidig er funksjonene gjennomgående for alle nivå i militære styrker (NATO, 2019a, s. 1-21). Fellesfunksjonen defineres i kapittel 4 – Drøfting.

Utfordringen med denne studien var først å fremst hvor vidt den skulle omhandle operasjoner i cyberdomenet eller om den skulle beskrive hvordan cyberdomenet påvirker militære operasjoner som

[5] I NATO - Joint Functions: Maneuver, fires, command and control, intelligence, information, sustainment, force protection and civil-military cooperation (CIMIC).

et av flere domener i et operasjonsmiljø. Det å vinkle oppgaven i retningen av å beskrive hvordan cyberdomenet, som et av flere krigføringsdomener, påvirker operasjonsmiljøet oppleves mest hensiktsmessig for å besvare problemstillingen.

Selv om operasjonskunsten i nyere militære doktriner knyttes til det fellesoperative nivå vil oppgaven legge mer vekt på hva operasjonskunsten er ment til å være og å gjøre enn nødvendigvis hvor den utføres.

Siden det er cyberdomenets påvirkning på operasjonskunsten som skal undersøkes vil ikke oppgaven ha et teknisk fokus, den vil fokusere på hvordan cyberdomenet kan anvendes og utnyttes i militære operasjoner fremfor hvordan det etableres og fungerer. Videre vil ikke oppgaven legge til grunn spesifikke aktører eller motstandere, men heller anvende relevante eksempler der det er hensiktsmessig.

Oppgaven har ikke til hensikt å gi det ene riktige svaret på hvordan cyberdomenet påvirker utøvelsen av operasjonskunst. Likevel vil oppgaven forhåpentligvis være med på å kunne øke forståelsen for hvordan cyberdomenet på noen områder kan påvirke militære operasjoner. Siden Norge ikke har en egen cyberdoktrine, men har ratifisert NATO sin cyberspace doktrine (AJP-3.20), kan denne oppgaven være et utgangspunkt for et slikt fremtidig arbeid. Uansett vil den trolig kunne bidra til kunnskap, utvikling og økt forståelse for to svært sentrale områder innen utøvelse av krigføring, nå og i fremtiden.

2 Teoretisk tilnærming

«Use the first moments in study. You may miss many an opportunity for quick victory this way, but the moments of study are insurance of success. Take your time and be sure» (Greenberg, 2019, s. 3).

I dette kapittelet vil både operasjonskunst og cyberdomenet gjøres rede for og diskuteres. Hensikten er å vise hva operasjonskunst og cyberdomenet er, hvordan begrepene forstås og deres betydning for militære operasjoner.

2.1 Operasjonskunst

2.1.1 Operasjonskunstens opprinnelse

Operasjonskunsten «operational art» oppsto som teori i Sovjetunionen på 1920-tallet. Den ble definert til å representere nivået mellom strategi og taktikk. I 1927 ga Aleksandr A. Svechin ut boken *Strategy*[6], hvor han sier følgende om krigskunsten: «In the art of war an operation means a combination of different actions aimed at achieving a goal set forth by strategy» (Svechin, 1927, s. 269). Denne slutningen trakk han på bakgrunn av observasjoner gjort gjennom grundige studier og analyser av tidligere kriger[7]. Operasjonskunsten og det operasjonelle nivå var til nå i historien ikke beskrevet. Derimot var både strategi og taktikk allerede behørig omtalt og diskutert av flere militærteoretikere.

Svechin hadde til hensikt å beskrive og forklare hvordan krigens karakter var i endring. Taktiske seire var ikke lengre avgjørende for å vinne kriger. Samtidig fremsto det mer tydelig at krig burde ses i sammenheng med andre maktmidler stater forvalter (Svechin, 1927, s. 100). Dette bidro til en oppfatning om at måten operasjoner ble planlagt, gjennomført og ledet på burde endres. Men var disse tankene virkelig nye?

Fra Napoleonskrigene og fremover hadde krig i stor grad dreid seg om å vinne slag og krigføringen ble primært ført gjennom landmakten. Med den andre industrielle revolusjon og 1.Verdenskrig ble det klart at krigens omstendigheter og dens karakter var i stor endring (Menning, 2005, s. 18). Strategien var alt mer avgjørende for staters eksistens (allianser, interne forhold og utvikling). Krigens karakter var i tillegg i hurtig endring som følge av teknologiske fremskritt. Krigens kompleksitet ble derfor søkt forklart gjennom grundige studier av historien – hensikten var å gi et mulig frempek på hvordan fremtidens kriger kunne bli og hvordan dens operasjoner burde gjennomføres (Menning, 2005, s. 3).

[6] Strategia på Russisk

[7] «…the book's center of gravity, was to make a careful study of recent wars and observe the way in which strategic art has evolved in the last 65 years and study the material preconditions which have determined this evolution» (Svechin, 1927, s. 65).

Disse tankene vokste på ingen måte frem i isolasjon. Fra tidligere var krig et tema som var nøye studert av flere, men oppfatningen av hva krig var og hvordan den burde føres og tilnærming til krigskunsten var derimot ulike.

Militærteorien kan defineres innen to paradigmer, hvor Baron Antoine-Henri Jomini og Carl von Clausewitz kan sies å være førende for henholdsvis den naturvitenskaplige og den samfunnsvitenskapelige retningen. Jomini representerer det naturvitenskapelige og beskriver hvordan en skal *føre* krig (Strachan, 2019, s. 177). Mens Clausewitz på sin side representerer det mer samfunnsvitenskapelige perspektivet og beskriver hvordan en skal *tenke* om krig (Strachan, 2019, s. 177). Både Clausewitzs - *Vom Krig* og Jominis - *The Art of War* har på mange måter vært styrende for forståelsen av strategi og taktikk siden 1800-tallet og frem til i dag.
Deres syn på strategi og taktikk var i noen grad ulik. I følge Jomini føres krigen av generalene. Det som besluttes av statsoverhodet [staten] er krigens karakter, altså hvorvidt den skal være offensiv eller defensiv (Jomini, 1862, s. 66). Målsettinger, operasjonslinjer og ledelse besluttes og utføres av de militære. «Strategy is the art of making war upon the map, and comprehends the whole theater of operations» (Jomini, 1862, s. 69). *Grand Tactics*[8] på sin side er utførelsen av planen. Planene kunne bestå av utallige slag og operasjoner, gjenkjennbart fra hvordan fellesoperasjoner i dag er tenkt gjennomført. Jomini kan sies å ha gitt oss oppskriften på hvordan vi skal vinne krigen, basert på egne erfaringer og opplevelser (H. Høiback, 2012, s. 108). Samtidig er det viktig å huske på at Jomini gjorde sine analyser på bakgrunn av Napoleons krigføring.

Napoleon Bonaparte var både hærfører og keiser. Han var på denne måten både staten og militærmakten. Napoleon førte krig i en tid hvor massehærene vokste frem. Til forskjell fra tidligere hvor krigene var mer begrensede [Kabinettskrig], ble de etter den franske revolusjonen omtalt som folkekriger. Strategien på dette tidspunkt handlet fortsatt om «the strategy of the single point», slik det også var tidligere under de mer begrensede krigene (Menning, 2005, s. 4). Det at kriger også i fremtiden fortsatt skulle avgjøres på bakgrunn av et slag skulle fort vise seg å være feil. Oppfattelsen av krigskunsten og strategi var mer begrenset til forskjell fra det som skulle komme. Krigenes karakter, med bakgrunn spesielt i den teknologiske utviklingen, endret synet på hvordan krig måtte føres og hvilken rolle strategien skulle ha i det hele.

[8] Grand tactics var i følge Jomini en av fem bestanddeler i «the Art of war». Han forklarer det som at: «Grand Tactics is the art of posting troops upon the battle- field according to the accidents of the ground, of bringing them into action, and the art of fighting upon the ground, in contradistinction to planning upon a map» (Jomini, 1862, s. 69).

Carl von Clausewitz, på lik linje med Jomini studerte også krig i Napoleons tidsalder. Til forskjell fra Jomini mente Clausewitz derimot at strategien handlet om å samordne alle slagene mot en felles målsetting. Han sier at militær aktivitet i sin natur kan være både taktisk og strategisk, men at det er signifikansen av handlingen som avgjør hvilke nivå aktiviteten handler på. Taktikken handler på sin side om det enkelte slag og trefning, mens strategien handler om utnyttelsen av de ulike slagene og deres betydning for å nå overordnede målsettinger (Clausewitz, 1984, s. 132). For Clausewitz var krig mye tettere knyttet til den politiske konteksten (H. Høiback, 2012, s. 108-109). Til forskjell fra Jomini så han krigen som noe mer overordnet, spesielt gjennom å forklare dens natur og dens karakter opp imot samfunnet for øvrig. Clausewitz sin treenighet kan derfor brukes til å forstå, beskrive og forklare operasjonsmiljøet og hvordan krig oppstår.

Operasjonskunsten oppsto i en tid preget av ulike retninger innen militærteorien. Den vokste frem som et resultat av at kriger ble mer og mer komplekse og i økende grad handlet om stormaktspolitikk. Behovet for å håndtere denne komplekse situasjonen ble i Sovjetunionen søkt løst gjennom å definere operasjonskunsten. Krigers karakter var i stadig endring. Derfor måtte også måten man tenkte om krig endres. En mer helhetlig tilnærming, hvor strategien fikk en langt større og mer betydelig rolle i utøvelsen av krigskunsten var nødvendig. Likevel handlet det for Forsvaret sin del fortsatt om å planlegge, gjennomføre og lede militære operasjoner. Strategi var ifølge Menning (2005), det som skulle lede en stat i forberedelsene for og gjennomføring og ledelse av kriger, da og i fremtiden (Menning, 2005, s. 7). Hullene mellom strategi og taktikk måtte tettes - løsningen ble operasjonskunsten.

2.1.2 Hva er kunst?

Begrepet *kunst* «*Art*» og krigføring har fulgt hverandre gjennom historien, og slik det er diskutert over har krigen, dens utøvelse og dens betydningen flere fasetter. Kunstbegrepet brukes om strategi så vel som om taktikk, men hvorfor brukes kunstbegrepet i sammenheng med krig?

Kunst, fra latin: *ars*, betyr ferdigheter. Begrepet kunst er altså ensbetydende med å inneha et sett med ferdigheter eller evnen til å utføre en handling (Heuser, 2016, s. 180). Når vi i dag hører ordet kunst er det lett å få assossiasjoner til malerier, statuer eller abstrakte figurer. Kunst handler om det visuelle, det fysiske og konkrete. På denne måten kan kunst forstås som noe kreativt uttrykt gjennom en fysisk handling eller ting. På den annen side handler også kunstbegrepet om det kognitive og abstrakte. Det å se muligheter fremfor begrensninger. Det å kunne forestille seg en situasjon og handle der etter. Det å kunne forstå og tolke på sin egen måte. Forklart gjennom at når noen ser på et kart så ser de kun et kart slik det er tegnet, mens andre klarer å se forbi kartet og ser terrenget. Uavhengig om kunsten uttrykkes fysisk eller kognitivt beskriver kunstbegrepet en handling som resulterer i en menneskelig aktivitet

(Kuusisto, Kuusisto & Roehrig, 2015, s. 170). Sammenhengen mellom disse to er likevel åpenbar da den fysiske tingen er resultatet av en kognitiv prosess som starter med en ide eller en forestilling om hvor en vil være eller hvordan noe skal eller bør være. I kunst handler det om å gjøre om et hvitt lerret til et kunstverk. I krig handler det om å gjøre en ufordelaktig situasjon om til en fordelaktig situasjon for sin egen del. Begge deler krever handling og stor grad av ferdigheter.

Innen militærteorien kan det sies å være vitenskap «science» som står i kontrast til kunsten. Science, fra latin: *scientia*, betyr kunnskap og klokskap. På denne måten kan vitenskap også forstås som en kognitiv egenskap. Mens utnyttelsen av vitenskapens funn kan anses som kunst, fordi kunsten også har en tydeligere praktisk dimensjon i motsetning til vitenskap (Heuser, 2016, s. 180). I United States Marine Corps (USMC) sin doktrine, MCDP 1[9] - *Warfighting* (1997), forstekes Hauser sin forklaring. MCDP 1 (1997) sier at ulike områder innen krigføringen faller inn under vitenskapskategorien, slik som ballistikk, mekanikk, effekten av våpen. Samtidig sies det at vitenskapen alene ikke er godt nok for å forklare krig som fenomen (USMC, 1997, s. 18). Doktrinen presiserer følgende:

> An even greater part of the conduct of war falls under the realm of art, which is the employment of creative or intuitive skills. Art includes the creative, situational application of scientific knowledge through judgment and experience, and so the art of war subsumes the science of war. *(USMC, 1997, s. 18)*

Det å føre krig og sloss er en kunst, hvorpå det å eksempelvis forske på krig og utvikle teknologi som skal benyttes i krigføringen er å betrakte som en vitenskap.

Selv om kunst og vitenskap kan sies å være to motsetninger er de samtidig svært symbiotiske. For det første danner vitenskapen grunnlaget for utøvelse av kunsten. Etterhvert som våpen, kjøretøy og maskiner har utviklet seg, har anvendelsen av disse midlene i stor grad påvirket måten vi fører krig på. Geværet gav oss ildkraft, mens kunsten lå i å utnytte ildkraften mest mulig effektivt for å overvinne motstanderen.
For det andre kan det påstås at kunnskap og klokskap kommer gjennom studering og skolering, og ikke bare gjennom praksis og erfaringer. For å i det hele tatt være i stand til å utøve krigskunsten må du kjenne til hva og hvorfor du bør gjøre noe for å oppnå ønsket sluttilstand. De fleste store militærteoretikere på 1800-, og 1900-tallet var eller hadde selv vært soldater og offiserer. Som eksempelvis Jomini, Clausewitz, Mahan, Corbett og Sir Basill Liddell Hart. De var både praktikere og teoretikere. På den måten ga deres studier økt legitimitet for å kunne mene noe om krig. Alle disse omtalte krig som en kunst og ikke som en vitenskap (Heuser, 2016).

[9] MCDP 1 – Marine Corps Doctrine Publication 1. MCDP 1 (1997) ersattet Fleet Marine Force Manual 1.

Til slutt er det likevel et faktum at [operasjons]kunsten, slik Svechin forklarer det, handler om det å tilpasse seg det operasjonsmiljøet krigen skulle føres i:

> A particular strategic policy must be devised for every war; each war is a special case, which requires its own particular logic rather than any kind of stereotype or pattern, no matter how splendid it may be. The more our theory encompasses the entire content of modern war, the quicker it will assist us in analyzing a given situation. (Svechin, 1927, s. 62)

Til å forstå operasjonsmiljøet er operasjonskunsten bedre egnet enn vitenskapen. Jo, vitenskapen er viktig for å være i stand til å sloss effektivt, men slik USMC (1997) forklarer det er og forblir krig et sosialt fenomen (USMC, 1997, s. 19). Som betyr at en både må forstå bestanddelene i operasjonsmiljøet, samtidig som man må forstå hvordan man på best mulig måte kan handle i en gitt situasjon. Vitenskapen gir nødvendigvis ikke de svarene, men den kan utnyttes for å finne løsninger. Svechin beskrev det på følgende måte: «There is no doubt that strategic practice is not a branch of scientific activity but is a field of application of an art» (Svechin, 1927, s. 71). Virkemidlene kan være de samme, mens måten de utnyttes på kan utgjøre forskjellen på seier eller nederlag.

2.1.3 Operasjonskunstens renessanse

Operasjonskunst i USA

Ut over 1930-tallet og i kjølvannet av 2.Verdenskrig forsvant ideen om operasjonskunsten i noen grad. Operasjonskunst som teori var i tillegg i liten grad adoptert av andre nasjoner utenfor Sovjetunionen. Derimot levde krigskunsten i beste velgående.

Tyskerne utviklet «Blitzkrig», som uten tvil ga gode resultater, spesielt innledningsvis i 2.Verdenskrig. Amerikanerne på sin side hadde ikke et doktrinelt grunnlag for å drive operasjoner av den størrelsen de gjorde under 2.Verdenskrig (Gabel, 1992). De eksisterende amerikanske doktrinene hadde et taktisk preg tilpasset mindre styrker i fredstid (Menning, 2005, s. 12). Likevel klarte de amerikanske styrkene gradvis å mestre kunsten å planlegge, gjennomføre og lede massive fellesoperasjoner som møtte de politiske og strategiske målsettingene, noe tyskerne på sin side ikke klarte (Frieser, 2005, s. 179). På samme tid viste russerne, etter innledende tilbakeslag, en mer perfeksjonert utgave av operasjonskunsten fra Stalingrad i 1943 og frem mot Berlin i 1945 (Menning, 2005, s. 11).

Etter 2.Verdenskrig opplevde verden et maktskifte. Vi gikk fra en multipolar- til en bi-polar verdensorden, med Sovjetunionen og Warszawapakten på den ene siden og USA og NATO på den andre. Atombomben endret samtidig måten man både så på krig og ikke minst hvordan krig kunne

føres. Fokuset på store fellesoperasjoner forsvant i noen grad, noe som også påvirket doktrineutviklingen (Menning, 2005, s. 13).

Første utgave av *U.S Army Field Manual (FM) 100-5 Operations* ble utgitt i 1976, med tilnavnet *Active Defence*. FM 100-5 Operations (1982) definerte og innførte det operasjonelle nivået i den amerikanske hæren. I samme doktrine bare fire år senere (1986) ble operasjonskunst nevnt eksplisitt for første gang i en amerikansk doktrine. Denne utviklingen hadde trolig sammenheng med den militærteoretiske renessansen som oppsto i det amerikanske Forsvaret i kjølvannet av Vietnamkrigen. Clausewitz og Vom Kriege ble igjen oversatt og brukt i doktrineutviklingen (Jørstad, 2004 I Sæveraas & Henriksen, 2007, s. 26). Vietnamkrigen ble på ingen områder en suksess for USA. Den er bare et solid bevis på at gjentatte taktiske seire ikke nødvendigvis vinner kriger.

Militærteoriens renessanse ble i stor grad brukt under utviklingen av de påfølgende FM100-5 Operations, hvor spesielt manøverkrigføring ble svært sentralt. Manøverkrigføringen handler primært om å komme seg innenfor fiendens beslutningssyklus og på den måten få han til å nå sitt kulimineringspunkt gjennom å konstant måtte reagere fremfor å agere. Denne måten å tenke på var i stor grad inspirert av tyskernes «Blitzkrig». Samtidig ble manøverkrigføring sett på som en løsning for å slå en konvensjonell overlegen fiende i Sovjetunionen (Mearsheimer, 1981, s. 106). Det operasjonelle nivået innføres og har til hensikt å knytte sammen taktiske metoder og middel med strategiske målsettinger (McCormick, 1997, s. 5). Likevel kan det argumenteres for at manøverkrigføring er mer en taktisk tilnærming enn nødvendigvis en strategisk tilnærming. Det handler mer om hvordan krigen skal føres på bakken enn om hvordan den skal vinnes politisk. Samtidig kan en også påstå at manøverkrigføring ligger nærmere operasjonskunsten og det strategiske nivå i sin tilnærming gjennom at det handler om å påvirke motstanderens vilje fremfor å nødvendigvis slå han fysisk:

> In the maneuver doctrine, maneuver is the ultimate tactical, operational and strategic goal while firepower is used primarily to create opportunities for maneuver. The primary objective is to break the spirit and will of the opposing high command...not to kill enemy troops or destroy enemy equipment. (Lind, 1997, s. 5)

Det er åpenbart at manøverteorien er inspirert av Clausewitz og andre tidligere militærteorier.

FM 100-5 Operations (1986) definerte operasjonskunst som «Operational art is the employment of military forces to attain strategic goals in, a theatre of war or theater of operations through the design, organization, and conduct of campaigns and major operations» (U.S.Army, 1986, s. 10). Videre i avsnittet om operasjonskunst beskrives hærens rolle som del av en militær kampanje, en

fellesoperasjon. Deretter snakkes det om viktigheten av å kjenne fiendens tyngdepunkt, hans center-of-gravity. Fokuset oppleves å hele tiden ligge på de kognitive egenskapene. Dette inntrykket forsterkes ytterligere når det sies at «Operational art requires broad vision, the ability to anticipate, a careful understanding of the relationship of means to ends, and effective joint and combined cooperation» (U.S.Army, 1986, s. 10). Sammenhengen med hvordan kunst defineres av Hauser (2016) er gjenkjennbar.

Distinksjonen mellom operasjonskunsten og taktikk er like tydelig i FM 100-5 (1986) som skille mellom strategi og taktikk var i tidligere militærteorier: «While operational art sets the objectives and pattern of military activities, tactics' is the art by which corps and smaller unit commanders translate potential combat power into victorious battles and engagements» (U.S.Army, 1986, s. 10). I tillegg til å skille på operasjonskunstens- og taktikkens rolle, defineres samtidig det nivåmessige skillet ved at korps er den øverste taktiske enhet.

FM 100-5 (1986) gjør enda et skille som er viktig i denne sammenheng: «...strategy derived from policy must be clearly understood to be the sole authoritative basis of all operations» (U.S.Army, 1986, s. 10). Dette er i samsvar med Svechin sin påstand om at hver krig er unik og at strategien må være i samsvar med krigens karakter (Svechin, 1927, s. 62). Ut ifra dette kan det påstås at operasjonskunstens renessanse og [gjen]oppdagelse i USA blir gitt en avgjørende rolle i den videre doktrinelle utviklingen og krigføringen. Ironisk nok utviklet og definert av deres motstander bare noen tiår tidligere. Samtidig høres ekkoet av Clausewitz og hans beskrivelse av krigens natur.

I dagens doktrine definerer den amerikanske hæren operasjonskunsten som «operational art is the pursuit of strategic objectives, in whole or in part, through the arrangement of tactical actions in time, space, and purpose» (U.S.Army, 2017, s. 2-1). Til forskjell fra når den først ble definert i 1986 ser vi her at definisjonen er mindre spesifikk. Den er ikke lenger begrenset til type operasjoner som kan forstås som at den skal være tilpasset alle typer operasjonsmiljø, samtidig kan definisjonen forstås til å være mindre nivå-avhengig.

Operasjonskunst i Norge

Forsvarets fellesoperative doktrine (2019) definerer operasjonskunst til å «omsette strategiske mål og ambisjoner til taktisk handling, og så styre taktiske operasjoner og aktiviteter i den retningen som bidrar til å realisere de strategiske målene» (Forsvarsstaben, 2019, s. 243). FFOD 2014 definerte operasjonskunst på samme måte som 2019 versjonen. Til forskjell fra de to nyeste utgavene definerte 2007 versjonen operasjonskunst noe rundere (Andersen & Ydstebø, 2016, s. 29). I 2007 ble operasjonskunst definert til å være «...en militær sjefs bruk av virkemidlene som står til rådighet for å oppnå de ønskede effekter og innfri de overordnede målene» (Forsvarsstaben, 2007, s. 173). I 2007 var ikke strategien en del av definisjonen, selv om den på den ene siden kan forstås til å beskrive det

fellesoperative nivå. På den annen siden kan den forstås til å være nivåuavhengig og i så måte allmenngyldig.

I 1995 fikk Norge sin første doktrine[10]. Men ikke før i år 2000 ble det utgitt en fellesoperativ doktrine. FFOD 2000 nevner operasjonskunst som begrep i svært liten grad. Den sier at «en del av operasjonskunsten består i å anvende styrker mot motstanderens vitale punkter på en slik måte at våpensystemene forsterker hverandre» (Forsvarets Overkommando, 2000, s. 104). En beskrivelse godt innenfor manøverteoriens tankegang om fiendens kulminerings- og tyngdepunkt. Likevel var innholdet i dagens definisjon av operasjonskunst ivaretatt gjennom at det samtidig sies at:

> Det militærstrategiske nivå må i tillegg til å gi direktiv som inneholder målsettinger, rammer og retningslinjer, stille styrker til disposisjon for å nå målsettingene. Innenfor disse direktivene bør det være opp til den operative sjefen å bruke styrkene slik han mener det er mest hensiktsmessig og rasjonelt for å nå målsettingene. (Forsvarets Overkommando, 2000, s. 104)

I likhet med 2007 versjonen, og til forskjell fra i 2014 og 2019, er det i denne forståelsen sjefen som vektlegges og hans evne til å lede tildelte styrker med bakgrunn i de ressursene han eller hun er gitt kommando over. Dette skyldes nok i stor grad at Norge i 1995 vedtok å ha et manøverorientert operasjonskonsept som sier at: «Et manøverorientert operasjonskonsept er sjefsorientert, og en operativ stab skal derfor organiseres for å legge forholdene til rette for en sjefsorientert ledelse» (Forsvarets Overkommando, 2000, s. 107). Et manøverorientert operasjonskonsept er fortsatt gjeldende for det norske Forsvaret i dag, men operasjonskunstens definisjon og forståelse av den er videreutviklet. Dette kan ha sammenheng med endringen av operasjonsmiljøet og de militære utfordringene vi nå står overfor, noe som kanskje kan sammenlignes med de erfaringene som ble gjort ut over 1900-tallet i Europa og senere i USA.

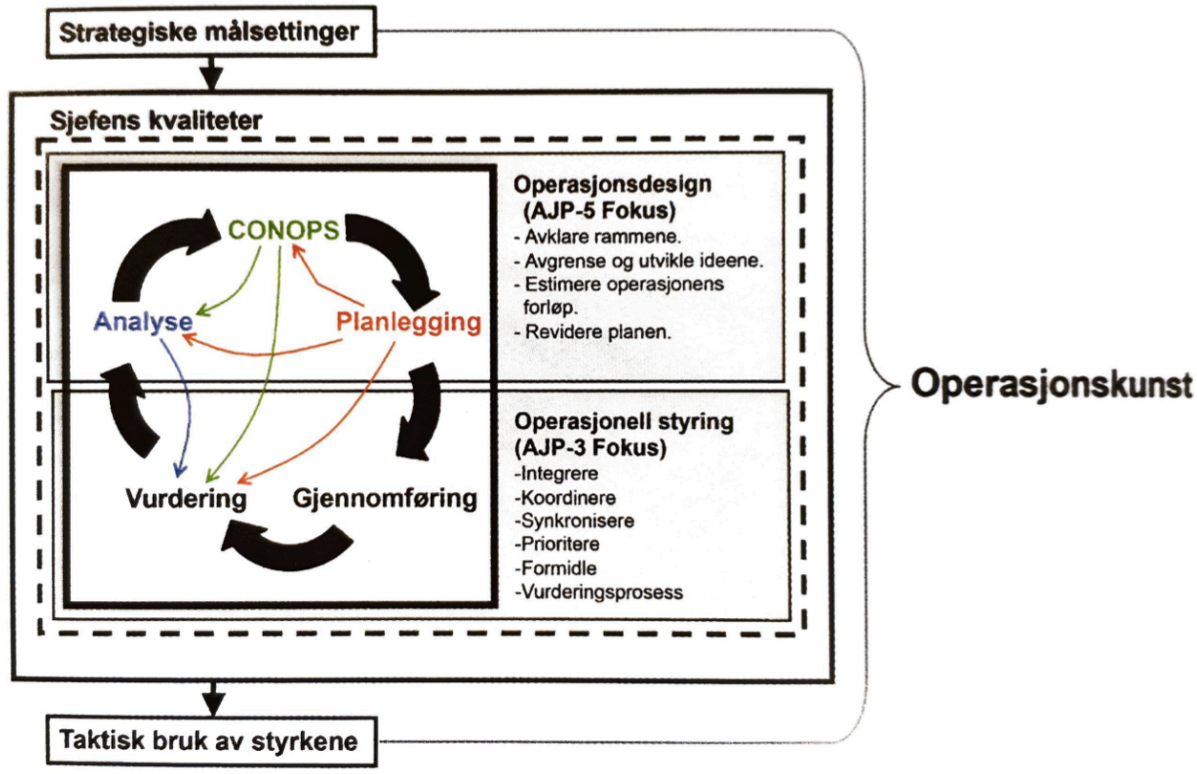
Operasjonskunst i NATO

USA og Norge har begge vært medlem i NATO siden 1949. Derfor skulle det være nærliggende å tro at deres syn på militærteorien i stor grad samsvarte. NATO definerer operasjonskunst som: «The employment of forces to attain strategic and/or operational objectives through the design, organization, integration and conduct of strategies, campaigns, major operations and battles» (NATO, 2019c, s. 93). Som i øvrige definisjoner er det hele tiden de strategiske målsettingene som pekes tilbake på og som operasjonskunsten søker å nå. Den ligner i større grad på *FM 100-5 Operations (1986)* sin definisjon enn den vi finner igjen i FFOD 2019. Derimot lyder U.S Army sin nåværende definisjon mer likt den

[10] *Forsvarssjefens grunnsyn på utvikling og bruk av norske militære styrker i fred, krise og krig (Forsvarsstaben, 2019, s. 10)*

norske enn NATO definisjonen. Samtidig skal det nevnes at NATO i stor grad har tatt begrepet videre og også gir den kunstneriske delen av fenomenet mening.

NATO AJP-01 sier at operasjonskunsten handler om å omgjøre strategiske føringer og målsettinger til taktiske handlinger gjennom at militære sjefer må tenke kreativt i sin tilnærming til militær problemløsning (NATO, 2017a, s. 4-5). Selv om operasjonskunsten kan oppleves å være sjefsrelatert, på samme måte som sjefens rolle i manøverteorien, presiseres det at operasjonskunsten realiseres like mye gjennom stabsarbeidet og de prosessene som gjennomføres, som hos sjefen selv (figur 2).



Figur 2: Sammenhengen mellom operasjonell styring, operasjonsdesign og operasjonskunst (Forsvarsstaben, 2019, s. 200).

NATOs planleggingsdoktrine (AJP-5) sier at: «Operational art is the conceptual framework underpinning the planning and conduct of operations» (NATO, 2019b, s. 1-1). Gjennomføringen og ledelsen av en militær operasjon er kun en del av operasjonskunsten, planleggingen er det som omgjør strategiske målsettinger til taktiske oppgaver.

2.1.4 Operasjonskunstens relevans

Operasjonskunst ble til fordi operasjonsmiljøet og krigføringen ble mer og mer kompleks. Den vokste frem som en «brobygger» mellom sttegi og taktikk (figur 3). Strategien skal i seg selv være visjonær

og overordnet, mens taktikken på sin side skal være mer håndfast og konkret. Synkronisering og koordinering av taktiske handlinger i tid og rom tilfaller det fellesoperative nivået som skal styre operasjonene slik at de overordnede målsettinger innfris (Forsvarsstaben, 2019, s. 11).

Figur 3: Gjennomkjøring av kommandonivåene (Forsvarsstaben, 2019, s. 186)

Siden 2.Verdenskrig har operasjonsmiljøet ytterligere ekspandert. Fra å bestå av tre fysiske domener består dagens operasjonsmiljø av fem[11] domener og flere miljøer[12]. Dette skulle i seg selv være nok til å validere operasjonskunsten som teori og behovet for utøvelsen av den i et økende og mer komplekst operasjonsmiljø. På den annen side kan det argumenteres for at dagens operasjonsmiljø i langt større grad enn tidligere vasker ut behovet for nivå-skillene fra politisk og strategisk nivå ned til stridsteknisk nivå (figur 4), fordi konfliktenes karakter er av en slik art at enkelte taktiske handlinger kan ha store strategiske konsekvenser og implikasjoner.

Operasjonskunsten relevans er fortsatt like stor som da den ble etablert om ikke større. Operasjonsmiljøets økende kompleksitet er en ting. En annen viktig faktor er den helhetlige tilnærmingen[13] og fokuset på symbiosen mellom en stats fire maktmidler (Diplomatic, Information, Military, Economic (DIME)) (NATO, 2017a, s. 1-3). Men det vil ikke si at dagens situasjon nødvendigvis er mer kompleks enn den som var tidligere, utfordringer mellom ulike samtider kan være vanskelig å sammenligne. Likevel kan det argumenteres for at det siden 2.Verdenskrig gradvis har blitt et mer utydelig skille mellom fred, krise og krig. Siden handlinger og aktiviteter under grensesnittet for krig både er mer utbredt og mulig å utnytte. Dette stiller store krav til både det politiske nivå sin forståelse for bruk av militærmakten, men samtidig også militære styrkers forståelse av de sikkerhetspolitiske rammer og utfordringer i sin anvendelse av egne maktmidler.

[11] FFOD 2019 beskriver verdensrommet som en del av luftdomene. Cyberdomenet er i så henseende det eneste nye domene siden verdensrommet alltid har vært der. Til forskjell har USA definert verdensrommet (Space) som et eget domene (TRADOC, 2018).
[12] Informasjonsmiljøet og det Elektromagnetiske spektrum (EMS) defineres som miljøer innen det ikke-fysiske domene (Forsvarsstaben, 2019, s. 22)
[13] I NATO: Comprehensive Approach

Forsvaret skal være dimensjonert for full-skala konvensjonelle høyintensitetskonflikter, noe som betyr at det kan argumenteres for at det fellesoperative nivået er avgjørende for å nå de strategiske målsettingene. På lik linje med at militære maktmidler skal samordnes i tid og rom for å bekjempe en motstander og oppnå ønsket effekt, må virkemidlene koordineres og synkroniseres. Den kan ikke samordnes hos de taktiske sjefene, den må gjennomføres og ledes fra det nivået som har best forutsetninger for å gjøre det. Dette kan bety at taktiske styrker opplever å ikke utnyttes full ut som del av en fellesoperasjon, men som FFOD 2019 sier er dette mindre betydningsfullt da det er de fellesoperative behovene som er styrende (Forsvarsstaben, 2019, s. 57).

Figur 4: Omgåelse av kommandonivåer (Forsvarsstaben, 2019, s. 186).

Det operasjonsmiljøet operasjonskunsten vokste frem under var i stadig endring. Krigers karakter endret seg raskt med bakgrunn blant annet i teknologisk utvikling. På den ene siden kan det påstås at operasjonsmiljøet under denne perioden var mindre komplekst sammenlignet med det operasjonsmiljøet vi opplever i dag. Siden omfanget var mindre og det var i stor grad landkrigen som dominerte (Andersen & Ydstebø, 2016, s. 30). Men også denne utviklet seg fort med de nye og økte mulighetene for troppeforflytning, ildkraft, beskyttelse, kommunikasjon og mobilitet. Luft- og sjødomenet muliggjorde større landoperasjoner. Stridsfeltets utbredelse ble større og større, kompleksiteten økte og behovet for fellesoperativt samvirke ble avgjørende for å vinne kriger. Ikke bare på tvers av nasjonale forsvarsgrener, men også på tvers av nasjoner.

Det er i denne sfæren operasjonskunsten må forstås. Det Jomini og Clausewitz presenterte etter sine studier og analyser av Napoleonskrigene og egen samtid er fortsatt gjeldende og relevant den dag i dag. Likevel gjorde ingen av de det teoretikerne i gamle Sovjet klarte, de så nemlig hele operasjonsmiljøet under ett. For Jomini og Clausewitz tilla ikke logistikken og de bakre områdene den oppmerksomheten Svechin og hans like gjorde. De beskrev og forklarte hvordan vi skal føre og tenke krig, da med fokus på den kinetiske krigen. Clausewitz fokuserte på «the use of armed forces in an engagement...the use of engagemanents for the object of the war» (Clausewitz, 1984, s. 128), uten å

forklare detaljene på hvordan logistikken var en del av krigskunsten. Jomini på sin side inkluderte logistikken, men den var fokusert på å understøtte det forstående slaget. Han beskriver forholdet mellom strategi, logistikk og taktikk som «Strategy decides where to act; logistics brings the troops to this point; grand tactics decides the manner of execution and the employment of the troops» (Jomini, 1862, s. 69). Svechin på sin side sier at «...operational art sets forth a whole series of tactical missions and a number of logistical requirements» (Svechin, 1927, s. 69). Han forsterker dette ved å si at logistikk er en av fire hoveddisipliner[14] som må studeres for å forstå krigskunsten. Dette underbygger omfanget og fokuset operasjonskunsten tilegnes og er med på å styrke teoriens gyldighet og relevans også i dag.

Oppgaven har til nå gjort rede for og diskutert operasjonskunstens bakgrunn, utvikling og relevans i rammen av militærteorien og hvordan den er anvendt og operasjonalisert gjennom førende doktriner. Videre i kapittelet vil det redegjøres for cyberdomenet, både som krigføringsdomene og operasjonsmiljø. Hensikten er å beskrive domenets særegenheter og belyse hvilke egenskaper som vil kunne ha betydning for utøvelsen av operasjonskunsten.

2.2 Cyberdomenet

Begrepet cyberspace dukket først opp i 1982 og ble introdusert av forfatteren Willian Gibson i novellen, *Burning Chrome* (SNL, 2019). Gibson definerte senere cyberspace i boken, *Neuromancer* (1984), til å være en verden sammenkoblet av datamaskiner. Det har vist seg at han skulle få ganske rett.

FFOD 2019 definerer cyber som «Et prefiks som viser at det ordet prefikset benyttes sammen med henviser til noe i cyberdomenet, eksempelvis cyberangrep eller cybertrussel» (Forsvarsstaben, 2019, s. 229). Andre sentrale begreper som også nevnes er cyberoperasjoner, som kan være enten offensive eller defensive, og cybersikkerhet som har til hensikt å beskrive en ønsket tilstand hvor systemers konfidensialitet, integritet og tilgjengelighet opprettholdes (Forsvarsstaben, 2019, s. 229). FFOD 2019, til forskjell fra NATO, bruker cyberdomene som begrep fremfor cyberspace.

[14] The art of war, in the broad sense, encompasses all aspects of the military profession, including: 1) studying weapons and other equipment used in warfare and studying defensive fortifications; 2) studying military geography and evaluating the resources at the disposal of different countries for waging war, studying social tendencies and analyzing possible theaters of military operations; 3) studying of military administration, which analyzes aspects of the organization of the armed forces, their administration and logistics, and finally 4) studying of the conduct of military operations (Svechin, 1927, s. 67).

Defensive cyberoperasjoner defineres som «defensive handlinger i eller gjennom cyberdomenet, utført i den hensikt å bevare egen handlefrihet i cyberdomenet» (Forsvarsstaben, 2019, s. 229).
Mens offensive cyberoperasjoner defineres som «handlinger i eller gjennom cyberdomenet som projiserer makt for å skape effekter som bidrar til militær sjef sine målsettinger» (Forsvarsstaben, 2019, s. 242). Begge definisjonen samsvarer med NATO sine definisjoner.

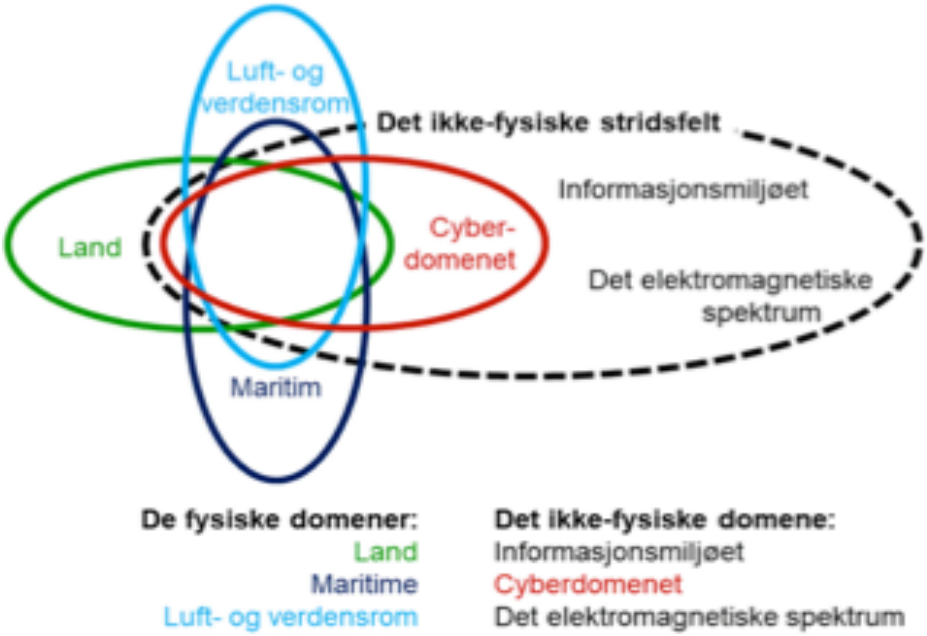
NATO definerer Cyberspace som «the global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data» (NATO, 2019c, s. 27; 2020a, s. 4). Det er flere ting som er verdt å merke seg med denne definisjonen. For det første omtales cyberspace som et globalt domene.
For det andre består det av et nettverk av informasjons- og kommunikasjonsteknologi og elektroniske systemer.
For det tredje dannes cyberspace av enten åpne- eller lukkede nettverk, hvor informasjons behandles, deles og oppbevares. Altså det muliggjør informasjonsutveksling og styring på ulike nivå gjennom hele operasjonsmiljøet.

FFOD 2019 har en tilnærmet lik definisjon av cyberdomenet. Det påpekes at det har global utbredelse og består av elektroniske systemer, informasjons- og kommunikasjonsteknologi som opererer i ulike former for nettverk hvor data og informasjon behandles, overføres og lagres (Forsvarsstaben, 2019, s. 25). I tillegg til dette sier FFOD 2019 i sin definisjon av cyberdomenet at det er et menneskeskapt fenomen. NATO forklarer det samme i sin cyberspace doktrine, men fremhever det som den elementære forskjellen fra de andre domene ved å si at «Cyberspace is also distinct in that its underlying physical elements are entierly man-made, which is different from Land, Air and Space and Sea» (NATO, 2020a, s. 2).
Videre består cyberdomenet av tre lag. Det fysiske-, det logiske- og det sosiale[15] lag. Det fysiske laget består av datamaskiner, servere, routere, kabler og annen infrastruktur avgjørende for forbindelse i cyberdomenet. Det logiske laget består av operativsystem, protokoller og software. Det er her koder og data lages og deles. Det sosiale laget er der hvor virtuelle identiteter skapes (NATO, 2020a, s. 4). Dette kan være e-post adresser, brukerprofiler og kontoer. En viktig presisering NATO gjør i denne sammenheng er å si at «the cyber-persona layer does not consist of real persons or organisations...» (NATO, 2020a, s. 4). På denne måten tilegnes ikke krigføringsdomenet kognitive egenskaper, som er menneskelige. Derfor kan den norske oversettelsen være misvisende. Derimot er den menneskelige dimensjonen tett knyttet til informasjonsmiljøet. Som er en sammenkobling av individer og

[15] I NATO: Cyber-persona layer.

organisasjoner eller informasjonssystemer hvor informasjon samles inn, prosesseres og deles (Forsvarsstaben, 2019, s. 25). Cyberdomenet muliggjør informasjonsmiljøets globale tilknytning og rekkevidde.

Det logiske laget er kjernen i cyberdomenet. Cyberdomenet er videre avhengig av det elektromagnetiske spektrum for å fungere, fordi det handler om å flytte og overføre data fra et sted til et annet. Det elektromagnetiske spektrum er avgjørende for at militære kommunikasjonssystemer, sensorer og effektorer skal kunne virke og utnyttes effektivt (Forsvarsstaben, 2019, s. 27). På denne bakgrunn kan det påstås at det elektromagnetiske spekteret i teorien kan påvirke innen hele operasjonsmiljøet (figur 5). Som betyr at selv om informasjonen i cyberdomenet ikke direkte angripes eller er utsatt for sårbarheter, kan mulighetene for å utnytte domenet likevel påvirkes.



Figur 5: Figuren viser hvordan det ikke-fysisk domene omslutter de fysiske domene. Sirklene illustrerer sammenhenger og representerer ikke faktiske størrelser (Forsvarsstaben, 2019, s. 136).

Cyberdomenet er et menneskeskapt fenomen og hadde sin spede begynnelse under den tredje industrielle revolusjonen[16]. Det innebefatter informasjons- og kommunikasjonsteknologi (IKT), elektroniske systemer og nettverk. Cyberdomenet er globalt, noe som betyr at det gir mulighet for

[16] Til forskjell fra de to foregående industrielle revolusjonene, oppsto den tredje revolusjonen i en internasjonal kontekst på 1970-tallet. Pådriveren her var i stor grad utviklingen og fremveksten av informasjons- og kommunikasjonsteknologi (IKT). Dette bidro til at vi gikk fra et mekanisk og analogt- til et digitalisert samfunn. Selv om den første datamaskinen ble utviklet allerede før den tredje industrielle revolusjonen, var det nå det virkelig skjøt fart. Den til nå siste, og fjerde industrielle revolusjonen, også kalt «Industry 4.0», bygger i stor grad på den foregående og dateres til rundt år 2010 (Sander, 2020).

forbindelse på tvers av geografiske barrierer. Cyberdomenets globale utbredelse gjør at det understøtter alle samfunnssektorer, militære som sivile. På denne måten integreres cyberdomenet med de fysiske domenene og skaper en gjensidig avhengighet. Det er i dette grensesnittet militære styrker og sjefer må være forberedt på å planlegge, gjennomføre og lede militære operasjoner.

2.2.1 Cyberdomenet som operasjonsmiljø

Før cyberdomenet som operasjonsmiljø beskrives forklares kort hva som menes med et operasjonsmiljø. Det er tidligere i oppgaven diskutert krigens utvikling og hvordan den kan forstås og har påvirket samfunnet. Dette er en del av operasjonsmiljøet. Det har videre blitt diskutert hvordan deler av militærteorier har blitt til og påvirket krigføringen. Dette er med på å forme vår oppfattelse og forståelse av miljøet vi skal operere i.

Operasjonsmiljøet må forstås gjennom en analyse av omverdenen. Forståelse er en egenskap militære profesjonutøvere er avhengige av for å lykkes i sin oppdragsløsning. Operasjonsmiljøet omfatter både det fysiske og ikke-fysiske stridsfeltet (Forsvarsstaben, 2019, s. 21).
NATO definerer operasjonsmiljøet som «...a composite of the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander» (NATO, 2017a, s. 1-5). I tillegg til å forklare hva operasjonsmiljøet er, gir samtidig NATO en pekepinn på hvilke hensyn og krav militære sjefer må ta og stilles overfor i sin analyse og vurdering av stridsfeltet. NATO sier at planlegging, gjennomføring og ledelse av militære operasjoner krever en helhetlig tilnærming[17]. Hensikten er å løse problemet eller utfordringen på best mulig måte. For å gjøre det må situasjonen analyseres og vurderes grundig. Operasjonsmiljøets økende kompleksitet utfordrer dette.

Selv om det fantes datamaskiner før 1960-tallet var de ikke godt utviklet eller etablert i nettverk. Det første nettverket av datamaskiner, ARPANET, ble etablert i 1969 i USA (Conti & Raymond, 2017). Siden den gang og frem til starten av 1990-tallet hvor internett virkelig tok av og ble allemannseie har utviklingen gått i rekordfart. I følge Lunde og Thune (2013) fantes det i 1991 ca 5000 nettverk, hvor i overkant av 30 land var sammenkoblet i Internett med om lag 4 millioner brukere (Lunde & Thune, 2013 I Johnsen & Kveberg, 2014, s. 11). På dette tidspunktet var vi ca 5 milliarder mennesker på jorden. Til forskjell var det i 2014 over 7 milliarder mennesker på jorden hvorav ca 40% av verdens befolkning var tilkoblet internett (Johnsen & Kveberg, 2014, s. 11). Siden 2014 har utbredelsen bare

[17] Comprehensive Approach betyr en helhetlig tilnærming hvor staters maktmidler (Diplomatic, Information, Military and Economic) ses i sammenheng med operasjonsjonsmiljøet. Operasjonsmiljøet (Operational Environment) består igjen av seks faktorer (Political, Military, Economic, Social, Information and Infrastructure (PMESII)), alle er faktorer som må analyseres og vurderes for å kunne beslutte hvilket maktmiddel som er best egnet for å løse et problem (NATO, 2017a).

økt og i 2020 antas det at over 60% av verdens befolkning har tilgang til internett (Clement, 2020). Internett er den dominerende og mest tydelige delen av cyberdomenet, noe som har stor påvirkning på operasjonsmiljøet. Både på grunn av dets hurtige utvikling, men også dets pågående ekspansjon. Samtidig finnes det lukkede nettverk med mer begrenset tilgang og tilgjengelighet.

Cyberdomenet, som et ikke-fysisk domene skiller seg fra de fysiske domene på flere området. For det første er cyberdomenet relativt nytt. Dets hurtige utvikling og utbredelse gjør at det i dag gir oss uante muligheter både sivilt og militært. På den annen side medfører disse mulighetene også flere sårbarhet som motstandere ønsker å utnytte til sin fordel. Derfor kan det påstås at et samfunn med mindre digitaliseringsgrad i teorien vil kunne være mindre sårbart digitalt sett, enn et samfunn hvor digitaliseringen har kommet langt, som eksempelvis i Norge.
For det andre gjør den globale utbredelsen og sammenkoblingen av mennesker og maskiner at cyberdomenet, til forskjell fra de fysiske domene, ikke har noen geografisk definerte grenser. Det som derimot også gjelder for cyberdomenet er nasjonale og internasjonale grenser i jurisdiksjonssammenheng, men hvor ansvaret er nasjonalt (Forsvarsstaben, 2019, s. 124; NATO, 2020b, s. 2). Som betyr at det fysiske laget alltid vil befinne seg innenfor et definert operasjonsområde eller en nasjonal grense.
For det tredje medfører den globale utbredelsen av cyberdomenet at «alt kommer nærmere». Det er dette som gir en motstander muligheten til å manøvrere over store avstander over lang tid uten at noen nødvendigvis vet om det. Samtidig kan en motstander ta seg over det samme «terreng» i løpet av millisekunder. Cyberdomenet gir med dette en mulighet for både overraskelse og tempo. Dette gjør at forholdet mellom det klassiske operasjonsområdet og cyberdomenet er spesielt utfordrende (Forsvarsstaben, 2019, s. 125).
For det fjerde er det enklere å skjule seg i cyberdomenet til forskjell fra de fysiske domenene. Samtidig kan det være vanskelig å avgjøre hvorvidt det er sivile eller militære aktører som beveger seg i nettet, som kan gjør det utfordrende å skille mellom sivile og militære mål, da domene understøtter alle sektorer (Forsvarsstaben, 2019, s. 26). Dette fører til at angrep eller kriminelle handlinger er vanskeligere å oppdage eller detektere, fordi det er bort imot umulig å bedrive effektiv beskyttelse av alt samtidig (Johansen, 2004, s. 20).
For det femte kan cyberdomenet bidra til at skadepanoramaet øker ved at det har et enormt nedslagsfelt. Skaden er nødvendigvis ikke kinetisk og like umiddelbar som ved et bombenedslag, men tilgangen på samfunnskritiske ressurser er svært god nå som bortimot alle tjenester og leveranser er digitaliserte. På den annen siden kan de allmenne konsekvensene minske ved at man, til forskjell fra tidligere, ikke lenger må kjempe seg gjennom terreng, landskap og byer hvor sivile bor for å nå de satte målsettingene som i konvensjonelle militære operasjoner.

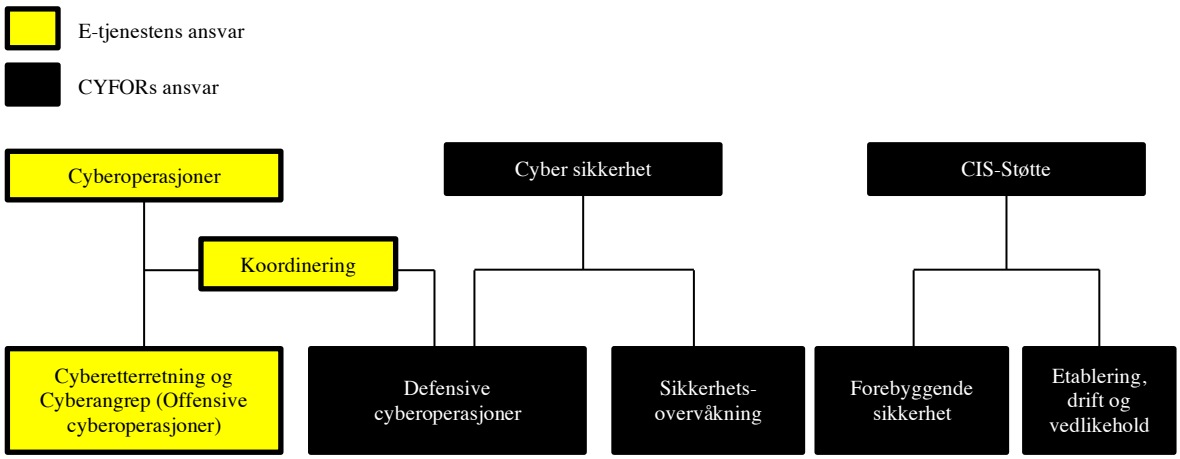
Til slutt er det viktig å påpeke at gitt cyberdomenets unge alder og den teknologiske utviklingen som skjer i verden er dette mest sannsynelig bare begynnelsen. Det å tro at en kan kontrollere cyberdomenet er trolig ren utopi. Eneste måten å sørge for at det ikke påvirker er å stenge det helt ned. Dersom dette gjøres vil verden slik vi kjenner den, teknologisk sett, flytte seg 50-60 år tilbake i tid, fordi det meste av tjenester er avhengige av cyberdomenet for å fungere. Heldigvis er ikke det menneskelige sinn avhengig av cyberdomenet for å fungere, men vi er strengt talt nødt til å tilpasse oss det. Både fordi det ikke er til å unngå, samtidig som det er med på å understøtte og styrke vår evne til å drive militære operasjoner.

Cyberdomenets muligheter og begrensninger må forstås. Militære operasjoner vil fremover stadig søke å «...i større grad øke sin operative evne gjennom å utnytte de mulighetene som samhandling i nettverk gir» (Forsvarsstaben, 2019, s. 25). Det moderne operasjonsmiljøet krever at en er i stand til å etablere situasjonsforståelse, utøve kommando og kontroll over styrker og på en god måte kunne benytte sensorer og effektorer som skal understøtte alle typer operasjoner på en effektiv måte. Cyberdomenet gir disse mulighetene. Militære sjefer og profesjonsutøvere må klare å utnytte de mulighetene cyberdomenet gir. Cyberdomenet må i likhet med de andre domenene, vies nok plass, fokus og oppmerksomhet i utøvelsen av Forsvarets primære oppgave som av tidligere sjef ved Forsvarets operative hovedkvarter, Rune Jacobsen, er sagt å være: «planlegging, gjennomføring og ledelse av militære fellesoperasjoner» (R. Jacobsen, 2015).

2.2.2 Cyberoperasjoner

Cyberoperasjoner gjennomføres for å sikre egen handlefrihet, både i cyberdomenet og i de fysiske domenene. Militære operasjoner kan enten gjennomføres ved å bli støtte av cyberdomenet, eller som isolerte operasjoner i det ikke-fysiske domene (Crowther, 2017, s. 72). Cyberoperasjoner kan være både defensive og offensive.

Oppgaven legger til grunn at cyberoperasjoner kun er de aktiviteter som er knyttet til- eller rettet mot en aktør, motstander eller fiende. Det vil si at forebyggende sikkerhet og etablering, drift og vedlikehold (CIS-støtte) av systemer og nettverk ikke er en del av cyberoperasjoner (figur 6), likevel er det en forutsetning for å drive cyber sikkerhetsoperasjoner.
Sikkerhetsovervåkning kan sies å være en del av defensive cyberoperasjoner gjennom at den har til hensikt å detektere og håndtere alvorlige hendelser gjennom risiko- og sårbarhetsanalyser som forebyggende tiltak (Forsvarsstaben, 2019, s. 126). Men kan samtidig også være en del av daglige operasjoner for å etablere og opprettholde situasjonsforståelse.



Figur 6: Organisering av cyberoperasjoner (Forsvarsstaben, 2019, s. 127).

Cyberoperasjoner defineres av NATO til å være «actions in or through cyberspace intended to preserve friendly freedom of action in cyberspace and/or to create effects to achieve commanders´ objectives» (NATO, 2020a, s. 4). Denne definisjonen er en sammenstilling av definisjonen for både offensive- og defensive cyberoperasjoner i NATO. Samtidig ser vi at den offensive cyberdefinisjonen også omhandler maktprojeksjon som en viktig del av det å oppnå ønskede effekter (NATO, 2020a, s. 4). Ved å tillegge den offensive definisjonen denne faktoren tillegges offensive cyberoperasjoner i stor grad en kognitiv og en fysisk dimensjon. Fordi projisering handler om å påvirke motstanderen til enten å tro at du har muligheten og kapabiliteten til å gjennomføre handlinger som vil påvirke deg eller at handlinger gjennomføres for å vise at en faktisk har slike kapabiliteter tilgjengelig. Den siste viser også vilje til å gjennomføre noe, fremfor kun å demonstrere det å ha evnen til å gjøre noe. I følge Berzins (2014) er det kampen om viljer som blir avgjørende fremover:

> ...modern warfare is based on the idea that the main battlespace is in the mind...wars are to be dominated by information and psychological warefare...The main objective is to reduce the necessity for deploying hard military power...making the opponent´s military and civil population support the attacker to the detriment of their own government and country.
> (Brezins, 2014, s. 5)

På den ene siden kan vi gi Brezins rett i å si at terskelen for å gå til krig kan være høyere enn noen gang og at statens samlede verktøykasse av maktmidler bidrar til et mer komplisert og høyt politisk spill, nettopp for å påvirke viljer mer «fredelig» fremfor bruken av militærmakten. På den annen side kan Brezins ta feil i at striden fremover vil handle om å forhindre bruken av konvensjonell

militærmakt «hard power», fordi militærmakt i den tradisjonelle forstand har vist seg så effektiv for å påvirke viljer, både i fortiden og i nåtiden at den rett og slett ikke kan unngås. Dersom Brezins har rett ligger ikke utfordringen nødvendigvis ikke kun i hvordan krigene skal føres, men også i det å definere hvor grensesnittet mellom fred, krise og krig går, kjent som gråsone-problematikken[18]. Dette oppnås ved utnyttelse av hybride trusler[19], som har til hensikt å beskrive staters utnyttelse og bruk av ikke-militære virkemidler (Forsvarsstaben, 2019, s. 28). Samtidig er det vanskelig å se for seg at militærmaktens betydning degraderes nevneverdig. Robert Art beskrev militærmaktens disiplinerende effekt som: «Diplomacy is the striking of compromises by states with differing perspectives and clashing of interests...It is the ultimate ability of each state to use its military instrument that diciplins the diplomats» (Art, 1996, s. 10). Dette er et eksempel på hvordan maktmidler kan understøtte hverandre uten at militærmakt anvendes, men samtidig bør den være klar ved behov.

Et konvensjonelt militært angrep mot en annen stat er i seg selv en tydelig krigserklæring og et sterkt signal om at viljen til å bruke makt er stor. Et angrep gjennom cyberdomenet derimot kan til forskjell være vanskelig å både detektere og derfor attribuere. Det at angripere ikke umiddelbart kan identifiseres bidrar til at responsen på angrepet kan bli fraværende eller for sen. Et overraskende konvensjonelt angrep kan en forsvarer i det minste mobilisere mot og fortsatt ha mulighet til å ta opp striden. I cyberdomenet er det ikke sikkert denne muligheten byr seg, fordi effekten vil kunne leveres umiddelbart og angriperen kan forsvinne like fort, fordi motstanderen har god mulighet til å skjule sin identitet (Forsvarsstaben, 2019, s. 128). Samtidig er avstand og rekkevidde en fordel angriperen også kan utnytte i det ikke-fysiske domene. Dette gjør at cyberdomenet bidrar til å ytterligere utfordre vår forståelse av konfliktspekteret og grensesnittet mellom fred, krise, konflikt og krig. Som i seg selv også utfordrer den kognitive sfæren ved å skape usikkerhet. Både til om egne kapabiliteter er gode nok for å motstå et angrep eller uvissheten om at det allerede kan ha forekommet et angrep som ikke er detektert ennå. Denne usikkerheten må derfor håndteres gjennom grundige og gode plan- og beslutningsprosesser hvor cyberdomenet, i like stor grad som de andre domenene og miljøene inkluderes og utnytte.

[18] Gråsone er definert som: a conceptual space between peace and war, occurring when actors purposefully use multiple elements of power to achieve political- security objectives with activities that are ambiguous or cloud attribution and exceed the threshold of ordinary competition, yet fall below the level of large-scale direct military conflict, and threaten US and allied interests by challenging, undermining, or violating international customs, norms, or laws (Popp & Canna, 2016 I Morris et al., 2019, s. 8).

[19] I følge FFOD 2019 er «Hybrid»-begrepet for uklart til å benyttes og tas inn i doktrinen. Likevel beskrives det «hybride» som et ikke-militært virkemiddel eller en irregulær styrke som tas i bruk før regulære militære styrker eller midler. FFOD forklarer det på følgende måte «Russisk politisk bruk av cyber og sosiale medier mot valg i vestlige demokratier har blitt brukt som eksempel på «hybridkrig»» (Forsvarsstaben, 2019, s. 28).

I Norge er det Cyberforsvaret som har oppgaven med å drive defensive cyberoperasjoner for å sikre Forsvarets egne nettverk og kapabiliteter. Etterretningstjenesten har på sin side ansvar for de offensive cyberoperasjonene (Forsvarsstaben, 2019, s. 125). Sjef Etterretningstjenesten er *Cyber Commander* i Forsvaret. Dette betyr at Sjef Etterretningstjenesten har overordnet koordinerende myndighet for militære cyberoperasjoner (Forsvarsstaben, 2019, s. 129).
Med denne oppgavefordeling ligger ansvaret for planlegging av offensive- og defensive cyberoperasjoner på det fellesoperative nivå. Hvor sjef Etterretningstjenesten har det offensive ansvaret og sjef Forsvarets operative hovedkvarter (FOH) har det defensive ansvaret som operativ sjef. Samtidig er det viktig å huske på at den militære kommunikasjonsinfrastrukturen også er avhengige av sivil kommunikasjons- og infrastruktur. For å skape redundans og robusthet i egne nettverk og system, gjennom å ha muligheten til å utnytte sivile kapabiliteter til militære formål ved behov. Samtidig som at trusler mot sivile nettverk også kan utgjøre risiko for militære nettverk og system. Dette krever stor grad av helhetsoversikt, kompetanse og ikke minst et tett samarbeide mellom etatene i Norge i rammen av Totalforsvaret.

Det fellesoperative nivået har ansvaret for å koordinere og synkronisere cyberoperasjoner. Men for å kunne gjøre dette må cyberkapabilitetene og kapasitetene, på lik linje med de i de fysiske domenene identifiseres, analyseres og vurderes opp imot de oppdragene som skal utføres på bakgrunn av strategiske føringer og direktiver, samt det operasjonsmiljøet det skal nyttes i. Hensikten er å utnytte cyberdomenet på en slik måte at den bidrar til å skape størst mulig effekt og synergi for den overordnede operasjonen, enten til støtte for en operasjon eller som en avgjørende operasjon i seg selv (NATO, 2020a, s. 7). Gitt cyberdomenets relativt unge alder, dets hurtige utvikling, dets globale utstrekning og tilgjengelighet, dets strategiske forankring og taktiske utøvelse, kan det fortsatt påstås at operasjonsmiljøets kompleksitet er økende. Dette er med på å utfordre utøvelse av operasjonskunsten.

2.3 Oppsummering teoretisk tilnærming

Det er i dette kapittelet søkt å beskrive og forklare hva som menes med operasjonskunst og cyberdomenet. Det spesielle og særegne med både cyberdomenet og operasjonskunsten er deres tette forankring til strategien, samtidig som de begge bidrar til militær avgjørelse på det taktiske nivå. Likevel er ikke disse fenomenene sett i sammenheng i særlig stor grad til nå. Dette kan ha sammenheng med at det på den ene siden fortsatt er et tema som ikke omhandles fordi forskningen ikke har kommet dit ennå. Det er nok med å beskrive og skape forståelse rundt sammenhengene. På den annen side kan det rett og slett være slik at planlegging av cyberoperasjoner er som all annen planlegging av militære operasjoner, noe det faktisk også burde være. Likevel kan det påstås at

cyberdomenets omfang utfordrer utøvelsen av operasjonskunsten på helt nye måter, som betyr at vi må tilpasse eksisterende metoder for å løse problemene i det ikke-fysiske domene tilnærmet likt som i de fysiske domenene.

Operasjonskunsten er forpliktet til ta inn over seg både de muligheter og begrensninger cyberdomenet tilfører dagens operasjonsmiljø. På den ene siden er det en erkjennelse at prioriteringer må gjøres for å kunne utnytte noe maksimalt. Samtidig kreves det kunnskap og kompetanse for at denne prioriteringen kan gjøres på en best mulig måte slik at kompleksiteten i militære operasjoner forblir håndterbar. Cyberdomenet har bidratt til å ytterligere utvide operasjonsmiljøet. Kunsten ligger i det å applisere nye kapabiliteter og muligheter til militær problemløsning.

Oppgaven vil med bakgrunn i dette fortsette å besvare problemstillingen: *Hvordan påvirker cyberdomenet utøvelsen av operasjonskunsten?*

I mangel av en norsk cyberdoktrine vil NATO sin cyberspace doktrine, *AJP-3.20 kapittel 1 - seksjon 2 - Joint Functions*, danne utgangspunktet for drøftingen. Bakgrunnen er at NATO AJP-3 og FFOD 2019 sier at fellesfunksjonene er selve grunnlaget og rammeverket for planlegging og gjennomføring av fellesoperasjoner (Forsvarsstaben, 2019, s. 136; NATO, 2019a, s. 21). Samtidig skal manøver, ild, kommando og kontroll, etterretning, informasjon, understøttelse, beskyttelse og sivilt-militært samarbeid bidra til en helhetlig tilnærming til problemløsningen og operasjonsmiljøene. Målsettingene og effekten søkes dermed oppnådd gjennom den fellesoperative koordineringen og synkroniseringen av taktiske handlinger i tid og rom.

For å oppnå effekter i de ulike fellesfunksjonene gjennom- og i cyberdomenet er en avhengig av god operasjonskunst. Utøverne av operasjonskunsten må på sin side forstå cyberdomenet for å kunne utnytte dets muligheter og unngå- eller mitigere dets begrensninger. Ved hjelp av fellesfunksjonene vil cyberdomenets utbredelse og omfang kunne belyses i flere av dets aspekt, samtidig som domenets påvirkning på utøvelsen av operasjonskunsten vil besvares.

3 Metode

«As understanding is contextual, it is perishable and requires continual development to maintain its validity» (MoD, 2016, s. 19).

3.1 Hensikt

Oppgaven søker å beskrive og forklare hvordan cyberdomenet påvirker utøvelsen av operasjonskunst. Hensikten er å etablere en dypere innsikt i- og forståelse for hvordan cyberdomenet kan påvirke planlegging, gjennomføring og ledelse av militære operasjoner. På denne måten kan studien gi merverdi for å videreutvikle kunnskapen til hvordan cyberoperasjoner kan forstås, integreres og anvendes som del av militære operasjoner. Selv om Jacobsen sier at man i samfunnsvitenskapelig forsking skal være mer forsiktig med å predikere (D. I. Jacobsen, 2015, s. 15), må det likevel gjøres visse antakelser om veien videre for at oppgaven skal kunne gi ytterligere verdi.

Under Cybermaktkonferansen 2020 poengterte professor Mass Lund Soldal at store deler av forskningen på cyberdomenet har en deskriptiv (beskrivende) tilnærming fordi cyber er et relativt ungt konsept. Han sier videre at kunnskapen rundt cyber og cyberoperasjoner ikke er god nok, derfor vil en normativ tilnærming som har til hensikt å si noe om hvordan det bør være mer utfordrende enn det å beskrive (Soldal, 2020). Dette underbygger oppgavens ambisjon og hensikt. Samtidig som det er med på å underbygge oppgavens metodiske tilnærming.

3.2 Valg av metode

Oppgaven nytter kvalitativ dokumentstudie med en pragmatisk tilnærming som vitenskapelig metode.

3.2.1 Dokumentstudie

Både operasjonskunst og cyberdomenet er sære som fenomen hver for seg, og kanskje mer sett i sammenheng slik oppgaven søker å gjøre. Dette gjør at det å forstå litteraturen og tankene bak er svært tidkrevende. Spesielt siden begge temaene for min del var relativ nye og uutforskede.

Fordelen med en dokumentstudie er at det kan være enklere å tolke sekundærdata enn primærdata. Sekundærdata endrer seg ikke og er tilgjengelig hele tiden. Dataene kan bearbeides og ses i sammenheng med andre funn og diskuteres fritt siden det allerede er publisert og tilgjengeliggjort. På samme tid vil ikke sekundærdata nødvendigvis gjenspeile alle tanker og ideer forfatteren har hatt underveis i skriveprosessen, noe som kan føre til at meninger og synspunkter oppfattes og forstås ulikt med opprinnelig intensjon. Dette kan spesielt være tilfellet når det gjelder operasjonskunst, da teorien ble skrevet for snart 100 år siden og har vært gjenstand for ulik tolkning og anvendelse opp gjennom

historien. Videre vil det ikke være noen tvil rundt gradering av informasjonen, da dokumentene som nyttes allerede er vurdert og gradert. Samtidig uteblir utfordringer tilknyttet behandling av personalopplysninger.

I tillegg, slik professor Soldal (2020) sier, er kunnskapen om cyberoperasjoner foreløpig generelt sett lav, noe som gjør at valget om dokumentstudie og bruken av sekundærkilder kan bidra til et større tilfang av relevant informasjon. Fordelen med at emnet er relativt ungt gjør at det både er aktuelt og spennende å skrive om, som fører til at tilfanget av litteratur er stor. På den annen side stiller dette store krav til kildekritikken, da «hvem som helst» kan mene og publisere noe uten at det nødvendigvis falsifiseres umiddelbart.

Oppgaven vil primært basere seg på førende og gjeldende militærteorier og doktriner i Norge og NATO. Øvrig litteratur er valgt for å underbygge eller utfordre allerede etablerte tanker. Siden studien søker å si noe om hvordan cyberdomenet påvirker utøvelsen av operasjonskunst vil oppgaven være en tilfellestudie (casestudie). Hvor cyberdomenet som krigføringsdomene og operasjonskunst som fenomen vil være de spesielle enhetene som studeres (D. I. Jacobsen, 2015, s. 97). Cyberdomenets påvirkning på utøvelse av operasjonskunsten drøftes med bakgrunn i dette i rammen av de åtte fellesfunksjonene.

3.2.2 Valg av litteratur

Utgangspunktet for valgt litteratur har vært militære doktriner, førende militærteoretiske publikasjoner, offentlige dokumenter, samt militære publikasjoner i tidskrifter og bøker. Doktrinene er valgt ut med hensyn til å beskrive og forklare hvordan militære styrker både skal tenke og forstå bruken og utnyttelsen av militære kapabiliteter, ressurser og teorier. I følge FFOD 2019 «...består et militært forsvar av tre bestanddeler; materielle ressurser, menneskelige ressurser og doktrine...» (Forsvarsstaben, 2019, s. 12). Doktrinene har et grunnleggende militærteoretisk utganspunkt og skrives av og for militært personell og avdelinger. Doktrinen blir på denne måten et autorativt militært dokument som beskriver militær maktanvendelse, på ulike nivå og innen ulike disipliner i det militære hierarkiet.

Både operasjonskunst og cyberdomenet er beskrevet i norske og allierte doktriner. I tillegg har NATO en egen doktrine, *AJP-3.20 Cyberspace Operations*, som beskriver hvordan cyberoperasjoner skal planlegges, gjennomføres og operasjonsvurderes, i rammen av en fellesoperasjon (NATO, 2020a, s. xiii). Denne er mye brukt og danner blant annet utgangspunktet for drøftingen av fellesfunksjonene.

Videre har boken, *On Cyber*, av Gregory Conti og David Raymond[20] (2017) vært flittig brukt. Den beskriver og forklarer hvordan cyberdomenet kan forstås i relasjon til flere av fellesfunksjonene, samtidig som den også bruker det taktiske, operasjonelle og strategiske nivået til å eksemplifisere og gi forklaringer til hvordan krigskunsten kan forstås i cyberkrigføring. Boken erkjenner at det doktrinelle grunnlaget for cyberdomenet og cyber operasjoner er tynt. Men samtidig brukes militær terminologi og begreper til å forklare og operasjonalisere forståelsen av cyberdomenet ut over en ren teoretisk tilnærming.

Siden oppgaven søker å forklare hvordan cyberdomenet påvirker utøvelsen av operasjonskunst, er operasjonskunst et svært sentralt begrep. Utgangspunktet her har vært både Svechin (1927) sin bok, *Strategy*, Clusewitz´, *On War* (1832) og Jomini´, *The Art of War* (1862) i oversatte versjoner, samt gjeldende nasjonale og allierte doktriner. I tillegg har det vært nyttet publikasjoner i militære tidskrifter, militære lærebøker og artikler som blant annet ble brukt som pensum ved stabsstudiet (2019/2020) ved Forsvarets høgskole. Ved å bruke publikasjoner fra pensum kan det påstås at flere sider av ulike problemstillinger belyses, da dette er en målsetting med tanke på vurderingsevne og evne for kritisk tenkning hos oss som elever.

Søkene etter litteratur har vært åpne. Søkemotorer som google scholar og Oria ved Forsvarets bibliotek har vært nyttet i tillegg til åpne søk på internett. I stor grad har det vært operasjonskunst og cyberdomenet eller cyberoperasjoner som er brukt som søkeord, både på norsk og engelsk uten spesielle begrensninger i tid. Men jeg har primært holdt meg til artikler publisert i tidskrifter tilknyttet statlige- eller militære departement og institusjoner.

3.2.3 En pragmatisk tilnærming

En pragmatisk tilnærming er valgt fordi den hverken gir store bindinger eller begrensninger på studien. Den påstår ikke at det ene er bedre enn det andre, men sier at det er studiens og forskerens behov som må være styrende (D. I. Jacobsen, 2015, s. 34). Samtidig setter dette store krav til at oppgaven ikke søker å favne alt, men kan ta noen standpunkt til hvordan den forholder seg pragmatisk til metode. Disse valgene beskrives nedenfor.

Tradisjonelt sett har det vært to tilnærminger som er dominerende i forskningen. Jacobsen (2015) sier at den *positivistiske* tilnærmingen som har sitt utgangspunkt i naturvitenskap og nær tilknytning til den

[20] Conti og Raymond har begge lang og bred erfaring fra det amerikanske forsvaret og med cyberoperasjoner. Conti har en doktorgrad i Computer science fra Georgia Tech og har blant annet ledet: «West Point´s cybersecurity reserch and education programs…and is currently Director of Research at IronNet Cybersecurity» (Conti & Raymond, 2017).
Raymond er tidligere hær offiser og har en doktorgrad i computer engineering.

kvantitative metoden og at den *fortolkningsbasert* tilnærmingen som på sin side forholder seg til samfunnsvitenskapen og den kvalitative metode, er de to tilnæmingene til hvordan empiri samles inn (D. I. Jacobsen, 2015, s. 31). Hensikten her er ikke nødvendigvis at det skal brukes enten tall eller ord for å forklare eller bevise noe, snarere handler det om hvordan man tilnærmer seg kunnskapen man søker etter. Så hvorfor er en pragmatisk tilnærming hensiktsmessig når cyberdomenets påvirkning på utøvelsen av operasjonskunst skal studeres?

Oppgaven søker på ingen måte å si at slik er det! Den vil heller fokusere på å si hvordan det kan være og hvordan det kan henge sammen. Cyberdomenet er menneskeskapt, likeledes er også operasjonskunst et fenomen som er menneskelig konstruert. Derfor er det ifølge Jacobsen (2015) vanskelig å si at noe faktisk er på den ene eller andre måten (D. I. Jacobsen, 2015, s. 22-23). Ontologisk[21] sett blir derfor tilnærmingen i denne oppgaven mer fortolkningsbasert enn positivistisk fordi både militærteori og doktriner er sosiale konstruksjoner som er i mer eller mindre konstant utvikling. Også epistemologisk[22] sett vil den fortolkningsbaserte retninger danne grunnlag for oppgaven. For selv om begge fenomenene er menneskeskapte er samtidig cyberdomenet høyst naturvitenskaplig i sin opprinnelse. Men det er ikke det som er interessant. Hvordan cyberdomenet driftes og er satt opp er i utgangspunktet likegyldig i denne sammenheng. Det som er interessant er hvordan cyber som krigføringsdomene både skaper muligheter og begrensninger for planlegging, gjennomføring og ledelse av militære operasjoner.

Videre søker oppgaven å ha en abduktiv tilnærming. En abduktiv tilnærming er en kombinasjon av den induktive[23] og deduktive[24] tilnærmingen (D. I. Jacobsen, 2015, s. 35). Abduksjon handler om hvordan nye hypoteser og tanker oppstår og hvordan vi velger mellom dem (Persson, 2019).
Det teoretiske utgangspunktet for denne tilnærmingen er at forskning er iterativt. Dette betyr at vi enten har tilegnet eller dannet oss en oppfatning av hva noe er eller hvordan det kan se ut og ha blitt til allerede. På denne måten vil en, til forskjell fra å være rent induktiv eller deduktiv hele tiden kunne gå tilbake og stille nye spørsmål eller endre deler av empirien, forskningen blir derfor en kontinuerlig prosess for å løse et problem (D. I. Jacobsen, 2015, s. 35). Jacobsen sier videre at det er:

> ...umulig bare å forholde seg til teori, fordi teorien ofte kommer som en følge av at man tidligere har observert noe. Samtidig er det naivt å anta at det er umulig å gå ut i verden som en ubeskrevet tavle – «tabula rasa» - helt uten antakelser og «før-dommer. (D. I. Jacobsen, 2015, s. 34)

[21] Ontologi: «slik ting faktisk er» (D. I. Jacobsen, 2015, s. 22).
[22] Epistiomologi: «læren om kunnskap» (D. I. Jacobsen, 2015, s. 23).
[23] En induktiv tilnærming handler om å går fra empiri (Data) til teori, en typisk samfunnsvitenskapelig tilnærming (D. I. Jacobsen, 2015, s. 34).
[24] En deduktiv tilnærming går fra en teori til å samle empiri for å bekrefte eller avkrefte teorien. Den deduktive tilnærmingen er et velkjent og oftest nyttes i naturvitenskaplig forskning (D. I. Jacobsen, 2015, s. 34).

Denne tilnærmingen er for øvrig også meget gjenkjennbar fra det militære systemet. Der hvor metoden er et utgangspunkt for hvordan eksempelvis en plan- og beslutningsprosess skal gjennomføres. Hvor faktorer som tid, rom og ressurser tilgjengelig er styrende for planleggingen. Samtidig som at de som skal gjennomføre prosessen, som profesjonsutøvere, allerede har kunnskap og erfaring som gjør at utgangspunktet trolig blir mer abduktivt, enn rent induktivt eller deduktivt.

Det neste som må vurderes er hvor vidt tilnærmingen skal være individualistisk eller holistisk. Oppgaven vil søke å ha en holistisk tilnærming. Som betyr at det er fenomenene i seg selv som er interessante og hvordan de påvirker helheten, og ikke forklares gjennom individers motiver og atferd (D. I. Jacobsen, 2015, s. 26). Dataene vil samles inn og kontekstualiseres, i stede for å isolere de slik som i et eksperiment. På denne måten vil det kunne være enklere å generalisere hvordan cyberdomenet faktisk kan påvirke utøvelsen av operasjonskunst. Ved å se på fenomener fremfor individer vil oppgaven slik sett være mer rettet mot det holistiske fremfor det individuelle.

Til slutt er det et spørsmål om nærhet eller distanse til fenomenet[ene] det forskes på. Den pragmatiske tilnærmingen tar et standpunkt som tilsier at det er vanskelig å unngå undersøkelseseffekter (D. I. Jacobsen, 2015, s. 37). Det vil si at det som forskes på påvirkes på den ene eller andre måten, enten ved direkte påvirkning fra forskeren sin side eller kognitive biaser[25] som oppstår i form av å tilhøre en profesjon som kan bidra til en form for undersøkelseseffekt (Coaker & Dobson-Keefe, 2015, s. 6). Siden dokumentstudie er valgt for å samle inn empiri unngås store deler av utfordringene knyttet til nærhet, noe som i større grad gjelder for undersøkelser hvor intervju, observasjon eller spørreundersøkelse nyttes som metode. Dette fordi forskeren vil på en eller annen måte kunne påvirke objektene eller deltakerne, enten gjennom sin tilstedeværelse eller gjennom spørsmålsformuleringer som kan være mer ledende og rettes tilbake mot forskerens standpunkt (D. I. Jacobsen, 2015, s. 38). Idealet om distanse tilhører opprinnelig den positivistiske tilnærmingen og er viktig med tanke på nøytralitet i forskningen.

3.2.4 Kritikk av metoden

Punktene over har redegjort for hvorfor jeg har valgt å nytte kvalitativ dokumentstudie med en pragmatisk tilnærming som oppgavens vitenskapelige metode.
Videre vil metodevalget drøftes i lys av alternativene som er valgt bort.

[25] Et kognitivt bias kan være et systematisk avvik fra hva som er mest rasjonelt eller en tankefeil som oppstår fordi vi søker å forenkle tolkningen av informasjon fordi den er for kompleks eller komplisert (Coaker & Dobson-Keefe, 2015, s. 6).

Observasjon og eksperiment er valgt bort da det ikke ville egnet seg som metoder for å gi svar på det studien ønsker å finne ut innenfor tidsrammen studien har. Samt at disse metodene ville påkrevd tilstedeværelse under ulike militære aktiviteter, som kunne utfordret gradering av oppgaven, i tillegg til at pandemien gjør at vi skal holde mest mulig avstand og unngå unødvendig nærkontakt.

Intervju er trolig den metoden som kunne vært mest nærliggende å nytte, som et alternativ til dokumentstudie, men er også valgt bort da dokumentstudie egner seg best besvarer oppgavens problemstilling innen gitte rammer. Samtidig er konsekvensene av å ikke nytte intervju som metode nøye vurdert og hensyntatt gjennom arbeidet med oppgaven.

Til forskjell fra denne oppgavens metodetilnærming, ville intervju gitt følgende muligheter. For det første kan et intervju enten være et supplement til en dokumentstudie eller det kan være primær metoden hvor teori og empiri hentes gjennom dokumentstudier for å understøtte intervjuet og videre analyse. Dette kan gi en studie mer bredde og sannsynligheten for at intervjuobjektenes personlige meninger tilfører noe nytt til en studie er til stede. I dette tilfelle ville trolig andre betraktninger om hvordan cyberdomenet påvirker utøvelsen av operasjonskunst kommet frem og kunne i så måte balansert oppgaven mer enn det som gjøres ved bruk av sekundærkilder.
For det andre gir intervju førstehåndsfortellinger. Førstehåndfortellinger betegnes som av Jacobsen (2015) som primærdata (D. I. Jacobsen, 2015, s. 65). I en dokumentstudie må man basere seg på andre- og tredjehåndsfortellinger, noe som kan gjøre det vanskelig å forvisse seg om i hvor stor grad informasjonen er akkurat slik den fremstilles. Likevel må styrende doktrine i NATO og Norge kunne anses som troverdige da de baseres på militære erfaringer som er med på å definere og standardisere den militære terminologien (Forsvarsstaben, 2019, s. 13). Primærdata på sin side gir forskeren økt grad av kontroll over den informasjonen som behandles og samles inn (D. I. Jacobsen, 2015, s. 172). På den annen side er det ikke sikkert intervju nødvendigvis gir den informasjonen en søker eller var ute etter, da intervjuobjektet kan forstå situasjonen og temaene på en annen måte enn det som var hensikten. Undersøkelseseffekten kan på denne måten fremprovoseres eller forsterkes. Dersom dette skal forhindres kan det være behov for mer direkte spørsmål eller forberedelser av intervjuobjektet, som igjen fører til at intervjuer kan komme i den situasjonen hvor forskeren leder eller styrer intervjuet i den retningen man selv ønsker. Forskeren vil fortsatt ha kontroll på dataene, men om det er god kontroll avgjøres ikke her.
For det tredje vil et intervju kunne være med på å nyansere et bilde eller en forestilling og antakelse forskeren har fra tidligere. Det er trolig enklere å avdekke standpunktene og motivene hos intervjuobjektet til forskjell i en dokumentstudie hvor det kun er teksten som snakker for seg. Likevel er det innen forskning tydelige posisjoneringer på anerkjente forskere og tidsskrifter, noe som gir formening om hvilke standpunkt hun eller han har. I tillegg søker doktriner å formidle militære

erfaringer, definere begreper og standardisere terminologi, som også er med på å definere hvilke standpunkt Forsvaret og alliansen har tatt.
For det fjerde vil forskeren etter at et intervju er gjennomført ha mulighet til å kvalitetssikre informasjonen. Dette gjøres ved å gjennomføre oppfølgingsintervjuer, noe som kan være nyttig etterhvert som studien skrider frem. Informasjonen i et intervju omtales av Jacobsen (2015) som mer spontan. Fordelen med dette er at en får det ærlige svaret. På den annen side kan de ærlige og spontane svarene også være mindre gjennomtenkt. Så selv om dokumentstudier baserer seg på informasjon som er lite spontan, kan det at informasjonen er skriftlig bety at den er mer gjennomtenkt og reflektert (D. I. Jacobsen, 2015, s. 172). Men dersom oppfølgingsintervjuer må gjennomføres blir studien i seg selv også mer tid- og ressurskrevende.

På samme måte som at ingen metode i utgangspunktet er bedre enn en annen, finnes det styrker og svakheter hos alle tilnærminger. Oppgaven har valgt dokumentstudie som foretrukne metode for å beskrive og forklare hvordan cyberdomenet påvirker utøvelsen av operasjonskunst. Jacobsen sier at: «...ingen undersøkelse kan gi et helhetlig bilde av virkeligheten...alle data bare gir en liten flik av virkeligheten...jo flere metoder vi anvender, desto flere vinklinger får vi...og da kan vi oppnå et noe mer helhetlig bilde» (D. I. Jacobsen, 2015, s. 174). Det å kun ha en tilnærming kan sies å være en svakhet med oppgaven. Likevel gir valgt metode oppgaven stor handlefrihet i at temaene kan belyses fra flere vinkling og nivå, og på denne måten unngå å prioritere respondenter slik man må gjøre i en intervjusituasjon. Samtidig er bevisstheten til at det også stilles store krav til kildekritikk av sekundærkilder stor. Derfor vil forskningens kvalitet omhandles i neste del av dette kapittelet.

3.3 Forskningens kvalitet

Metoden som velges er med på å gi forskningen kvalitet. Samtidig er det ulike fallgruver som nødvendigvis ikke kommer frem av den foretrukne tilnærmingen. Innsamling av empiri er metoden, derfor er bevisstheten rundt empiriens gyldighet og relevans viktig, samtidig som at den skal være pålitelig og troverdig (D. I. Jacobsen, 2015, s. 16). Oppgavens validitet og reliabilitet, samt min rolle som forsker og etiske problemstillinger omhandles derfor videre i kapittelet.

3.3.1 Validitet

Oppgavens validitet avgjøres først og fremst gjennom de slutningene som gjøres. Studien har som utgangspunkt at det trolig finnes flere svar på spørsmålet som stilles i denne oppgaven. Likevel er dokumentene behandlet på en slik måte at informasjonen ikke er søkt mistolket, forenklet eller endret. Samtidig er kildematerialet relevant da det for det første er hentet primært fra militære doktriner og tidsskrifter. Uten at det nødvendigvis er her alle svarene finnes. Doktriner har til hensikt å «...formidle militære erfaringer (best practice), definere begreper og standardisere den militære terminologien»

(Forsvarsstaben, 2019, s. 13). Dette kan i seg selv være en utfordring med tanke på overførbarheten mot andre organisasjoner og etater, da ulik terminologi nyttes i ulike miljøer, og om det doktrinene beskriver er representativt for virkeligheten.

Cyberdomenet til forskjell fra operasjonskunsten som fenomen er relativt ungt, men samtidig et område hvor tilfanget av data er stort. Likevel oppleves operasjonskunsten som en bredt akseptert teorie med bakgrunn i dens rolle i doktrinene. Dette stiller igjen store krav til at de dokumentene som omfattes av oppgaven granskes med et kritisk blikk for nettopp å ivareta den interne gyldigheten. Overførbarheten vil trolig kunne være stor, både innen det militære system og overfor sivile etater og organisasjoner. Fordi faktorene som drøftes er gjenkjennbare og relevante for operasjoner i cyberdomenet, samtidig som at domenet i stor grad omslutter og omfatter både den militære- og den sivile sfæren. I norsk sammenheng er dette en stor fordel gitt det tette samarbeide eksempelvis Totalforsvaret krever.

3.3.2 Reliabilitet

Siden reliabilitet handler om i hvor stor grad studien eller forskningen er til å stole på forstås reliabilitet i denne sammenhengen som den tilliten jeg som forsker klarer å etablere gjennom mine tanker, tolkninger og ideer, samt min kunnskap, forståelse og uttrykte synspunkter i denne studien. Det at dokumentstudie nyttes som oppgavens metode gjør at den er svært etterprøvbar, både for å teste funn og ettergå kilder. Den største trusselen med tanke på metodevalget er min evne til å forstå det forfatterne kommuniserer og omsette dette til en studie på en troverdig måte. Nyeng (2012) sier at:

> ...vi vet at også vitenskapelig kunnskap kan vise seg å være usann og bli erstattet av ny kunnskap. Den nye kunnskapen har vi så, inntil videre, grunn til å tro på, ikke fordi vi kan garantere at den er sann, men fordi den er metodisk frembrakt og velbegrunnet. (Nyeng, 2012, s. 9)

Han fremhever det som tidligere er nevnt og som Jacobsen også poengterer, at ingen metode er fullkommen, alt kan ikke studeres samtidig, men å ha sannheten som ideal i forskningen er avgjørende viktig. Man er likevel ikke forpliktet til å finne sannheten, så lenge en handler innenfor de vitenskapelige normer (Nyeng, 2012, s. 10). Oppgaven representerer derfor min forståelse av hvordan cyberdomenet påvirker utøvelsen av operasjonskunsten.

3.3.3 Forskerens rolle og kjennskap til temaet

Bakgrunnen for at jeg valgte å skrive om cyberdomenet og operasjonskunst er flere og det at jeg jobber i Forsvaret er ingen hemmelighet. Operasjonskunst var et valgfag Forsvarets høgskole tilbød under andre semester på stabsskolestudiet. Før dette hadde jeg ikke reflektert mye rundt hva operasjonskunst var, selv om andre militærteorier var godt kjent. Grunnen til at jeg søkte dette

valgemnet var fordi jeg hadde fått jobb ved Forsvarets operative hovedkvarter, altså på det fellesoperative nivå. I henhold til teorien er det på det operasjonelle nivået operasjonskunsten utøves, derfor ville jeg vite mere om det.
Cyberdomenet ble valgt fordi jeg ikke kunne så mye om det fra tidligere. Det er et relativt nytt, men voksende fagfelt i militær sammenheng. Aktualiteten cyberdomenet har både sivilt og militært gjør at det har og fortsatt vil ha store påvirkninger på planlegging, gjennomføring og ledelse av operasjoner nå og fremover. Derfor er relevansen av ervervet kunnskap stor.

Nysgjerrighet og kompetanseheving er det som har drevet meg gjennom denne prosessen. «Krigen» i cyberdomenet foregår nå. Og det er lite som tyder på at det blir mindre aktuelt fremover. I og med at jeg fra tidligere i liten grad har erfaring med og studert både operasjonskunst og cyberdomenet har jeg gjennom denne prosessen fått mulighet til å fordype meg i temaene. På den ene siden gjorde min bakgrunnskunnskap at jeg ikke hadde noe nært forhold til temaene, slik at objektiviteten var der fra starten av. Jeg gikk inn med et åpent sinn. På den annen siden kan min tilsynelatende objektive tilnærming ha bidratt til at jeg fort ble subjektiv i mitt tankesett siden alt nytt jeg leste fremsto logisk og rett. Dette kalles *Information and availability bias* (Coaker & Dobson-Keefe, 2015, s. 8-9). Det at jeg var bevisst slike kognitive biaser har vært med på å opprettholde en kritisk sans.

Med bakgrunn i diskusjonen i dette kapittelet kan det påstås at jeg som forsker går inn i prosessen med åpent sinn og få forutinntattheter. Idealet er at prinsippet om avstand etterleves. Likeledes søkes det å samle og analysere empiri som bidrar til å opprettholde en helhetlig forståelse og tilnærming til fenomenene gjennom hele studien. Utfordringen ligger i å ikke relatere alle nye tanker og problemstillinger til tidligere erfaringer. Likevel blir det å holde nødvendig kritisk avstand viktig (D. I. Jacobsen, 2015, s. 57). Mitt ønske er at studien kan bidra til utvikling i Forsvaret, slik den har gjort for meg.

3.3.4 Etiske problemstillinger

Det er knyttet færre etiske problemstillinger til dokumentstudie enn til andre kvalitative metoder. For det første unngås etiske dilemma som gjerne kan oppstå mellom en forsker og den eller de som skal undersøkes (D. I. Jacobsen, 2015, s. 45). Dette betyr at jeg i liten grad må tenke på å skjule studiens hensikt og på denne måten står i fare for å svekke oppgavens relevans.
For det andre vil det ikke kunne oppstå noen interesse- eller personkonflikter i forbindelse med studien. Fordi all dokumentasjon som nyttes allerede er publisert. Likevel skal en være forsiktig med å utnytte materialet og dra det helt ut av kontekst. Dette er også viktig for reliabiliteten.

Jacobsen (2015) knytter likevel noen problemstillinger til det denne oppgaven studerer. Ikke temaene i seg, men det å studere egen organisasjon. På den ene siden er dette veldig vanlig fordi det kan føles trygt, man har en interesse for det en jobber med og det kan bidra til utvikling på arbeidsplassen (D. I. Jacobsen, 2015, s. 56). Samtidig kan det gi enklere tilgang på informasjon. Selv om man selv ikke har god kjennskap eller kunnskap til et tema, er det «alltid» noen andre som har det. Relasjoner på arbeidsplassen kan igjen bidra til økt åpenhet (D. I. Jacobsen, 2015, s. 56). Likevel skal en være forsiktig med denne tilnærmingen og svært bevisst hvilke ulemper dette også kan medføre. Van Hecke (2007) kaller dette for «blinde flekker», som betyr at en som studerer eget virke eller egen organisasjon kan komme i fare for å bli forutinntatt (Van Hecke, 2007 I D. I. Jacobsen, 2015, p. 57). Det å tro at oppgavens innhold ikke utfordres av kognitive bias er vanskelig å se for seg at ikke forekommer, slik vil det trolig også alltid være. Å forholde seg 100% objektiv går ikke, fordi det er forskeren som i stor grad velger tema, problemstilling, design og så videre. Valgene tas selvfølgelig på bakgrunn av interesse og nysgjerrighet, å studere noe man ikke brenner for virker trolig mot sin hensikt og gjør mest sannsynlig forskningen mindre god.

Denne oppgaven har på ingen måte en ambisjon om å bevise at noe er galt i Forsvaret eller å ramme enkeltpersoner. Den søker å beskrive og forklare to fenomen som anses å være avgjørende viktig for hvordan militære kapabiliteter og styrker kan anvendes og hvordan dagens operasjonsmiljø påvirker krigføringens karakter. Den søker å bidra med kunnskap, forståelse og kompetanse om cyberdomenet.

4 Drøfting

«In order to prepare for and conduct complex and multidimensional operations, it is necessary to conduct operations planning to develop appropriately detailed operations plans, which address all relevant factors for the efficient and successful conduct of an operation» (NATO, 2021, s. 1-7).

Oppgaven har til nå beskrevet og forklart hva operasjonskunst og cyberdomenet er og hvordan de kan forstås i rammen av militære operasjoner. Forankringen av dette er primært gjort gjennom militærteoretiske perspektiver og førende doktriner.
Videre vil oppgaven drøfte hvordan operasjonskunsten, sett i lys av de åtte fellesfunksjonene: kommando og kontroll, manøver, ild, etterretning, informasjon, understøttelse, beskyttelse og sivilt-militær samarbeid, påvirkes av cyberdomenet.
Fellesfunksjonene opptrer på ingen måte i isolasjon, men i symbiose. Likevel vil oppgaven søke å se den enkelte funksjon mest mulig isolert for å best kunne beskrive og forklare hvordan cyberdomenet påvirker utøvelsen av operasjonskunsten.

4.1 Kommando og kontroll (K2)

NATO sier at en effektiv K2 struktur er nødvendig i forbindelse med planlegging, gjennomføring og ledelse av cyberoperasjoner (NATO, 2020a, s. 9). Gitt domenets strategiske betydning og globale utstrekning kan det påstås at cyberdomenet er med på å utfordre og endrer måten vi både tenker og fører krig på. Det norske Forsvarets baserer sin utøvelse av kommando og kontroll på oppdragsbasert ledelse (OBL) (Forsvarsstaben, 2019, s. 178). Men er OBL en egnet ledelsesfilosofi for å gjennomføre cyberoperasjoner, gitt domenets karakter?

Situasjonsforståelse er avgjørende for å understøtte effektiv kommando og kontroll av militære operasjoner. Fordi hurtighet og tempo i beslutningssyklusen er betydningsfullt for utfallet av en handling. FFOD (2019) poengterer en viktig faktor som er mer fremtredende i cyberdomenet enn noe annet sted og som i stor grad påvirker måten vi utøver kommando og kontroll på. Nemlig det at «...trusselen er omfattende allerede i fredstid og kan utgjøre en betydelig risiko for styrkene og lederskapet» (Forsvarsstaben, 2019, s. 130). Dette betyr at selv om en ikke er i krig, kan forberedelsene allerede være i gang og operasjonsmiljøet formes slik at dersom en situasjon skulle oppstå og eskalere kan det allerede være etablert en potensiell fordel hos en motstander. Eller så kan krigen allerede være iverksatt, vi bare vet ikke om det ennå. Fordi vi hverken ser, hører eller føler den. Situasjonsforståelsen etableres gjennom informasjon og kunnskap om og i operasjonsområdet og øvrige interesseområder, noe som underbeygger behovet for definerte interesse- og ansvarsområdet

også i cyberdomenet. En slik dimensjon utfordrer utøvelsen av operasjonskunst både i tid og rom. Felles situasjonsforståelse etableres på tvers av domenene og er med på å danne sjefers beslutningsgrunnlag. Cyberdomenet muliggjør asymetriske virkemidler og utfordrer samtidig oppfatningen av konfliktspekteret, noe aktører søker å utnytte i utstakt grad.
Cyberdomenet bidrar videre til at gråsoneproblematikken kan være med på å utfordre gjeldende ledelsesfilosofier i NATO. Det norske Forsvaret har valgt oppdragsbasert ledelse (OBL) som sin ledelsesfilosofi (Forsvaret, 2020). NATO og USA utøver mission command (NATO, 2017a, s. 5-1; U.S.Army, 2019, s. 1-3). Mission command er i utgangspunktet det samme som oppdragsbasert ledelse (Forsvaret, 2020, s. 13). Felles for filosofiene er at de stammer fra det tyske *Auftragstaktik,* som var en sentral del av *Blitzkrieg* og som er kjernen i utøvelse av manøverkrigføring (Conti & Raymond, 2017, s. 90). Hvor desentralisering, initiativ, handlefrihet og ansvar er viktige prinsipper (Forsvaret, 2020, s. 8). Gitt cyberoperasjoner strategiske karakter kan det argumenteres for at en annen ledelsesfilosofi kan være bedre egnet for både styring og ledelse av slike operasjoner. Forsvarets fellesoperative doktrine sier at «Grunnet domenes spesielle og strategiske karakter skal offensive cyberoperasjoner alltid være godkjent på strategisk nivå» (Forsvarsstaben, 2019, s. 131). En føring som kan minne mer om noe tatt ut fra en ordrebasert ledelsesfilosofi[26] enn fra OBL. Men det er det ikke.

En oppfatning av at mission command eller oppdragsbasert ledelse ikke legger til rette for ordrestyrt ledelse er feil. En viktig presisering her er forskjellen mellom ordrestyrt ledelse og ordrebasert ledelse. Ordrebasert ledelse er en egen ledelsesfilosofi som til forskjell fra oppdragsbasert ledelse vektlegger sentralisering, streng disiplin, lydighet og stor grad av føyelighet (Ben-Shalom & Shamir, 2011, s. 102). Ordrestyrt ledelse er på sin side en del av oppdragsbasert ledelse og i så måte situasjonsavhengig (Forsvaret, 2020, s. 8).

Oppdragsbasert ledelse består av både intensjonsbasert ledelse og ordrestyrt ledelse Dette skaper handlefrihet i utøvelsen av lederskap og er representerer ikke bare en filosofi, men også et langt mer positivt og riktig menneskesyn, i hvertfall i vår del av verden. Likevel er det rimelig å anta at midler og systemer som gir økt mulighet for kommando og kontroll vil utnyttes på en eller annen måte. For som Høiback og van Loon (2012) sier: «Det er liten grunn til å tro at politiske myndigheter og militære sjefer vil la vær å bruke sin 10.000 km lange skrutrekker når teknologien åpner for at de kan gjøre nettopp det (H Høiback & van Loon, 2012, s. 354). Fordelen i vår filosofi ligger likevel i at

[26] Også kjent som Detailed Command eller Command by Veto I NATO. Der Auftragstaktik er ekvivalenten til oppdragsbasert ledelse er Befhelstaktik det samme som ordrebasert ledelse.

dersom vår avhengighet av teknologiske midler for å kommunisere og utveksle informasjon skulle forsvinne, har vi fortsatt et grunnlag for at både evnen og viljen til å fortsette er til stede, selv om graden av kontroll svekkes.

Cyberdomenet styres ikke utelukkende av mennesker, det gjøres i en kombinasjon med maskiner og nettverk. Så hva nå og hva betyr dette for operasjonskunsten? Både mennesker og maskiner kan ta beslutninger, men kun menneskene møter konsekvensene. Conti og Raymond (2017) beskriver fire ulike modeller som forklare K2-relasjoner som er direkte overførbare mot cyberdomenet (Conti & Raymond, 2017, s. 218-224):

1) Den første kaller de menneske til menneske (H[27]2H). Mennesker har alltid ført kommando over andre mennesker i militære operasjoner (Conti & Raymond, 2017, s. 218). En generell oppfatning er likevel at teknologisk utvikling har bidratt til økt grad av situasjonsforståelse på alle nivå i organisasjonen, noe som utelukkende er positivt. På den annen siden kan dette ifølge Gundersen 2015 også bidra til at sjefer har mulighet til å detaljstyre operasjoner over store distanser som bidrar til økt kontrollbehov oppover i systemet (Gundersen, 2015, s. 236). Politisk og strategisk sensitivitet kan være en bakgrunn for dette, samtidig som det å bare ha muligheten også er en grunn, men hvor på ledelsesfilosofiskalaen befinner vi oss da? Uavhengig av dette er det fortsatt mennesket som fører kommando og kontroll.

2) Den andre omtales som menneske til maskin (H2M[28]). Dette er heller ikke noe nytt. Fjernstyring av datamaskiner, droner og satellitter er eksempler på dette. På denne måten opprettholde mennesket fortsatt både kommando og kontroll.

3) Den tredje er motsatt av den forrige og innebærer at maskiner også kan lede menneske (M2H). Eksempler på dette er GPS signaler som på egenhånd forteller deg hvor du er og om nødvendig også leder deg dit du skal. Teknologi kan manipuleres eller forstyrres og vil derfor kunne utnyttes av en motstander eksempelvis som et villedende tiltak.

4) Den fjerde og siste, og kanskje minst utforskede er maskiner som leder maskiner (M2M). I dette tilfellet er det snakk om uavhengige og fullautonome systemer som på egenhånd utfører oppdrag. Eksempelvis en autopilot i et fly eller en dronesverm (Ignatius, 2016 I Conti & Raymond, 2017, s. 218).

[27] H: Human
[28] M: Machine

I tillegg til å være beskrivende for hvordan kommando og kontroll har utviklet seg gjennom historien i takt med teknologien kan modellen også brukes for å bevisstgjøre oss viktigheten av å ikke slippe kontrollen. Fordi hvis vi kommer til en situasjon der det fjerde forholdet (M2M) er realiteten har vi trolig begrensede muligheter til å reversere handlingene. Et slikt forhold krever at systemene er autonome og er ifølge Conti og Raymond ikke lurt, fordi «The more intelligent system become, the more difficult they will be to controle» (Conti & Raymond, 2017, s. 221). Likevel er det denne retningen man går i. Den amerikanske Hæren sier at slike system er fremtiden og vil bli mer og mer vanlig (TRADOC, 2017, s. 14). Dette betyr at vi må utvikle løsninger som har til hensikt å ivareta kontrollfunksjonen. Samtidig som vi skal tilegne oss kunnskap og kompetanse til å utvikle og anvende teknologi som gir oss fordeler opp imot en motstander. Oppdragsbasert ledelse er derfor fullt ut appliserbart også for bruk under planlegging, gjennomføring og ledelse av cyberoperasjoner. Men, det må være en bevissthet om at maskiner pr tid ikke har fri vilje eller samme evne som mennesker til nødvendigvis å tenke rasjonelt, den gjør jo bare som den blir fortalt. Fordi cyberdomenet er tross alt et menneskeskapt domene. Likevel tilsier teknologisk utvikling at et scenario hvor maskiner tenker selv[29] og kan erstatte mennesker ikke er utenkelig også hva angår evnen til å vurdere og handle på bakgrunn av en situasjonsforståelse og ikke bare fordi den gjør slik den har blitt fortalt.

Det å ha en fullverdig og godt integrert ledelsesfilosofi er viktig. Vel så viktig er muligheten og begrensingene cyberdomenet gir i utøvelsen av kommando og kontroll. På denne måten vil et K2-design kunne være med på å optimalisere utøvelse av operasjonskunsten ved at det på den ene siden planlegges for hvordan operasjonene på best mulig måte kan understøttes av effektive kommando, kontroll og informasjonssystemer (K2iS). Altså, hvordan muliggjøres samhandlingen best ved å tilrettelegge for og beskytte kommunikasjons- og informasjonsutvekslingen. På den annen side kan en planlegge med hvordan en oppnår tilstrekkelig understøttelse av operasjonene. Hvor en planlegger for og tar risiko med at muligheten for kommunikasjonen og situasjonsforståelse kan og vil bli degradert på en eller annen måte. I en slik situasjon er en prisgitt en oppdragsbasert ledelsesfilosofi, da operasjonene vil fortsette med bakgrunn i sjefens intensjon, slik filosofien legger til rette for (Forsvaret, 2020, s. 8). Avveiningene her ligger i tid, rom og ressursers tilgjengelig opp imot den fiendtlige vurderingen. På denne måten kan det besluttes om det vil være hensiktsmessig å enten endre egen K2 struktur eller om den må sikres i større grad for å redusere svakheter og sårbarheter.

Operasjonskusten vokste som kjent frem i mellomkrigstiden og som et resultat av at militære operasjoner ble alt mer komplekse i sin karakter og operasjonsmiljøet ekspanderte. Flere nasjoner mestret ikke denne kompleksiteten og tapte derfor kriger. Kommando og kontroll er i denne

[29] Kunstig intelligens (Artificial Intelligence – AI)

sammenheng avgjørende. Militære organisasjoner har både før og senere blitt tvunget til å tilpasse seg og utnyttet utviklingen innen den vitenskapelige delen av krigføring for å opprettholde et fortrinn overfor sine motstandere i utøvelsen av operasjonskunsten. Teknologien muliggjør sjefers evne både til å nå lengre og hurtigere i- og utenfor et operasjonsområde, samtidig som at den er med på å utfordre konfliktspekteret og oppfattelsen av krig. Likevel er vi fortsatt bundet til at hurtigheten først og fremst ligger i sjefers evne for å ta beslutninger basert på rådende situasjonsforståelse (Conti & Raymond, 2017, s. 215). Cyberdomenet påvirker utøvelsen av operasjonskunsten i denne sammenheng på den måten at det er et forsterkende middel for opprettholdelse av situasjonsforståelse og utøvelse av kommando og kontroll, samtidig som det også gjør det mer sårbar. Begrensningen ligger nødvendigvis ikke i teknologien, men i hvordan, av hvem og i hvilken grad den utnyttes.

4.2 Manøver

Militære doktriner omtaler manøver som en avgjørende handling. US Army omtaler i sin Multi Domain Operations doktrine viktigheten av å utnytte manøverrom for å nå strategiske og operasjonelle målsettinger, slik at politisk sluttilstand kan oppnås (TRADOC, 2018, s. viii). NATO på sin side har til hensikt å utmanøvrere fienden. Dette søkes oppnådd gjennom å splitte samhold og samhandling slik at motstanderens kapabiliteter ikke oppnår ønskede effekter og målsettinger (NATO, 2019a, s. 1-21). FFOD 2019 er ikke like tydelig og eksplisitt som de to andre nevnte doktrinene. I stedet for å omtale militære aktiviteter og handlinger som manøver, sier den at «motstanderen skal bringes i en situasjon der han ser seg bedre tjent med å avbryte striden enn med fortsatt å yte motstand» (Forsvarsstaben, 2019, s. 53). Implisitt sier også FFOD at hensikten er å manøvrere på en slik måte at fienden enten gir opp eller blir slått, noe som gjør at manøverteorien om viljens relevans skinner tydelig gjennom.

Det å manøvrere i cyberdomenet er i teorien ikke ulikt det å manøvrere i de fysiske domenene. Alt vi gjør er en manøver fordi det har til hensikt å gi en fordelaktig posisjon som enten på kort eller lang sikt vil gagne oss (NATO, 2020a, s. 8). Det betyr at vi planlegger med faktorer som vil påvirke vårt oppdrag i de ulike domenene, samtidig som vi også analyserer hvordan vi forventer at en motstander vil utnytte sine ressurser mot våre styrker for å løse sine oppdrag og nå sine målsettinger. Likevel er det noen karakteristika ved cyberdomenet som skiller seg fra de fysiske domene. Faktorer som i stor grad vil påvirke planlegging og utfordre tradisjonelle tanker om krigføring og manøver. Spesielt tid og rom, men også styrke-dimensjonen vil kunne oppleves annerledes annerledes.

Tid og rom er universelle faktorer som påvirker alle aspekter av krigføringen. Den teknologiske og industriell utviklingen de siste to-hundrede år har i stor grad påvirket krig i en retning som har gjort den mer dynamisk og langt mer uforutsigbar. Dette tvinger også profesjonutøvere til å endre

oppfatning av hvordan operasjoner planlegges, gjennomføres og ledes. Bruce Menning (2013) sier i forordet til sin oversettelse av Issersons - *The Evolution of Operational Art* at det var troen på en rask og avgjørende seier som førte til at 1. Verdenskrig endte i en fire år lang utmattelseskrig (Menning, 2013 IIsserson, 1932/1936/2013, s. ix). Krigens karakter endret seg raskt med bakgrunn i teknologisk utvikling, noe generalene derimot ikke hadde klart å tilpsse seg.

I de fysiske domenene har infrastruktur som jernbaner, veier, havner, flyplasser og industri hele tiden vært med på å utvikle krigføring og utfordre tid og rom perspektivet. I det ikke-fysiske domene er det nettverk og systemer som skaper muligheter. Muligheten til å forflytte styrker hurtigere og over lengre og lengre avstander har vært med på å utvide operasjonsområder og derav også endre operasjonsmiljøet. I dag kan effekter potensielt oppnås uten forflytning av styrker, men kun ved hjelp av noen tastetrykk (NATO, 2020a, s. 8). Samtidig som at cyberdomenets globale utstrekning tilfører krigføringen enda en dimensjon. Cyberdomenet har på denne måten bidratt til at operasjonsmiljøet har ekspandert ytterligere. Manøverrommet har med dette blitt utvidet.

Den teknologiske utvikling har bidratt til at systemer, nettverk og maskiner kontinuerlig øker sin globale rekkevidde. I dokumentaren, *The Social Dilemma*, sier Randima Fernando at datamaskiners prosesseringsevne har økt med ca 1 billion siden 1960-tallet. Ingenting annet i verden er i nærheten av å ha en tilsvarende utvikling (Orlowski, 2020). Denne påstanden underbygges av Joseph Nye som sier at bakgrunnen for vår evne til å håndtere og behandle all informasjonen vi har tilgang til skyldes at datakraften i snitt har doblet seg hver 18. måned de siste 30 år (Nye, 2011, s. 114). Det Fernando og Nye egentlig referer til her er Moore´s lov[30]. Samtidig er det viktig å tenke på at selv om cyberdomenet gir oss muligheten til å utfordre tidsaspektet på nye måter hjelper det lite hvis det ikke utnyttes på riktig måte. Ja, teknologien gir oss muligheten til å nå en brannmur på andre siden av jordkloden innen millisekunder, men hvis du ikke kommer gjennom sperringen eller vet hvordan du skal utnytte tilgangen er en like langt. Posisjonering og disponering av egne ressurser er like avgjørende her som forberedelsene til en hvilke som helst annen operasjon. Samtidig kan det svært tidkrevende å finne svakhetene som kan utnyttes.
Forutsatt at vi nå har muligheten til å passere brannmuren og etablert et brohode oppstår nye dilemmaer med hensyn til tid. På den ene siden kan vi vente. Fordelen med dette er at risikoen for å bli oppdaget reduseres. Det at man står på utsiden, gjør at sannsynligheten for å bli oppdaget er mindre, samtidig som det gir tid til å finne den beste veien inn. Likevel vil dette også bety økt risiko for den

[30] Moore´s lov: Moores lov handlet først om økonomi. Den sier at det mest økonomiske antall transistorer som kan integreres i en brikke fordobles hver 24.måned [opprinnelig hver 12.mnd]. Det er ikke en lov, men en prediksjon basert på observasjon som Gordon E. Moore gjorde i 1965 og som ble verifisert i 1975. I 1975 ble tiden endret til 24.måeder på grunn av teknologiske endringer (Store Norsk Leksikon, 2015).

som ønsker tilgang gjennom at muligheten som nå har oppstått forsvinner fordi «terrenget» i cyberdomenet kan endre seg fort gjennom at den svakheten som lå åpen for å bli utnyttet blir avdekket og feilrettinger finner sted (som eksempelvis i et virusprogram eller operativsystem oppdatering). På den annen siden kan vi ta risikoen og gå inn så fort som mulig, da i den vissheten om at vi kan oppdages og på denne måten også miste muligheten vi har fått eller tatt. Samtidig som at attribusjon kan bli enklere dersom angriperen oppdages når handlingen gjennomføres. Dette tilsier at planlegging, gjennomføring og ledelse av cyberoperasjoner krever stor grad av situasjonsforståelse, oppmerksomhet og fokus, er tidkrevende, samtidig som det stiller store krav til kunnskap og kompetanse om cyberdomenet.

Cyberdomenets globale rekkevidde gjør at manøvermuligheten gjennom domenet er stor. Forutsetningen er selvfølgelig at det som skal nås er tilkoblet et nettverk slik at det er mulig å etablere tilgang, eller er det slik?
For å kunne gjennomføre et cyberangrep er man avhengig av tilgang på det en skal manøvrer mot eller til. De fysiske domenene har her, til forskjell fra cyberdomenet den fordelen av at det i liten grad endres. Terrenget på land, på sjøen eller i luften forblir tilnærmet konstant. Aktiv bruk av hinder og sperringer vil selvfølgelig kunne begrense en motstander, men ikke nødvendigvis nekte tilgang. Derimot skjer det endringer i cyberdomenet konstant (Conti & Raymond, 2017, s. 85). Dette på grunn av den hurtige utviklingen på teknologisk side. Conti og Raymond sier at terrenget i cyberdomenet kontinuerlig vil kunne endre seg siden domene er menneskeskapt og finner sted i en jungel av maskiner og nettverk (Conti & Raymond, 2017, s. 88). En begrensningen kan selvfølgelig være at noe eller noen ikke er koblet i et nettverk, som betyr at målet i utgangspunktet er utenfor rekkevidde. Dette kan forstås som den operasjonelle rekkevidden, hvor tilknytningen i nettverk er muligheten og/eller begrensningen (Conti & Raymond, 2017, s. 116). Likevel vil det som ikke er tilstede i cyberdomenet ha en form for fysisk tilstedeværelse, et fysisk lag, slik at muligheten for å nå målet fortsatt vil være der selv om det er utilgjengelig i deler av cyberdomenet. Synergien mellom domenene er derfor avgjørende for å hurtig kunne tilpasse og endre egen manøver. Operasjon Olympic Games, cyberangrepet mot det iranske atomprogrammet med dataormen Stuxnet[31], er et godt eksempel på hvordan en cyberoperasjon mot et lukket nettverk kan gjennomføres.

[31]Stuxnet er et av de mest kjente cyberangrepene som noen gang er blitt gjennomført. Angrepet fant sted i Natanz i Iran i år 2010 og hadde som mål å ramme det iranske atomprogrammet ved å bryte ned og ødelegge atomsentrifuger. Stuxnet er den første registrerte dataormen (worm) og klarte å penetrere et lukket nettverk, utenfor rekkevidden av internett eller andre digitale systemer. Angrepet fant sted i det logiske laget i cyberdomenet og klarte over tid å bryte ned og ødelegge styringssystemene som monitorerte og kontrollerte sentrifugene, ved å gi systemet kommandoer som gjorde at sentrifugene sakte men sikkert brøt seg selv ned. I tillegg var Stuxnet designet slik at den skjulte egne spor i systemene. Dataormen fikk mest sannsynlig tilgang til det lukkede nettverket gjennom infiserte minnepinner. Stuxnet ble designet til å utnytte svakheter og sårbarheter i systemets operativsystem (Libicki, 2016, s. 14-18).

Operasjoner i det fysiske domenet kan øke vår sårbarhet i cyberdomenet. I et scenario hvor Norge blir angrepet og vi må forsvare oss fra øst mot vest i Finnmark vil mye av vår kommunikasjonsinfrastruktur, både sivil og militær, eksponeres for motstanderen ettersom terreng oppgis eller tapes. Dette tilsier at cyberoperasjoner også vil ha en avgjørende rolle i en defensiv manøveroperasjon. En kontrollert nøytralisering av cyberdomenet vil være nødvendig, dersom det ikke skal kunne utnyttes av motstanderen. Dette kan gjøres enten ved å fysisk ødelegge materiell og utstyr som muliggjør forbindelser i cyberdomenet, eller at man gjennom cyberdomenet stenger ned og nøytraliserer nettverk og utstyr. På den annen side kan de samme nettverkene forbli tilgjengelige for motstanderen. I stede for å stenge ned nettverkene eller ødelegge de kan de manipuleres slik at de kan utnyttes i forbindelse med informasjons- og påvirkningsoperasjoner, samtidig som egne styrker kan opprettholde en form av kontroll i det logiske nettverket. Uavhengig av handlemåte vil slike operasjoner på tvers av domenene kreve tett koordinering og synkronisering i tid og rom.

Selv om cyberdomenet ikke har definerte grenser, slik det fysiske domene har, må domenet avgrenses. Area of Interest (AOI) og Area of Responsibility (AOR) er velkjente begrep for å definere militære operasjonsområder og vil kunne være like anvendbare for cyberdomene. Viktigheten her ligger i at vi for det første må etablere et felles begrepsapparat som fundament for kunnskap og forståelse. Fordi forskjeller i hvordan noe omtales og forstås er med på å begrense mer enn det vil utnytte bruken av en kapabilitet eller kapasitet. Selvfølgelig er det eksperter som både designer og utfører oppdragene, men de planlegges, gjennomføres og ledes i rammen av fellesoperasjoner enten på operasjonelt eller strategisk nivå. Dette betyr at operative sjefer må kunne forstå hva de beslutter og på hvilket grunnlag en avgjørelse tas. Samtidig er det viktig å huske at store deler av cyberdomenet ikke er militært, noe som medfører at andre etater og organisasjoner har store interesser innenfor potensielt det samme operasjonsområdet som oss (Crowther, 2017, s. 74). Utfordringen ligger samtidig i at hele cyberdomenet i utgangspunktet er en del av operasjonsområdet. I norsk sammenheng er det Cyberforsvaret som beskytter Forsvarets nettverk og systemer, hvorpå Etterretningstjenesten utfører offensive cyberoperasjoner, både i og utenfor det militære nettverk (Forsvarsstaben, 2019, s. 125). Samtidig kan militære styrker også være avhengig av sivil kommunikasjonsinfrastruktur for å operere egne systemer. I en totalforsvarssammenheng viser dette viktigheten av samarbeid på tvers av sektorer og behovet for en tydelig definering av ansvarsområder, også i cyberdomenet.

En annen distinksjon er det menneskelige aspektet om fysisk tilstedeværelse i strid. I en tradisjonell militær manøveroperasjon er man i stor grad avhengig av fysisk tilstedeværelse. Forvirring, skjul og dekke er alle metoder som militære styrker bruker for å redusere sannsynligheten for å bli oppdaget og øke egen handlefrihet. Derigjennom reduseres samtidig risikoen forbundet med oppdraget eller

operasjonen og risikoen overfor egne styrker[32]. Men risikoen kan på sin side reduseres til det minimale gjennom utnyttelse av cyberdomenet ved at svært få soldater i det hele tatt må deployeres inn i et operasjonsområde. Gitt rekkevidden og mulighetene cyberdomenet gir kan altså defensive- så vel som offensive oppgaver tidvis erstatte menneskelig kampkraft. NATOs cyberspacedoktrine sier at cyberoperasjoner har potensial til å bidra til operasjonell måloppnåelse uten å fysisk deployere styrker inn i et operasjonsområde (NATO, 2020a, s. 8). På denne måten evner man å påvirke motstanderens evne og vilje gjennom å utnytte cyberdomenet for å nå samme målsetting, men med andre midler, noe Stuxnet er et godt eksempel på.

Dynamikken og endringsmulighetene i cyberdomenet utfordrer hvordan manøver oppfattes og kan forstås. Manøvrering i cyberdomenet kan forstås på den tradisjonelle måten som i det fysiske domene, hvor det å kontrollere deler av domenet er effekten i seg selv (NATO, 2020a, s. 1). En annen oppfatning kan være at cyberdomenet forstås som det nye og ukjente terrenget som det er, hvor effekten av å eie narrativet er vel så viktig som fysisk kontroll (NATO, 2020a, s. 1). For selv om det kan forstås i tradisjonell forstand bør militære profesjonutøvere i stede for å tilpasse sin oppfatning av cyberdomenet til tradisjonell militær tenkning tilpasse seg cyberdomenets muligheter og begrensninger som vil utfordre det tradisjonelle og styrke vår evne for utøvelsen av operasjonskunst. Eller som Paul J. Springer sier: «To ensure success, the conduct of war requires rapid and effective adaption to changing circumstances (Springer, 2016 I Libicki, 2016). Denne måten å tilpasse seg operasjonsmiljøet vil trolig også være formålstjenlig med tanke på at krigføring handler like mye eller mer om vilje enn om fysisk ødeleggelse og kontroll, som er i tråd med Brezins (2014) sin påstand om at striden foregår i bevisstheten. For tilpasning handler utelukkende om vilje. Selv om sammenhengen mellom de to kan argumenteres for å være tett, er det viktig å huske på at cyberdomenet er svært ungt og ifølge Conti og Raymond er militære doktriner for cyberoperasjoner fortsatt umodne (Conti & Raymond, 2017, s. 11). En påstand som støttes. Samtidig sier de at tradisjonell militærteori er velutprøvd og har i stor grad overlevd tidens tann og på denne måten fremstår moden. Det betyr likevel ikke at det er allmenngyldig, men at prinsippene kan være det og at utgangspunktet for videre utvikling er godt.

Hensikten med manøvrering og manøverkrigføring er vel forankret i manøverteorien og handler om å tilrive seg initiativet gjennom å opprettholde et relativt høyere tempo enn det motstanderen har eller klarer å gjøre. Initiativet kan tas gjennom å overraske fienden på en slik måte at han starter på bakbena og havner i ubalanse. John Boyd beskrev dette som å komme innenfor motstanderens

[32] Risk to Force – Risk to Mission er en egen analyse som gjøres i forbindelse med planlegging av operasjoner.

beslutningssyklus[33] (Boyd, 1986). I tillegg til at dette har en fysisk dimensjon er den psykologiske dimensjonen like viktig i manøverteorien, der kampen om viljene er det sentrale.

Overraskelse er en måte å tilrive seg initiativet på og kan synes enklere å oppnå i cyberdomenet enn i de fysiske domenene. Dette fordi at muligheten for å skjule seg, eksempelvis gjennom å utgi seg for å være noe annet enn det man er eller ved å «være en i mengden» uten å avsløre egne hensikter er stor. Initiativet kan samtidig tilrives gjennom enten å utnytte tilgjengelige kapabiliteter og kapasiteter på en slik måte at synergien av egne fellesfunksjoner blir større enn motstanderens. Den siste kan syntes vanskeligere og mer utfordrende i cyberdomenet gitt muligheten motstanderen har til å endre terrenget til egen fordel, ikke bare det å utnytte det til egen fordel som i de fysiske domene. Samtidig som utbredelsen av cyberdomenet kan gjøre «lendeorienteringen» mer utfordrende og derfor det å planlegge for vanskeligere og mer tidkrevende, gitt endringer i og utbredelsen av domenet. Men egen hensikt og vilje kan likevel enklere skjules, gitt at attribusjon fortsetter å være langt mer utfordrende i det ikke-fysiske domenet.

Manøver som fellesfunksjon er avgjørende for å drive krigføring. Dette gjelder like mye i det ikke-fysiske domene som i de fysiske. De andre fellesfunksjonene vil både tilrettelegge for- og understøtte manøvrering i operasjonsområdet, men manøver i cyberdomenet forutsetter tilgang til det [et] logiske-lag. På denne bakgrunn kan det argumenteres for at cyberdomenet stiller nye krav til hvordan operasjonskunsten utøves i militære fellesoperasjoner. Det stiller ikke bare krav til teknisk kunnskap og kompetanse, men også i stor grad faglig innsikt og forståelse for hvordan cyberdomenet kan utnyttes for å manøvrere i utvidet og mindre avgrenset operasjonsområde. Faktorene tid, rom og styrker er tidløse, men gis likevel utvidet betydning. Cyberdomenet påvirker operasjonskunsten gjennom at operasjonsmiljøet og manøverrommet utvides som potensielt gjør planlegging, gjennomføring og ledelse av militære operasjoner mer komplekst.

4.3 Ild

Cyberdomenet muliggjør samhandlingen mellom sensorer, effektorer og beslutningstakere. Ild handler om å utnytte tilgjengelige effektorer, både dødelige og ikke-dødelige, på en mest mulig fordelaktig måte. NATO sier at cyberoperasjoner er et viktig virkemiddel i den forstand at det har stor rekkevidde og hurtig kan levere effekter innen et bredt spektrum[34], noe som gir sjefer stor handlefrihet (NATO, 2020a, s. 8). For å drive effektiv målbekjempning er en avhengig av grundig og god etterretning, samtidig som informasjon effektivt kan distribueres i- og gjennom det ikke-fysiske domene, slik at

[33] Boyd refererte til beslutningssyklusen som OODA-Loop: Observe, Orient, Decide, Act.
[34] Cyberoperasjoner kan levere både psykologiske, logiske og fysiske effekter (NATO, 2020a, s. 8)

tidsriktige beslutninger kan tas. I tillegg fasiliterer manøver for at effekten kan leveres på rett sted til rett tid. For utøvelse av operasjonskunsten betyr cyberdomenet nye metoder og midler for både å utnytte, levere og oppnå effekter på.

Selv om ilden har evne til å påvirke en fiende eller motstander både fysisk og psykologisk har den lite til ingen hensikt dersom den ikke bygger opp under en høyere målsetting. Clausewitz sa at teknologien drev mennesket til å sloss mer effektivt. Samtidig sa han at våpen i seg selv ikke er essensielt for krig som konsept, da det også finnes andre former for handlinger som kan påvirke en motstander like effektivt (Clausewitz, 1984, s. 2). Cyberdomenet er i seg selv ikke et våpen, men det gir flere muligheter til å drive effektiv og målrettet påvirkning, samtidig som det er i stand til å levere våpen som ødelegger fysisk infrastruktur.
Cyberdomenet er blant annet svært sentralt i måten Russland og Kina driver sine informasjonsoperasjoner, både internt og eksternt , som en del av sin asymmetriske krigføring (Grzegorzewski & Marsh, 2021). Dette viser at kampen om narrativet allerede pågår i cyberdomenet og den primært føres fra det politiske og strategiske nivået. Dette er trolig grunnen for at maktprojeksjon er en del av definisjonen for offensive cyberoperasjoner.

Cyberoperasjoner kan ikke gjennomføres uten tilgang til et logisk lag. Dette gjelder både i defensive- så vel som offensive operasjoner. Gjennom det logiske laget får en tilgang til software, protokoller, nettverk, nettsteder, applikasjoner eller styringssystemer. Det er disse områdene som er målene og som cyberoperasjoner har til hensikt å manøvrere i og mot for å kunne ramme. Det logiske laget utgjøre selve forsvars- og angrepsflaten i cyberdomenet. Samtidig er det viktig å tenke på at det fysiske laget muliggjør etablering og drift av det logiske laget gjennom og mellom enheter i et nettverk. Disse to lagene er igjen forutsetninger for at personer eller organisasjoner kan opprette virtuelle identiteter som e-mailadresser, kontoer i sosiale medier eller aliaser (NATO, 2020a, s. 4). Symbiosen mellom de tre lagene er helt tydelig, men forutsetningen for cyberoperasjoner er likevel muligheten til å manøvrere i et logisk lag, uavhengig av hvilket lag som skal rammes og hvor effekten søkes oppnådd.

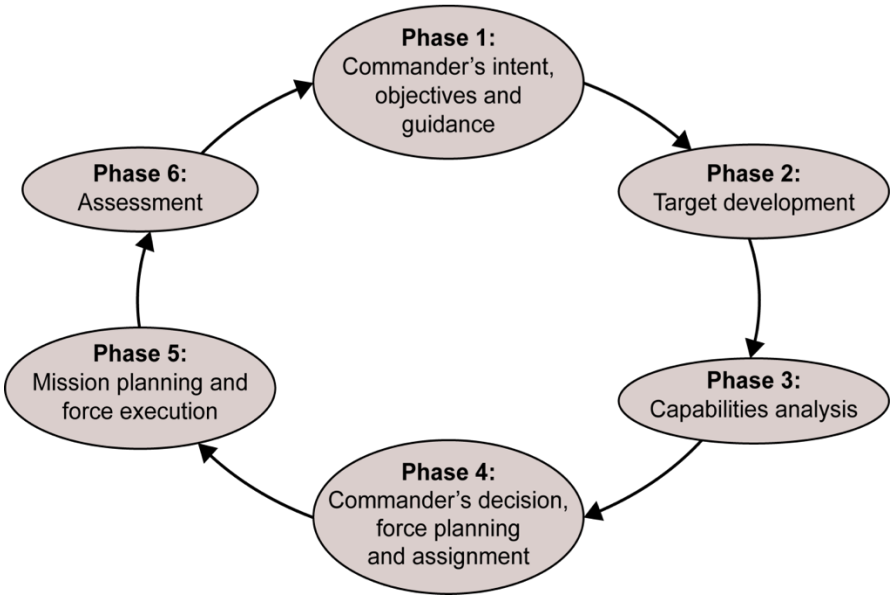
Effektene cyberoperasjoner skaper handler ikke kun om fysisk ødeleggelse. For i hvilke grad kan cyberoperasjoner levere våpen og effekter som skaper fysisk ødeleggelse? Til forskjell fra de kinetiske effektene som oppstår på bakgrunn av effektorer i de fysiske domenene som bomber, granater, kuler og krutt, kan påvirkningen og effektene fra cyberoperasjoner oppfattes mindre dramatiske. Fordi cyberoperasjoner kan eksempelvis som i tilfellet Stuxnet påvirke et styringssystem som gradvis bidro til at atomsentrifugene ble ødelagt, eller det kan ta ut strømnettet i et område, der den fysiske ødeleggelses nødvendigvis ikke fremstår like brutal som ved bruken av andre effektorer. Det kan også være med på å påvirke viljer gjennom eksempelvis å spre feilinformasjon. Som vi så i Georgia i august

2008, hvor russerne stengte ned eller tok kontroll over alt av kommunikasjonsinfrastruktur før de angrep. Dette ble gjort gjennom omfattende dataangrep fra russisk territorium som isolerte Georgia fra omverdenen og Russland kontrollerte krigens narrativ (Karlsen, 2015, s. 292). Eller som ved statskuppet i Myanmar 1.februar 2021 hvor Telenor sitt nett ble stengt ned og derigjennom gav Hæren større grad av kontroll over informasjonsutveksling. Dette viser samtidig den umiddelbare effekten cyberoperasjoner, eller påvirkning av cyberdomenet kan ha og hvor effektivt det kan være. I tillegg til å ramme på den måten en ønsker bidrar også slike angrep til overraskelse, som gir angriper et stort fortrinn. Konsekvensen av dette er ikke nødvendigvis umiddelbare tap av liv, men de operasjonelle, strategiske og politiske ringvirkningene kan derimot bli store. Det kan også påstås at cyberangrep kan skape vel så store fysiske skader ved at det tar ut enheter i det fysiske laget.
Vi vet at moderne kampsystem som stridsvogner, luftvern, stormpanservogner og ledelsesnoder alle belager seg på moderne teknologier. Den norske stormpanservognen (CV9030n) inneholder eksempelvis bort imot 200 IP-adresser og er dermed et høyteknologisk kampsystem som er ment å fungere i et nettverk (Dalløkken, 2014). Samtidig sier dette noe om sårbarheten til slike plattformer, som igjen betyr at fysisk ødeleggelse kan gjennomføres og muliggjøres vet at cyberoperasjoner reduserer eller nøytraliserer en motstanders kampkraft. Disse muligheten gir cyberoperasjoner et større handlingsrom og deres karakter kan med dette også bli langt mer taktiske fremover.

Metodisk målbekjempning[35] er en avgjørende prosess i enhver operasjon. Fordelen med dette er at målbekjempningsprosessen er like anvendbar for å planlegge operasjoner i cyberdomenet som i de fysiske domenene. NATOs doktrine for targeting, AJP-3.9 sier at «Joint targeting provides a methodology that aids decision-making linking objectives with effects through the appropriate prosecution of prioritised targets and the assessment of any effect generated. It is flexible enough to be adapted to any type of operation» (NATO, 2016b, s. 1-4). Denne prosessen består av seks faser (figur 7). De fem første fasene krever tett samarbeid og koordinering på tvers av fellesfunksjonene og oppleves å være like lett eller like vanskelige for de ulike domenene med tanke på hvilke effekter som skal oppnås og hvordan oppdragene skal utføres. Derimot kan det påstås at fase seks, vurdering, vil være den fasen som betyr mest forskjell mellom det fysiske og det ikke-fysiske domene. Siden effektene i- eller fra cyberdomenet ikke nødvendigvis er umiddelbart synlig eller syntes i det hele tatt for egne styrker, slik eksempelvis et kinetisk nedslag kan være. Denne bevisstheten er avgjørende viktig fordi det er en forutsetning spesielt i operasjoner der cyberoperasjoner skal fasilitere for en manøver i et eller flere av de fysiske domene. NATOs cyberdoktrine sier i denne sammenheng at det å vurdere en effekt og skadeomfang kan være vanskeligere i en cyberoperasjon enn i en operasjon utført

[35] Targeting i NATO

med tradisjonelle fysiske midler og metoder (NATO, 2020a, s. 21). Dette medfører risiko og skaper usikkerhet, som vil påvirke utøvelsen av operasjonskunsten.



Figur 7: NATOs targeting-prosess (Joint targeting cycle) (NATO, 2016b, s. 2-2).

Cyberdomenet omslutter ikke bare de andre krigføringsdomene, det inngår og omfatter også de andre maktmidlene stater besitter. I følge den amerikanske hæren vil diplomatiske-, informasjons-, militære- og økonomiske (DIME[36]) midler knyttes enda tettere sammen for å være i stand til både hurtigere og mer effektivt levere DIME-effekter både i den fysiske, psykologiske og moralske dimensjonen (TRADOC, 2017, s. 19). Dette betyr at operasjonskunstens rolle og relevans fortsatt vil være svært viktig fordi politikken og strategien på en måte kan bli mer kompleks, men samtidig også mer integrert i den militære sfæren, på alle nivå. I tillegg vil dette trolig også bety en tettere integrering mellom militære og sivile effekter i og gjennom cyberdomenet.

Bevissthet rundt bruken av cyberdomenet og cyberoperasjoner i rammen av militære operasjoner er viktig fordi det på mange måter har omdefinert og endret hvordan vi kan oppfatte utnyttelsen av ild som fellesfunksjon. Effekten av å angripe det iranske atomprogrammet i 2010, slik Stuxnet gjorde, ville kanskje også vært oppnådd ved å bombe eller sprenge anlegget. Kinetisk ødeleggelse kunne til og med forsinket anrikningen av uran ytterligere. Likevel var Stuxnet et angrep som fysisk ødela atomsentrifugene, det var et angrep som skapte ødeleggelser gjennom det logiske laget. Brukt på denne måten bidrar cyberoperasjoner samtidig til å redusere fysisk skade på personell. Effekten av

[36] DIME – Diplomacy, Information, Military, Economic

militære operasjoner, ses ikke i isolasjon, men i avhengighet med de andre maktmidlene stater disponerer. Grunnlaget for at vi i det hele tatt kan drive metodisk målbekjempning avhenger av grundig etterretning, samt evnen til å levere rett effekt, på rett sted, til rett tid. I denne sammenheng har cyberoperasjoner et enormt potensial fremover som kapabilitet og effektor. I dette ligger dog kjerne i operasjonskunsten, hvor strategiske føringer og målsettinger omsettes til taktiske handlinger. Og så er det viktig å huske på at selv om cyberdomenet er et ikke-fysisk domene, vil effektene det skaper alltid være fysiske i sin form.

4.4 Etterretning

Etterretning en premissleverandør for planlegging, gjennomføring og ledelse av operasjoner. Kunnskapen om operasjonsmiljøet gjennom tilgjengelige data og informasjon identifiseres, vurderes og analyseres og blir til etterretning. Hensikten er å identifisere trusler og samtidig finne muligheter som kan utnyttes i beslutningstaking (NATO, 2016a, s. 3-1). Etterretning bidrar på denne måten til å redusere risiko som gjør at hvordan egne kapabiliteter og kapasiteter disponeres i tid og rom blir best mulig. Dette krever stor grad av samarbeid og integrering mellom de som leder operasjonsplanleggingen og de som leder etterretningsprosessen[37].

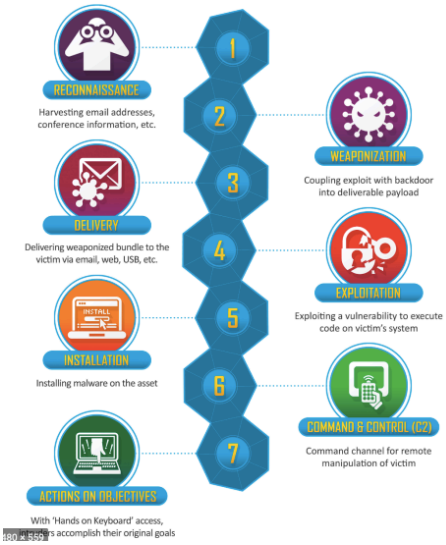
Cyberdomenet egner seg særdeles godt for etterretningsaktiviteter. Etterretning består av flere disipliner[38] som alle har til hensikt å bidra inn mot det å skape en helhetligforståelse av det gjeldende eller et potensielt fremtidig operasjonsmiljø. I en verden hvor muligheten for informasjonsdeling blir større og større, øker også tilfanget av informasjon. Samtidig som at fler og fler av verdens befolkning har muligheten til å koble seg på internett gjør dette også at tilfanget og tilgangen til informasjon om personer, bedrifter og organisasjoner øker. NATO påpeker her at: «Cyberspace is fundamental to the availability and sharing of information and plays a major role, especially in contributing to the intelligence collection disciplines, within a joint mission» (NATO, 2020a, s. 9). Åpne og lukkede nettverk har på denne måten skap et paradis for de som er ute etter informasjon og som har mindre gode hensikter. Majoriteten av etterretningsdisiplinene innretter seg nettopp mot det ikke-fysiske domene. Dette bidrar til å understøtte utøvelse av operasjonskunsten.

[37] Denne prosessen er kjent gjennom ulike navn og betegnelser som Intelligence Preperation of the Battlefield (IPB) og Intelligence Preperation of the Operational Environment (IPOE). NATO bruker IPOE som sin standard, men kaller det Joint Intelligence Preperation of the Operational Environment (JIPOE) (NATO, 2016a).
[38] AJP-2 beskriver følgende disipliner innen etterretning (NATO, 2016a, s. 3-9 - 3-11): Acoustic Intelligence (ACINT) – som er analyse av lyd og lydbilder. Human Intelligence (HUMINT) – har til hensikt å tilegne seg informasjon fra andre mennesker. Dette skjer både i det fysiske og ikke-fysiske domene. Imagery Intelligence (IMINT) – analyserer bilder og video. Signal Intelligence (SIGINT) – handler primært om å utnytte det elektromagnetiske spekteret (EMS). Measurement and Signature Intelligence (MASINT) – innebærer vitenskapelige og teknisk analyse av data i det EMS for å lokalisere en sender eller mottaker. Open Source Intelligence (OSINT) – innebærer å samle inn data fr åpne kilder som alle har tilgang på.

Etterretningsprosessen er overførbar til operasjonsplanlegging også for cyberoperasjoner. Etterretningsprosessen består av fire deler: Styring, innsamling, bearbeiding og fordeling av informasjon (figur 8) (Forsvarsstaben, 2019, s. 141; NATO, 2016b, s. 4-2). Denne prosessen er grunnlaget for den etterretningsmessige planprosessen. Ambisjonen er å dekke et informasjonsbehov uavhengig av domene for å etablere et best mulig beslutningsgrunnlag for den militære sjefen.

Figur 8: Etterretningsprosessen. I midten er Intelligence Requirement Management og Collection Management (IRM/CM), som er avgjørende for å opprettholde kontroll og fremdrift i prosessen (Forsvarsstaben, 2019, s. 141).

Etterretningens avgjørende plass i operasjonsplanlegging fremgår også tydelig i Lockheed Martin sin Cyber Kill Chain (figur 9). Rekognosering er det første steget som skal danne grunnlag for de påfølgende stegene og den avgjørende handlingen mot målet i steg syv, hvor påvirkning iverksettes. Steg 1 i Cyber Kill Chain kan derfor sammenlignes med etterretningsprosessen, mens de øvrige stegene er gjenkjennbare fra targetingprosessen. På lik linje som at denne er gjeldene i et cyberangrep er modellen også anvendbar i forbindelse med defensive cyberoperasjoner. På sikt vil etterretningsoperasjoner ifølge Glenn Crowther bli mer og mer cyber-rettet og metoder for innsamling og analyse vil forbedres (Crowther, 2017, s. 68). Derfor er det ikke urimelig å anta at utviklingen også kan komme til å påvirke måten og metoden vi driver operasjonsplanlegging på i dag. En økende kompleksitet i operasjonsmiljøet må derimot ikke føre til økt kompleksitet i planlegging, forhåpentligvis heller det motsatte.



Figur 9: Cyber Kill Chain (Lockheed Lockeed-Martin, 2020).

Etterretningsprosessen er avhengig av at operasjoner i cyberdomenet avgrenses. Som tidligere nevnt er det hensiktsmessig med både et definert ansvarsområde og interesseområde uavhengig av domene. Siden tilfanget på informasjon i cyberdomenet i dag er monumental bør innhenting fokuseres mot det som er avgjørende for operasjonen som skal gjennomføres eller understøttes. En viktig presisering som gjøres av FFOD (2019) i denne sammenheng er å beskrive forskjellen mellom etterretning og overvåkning. Doktrinen sier at «skillet går i hovedsak på aktivitetens intensjon – hva informasjonen skal brukes til» (Forsvarsstaben, 2019, s. 143). Der overvåkning er ment for å skape et situasjonsbilde og heller kan ses som et tiltak under styrkebeskyttelse fremfor som del av etterretningsprosessen. Denne oppgaven kan utføres av andre militære eller sivile styrker som igjen er med på å danne grunnlag for etterretningen. Etterretningen på sin side utarbeider «...vurderinger av aktørers intensjoner, evner og kapasiteter, taktikk og strategi, og vurdere potensielle trusler» (Forsvarsstaben, 2019, s. 143). Likevel kan felles sensorer brukes for å løse begge typer oppdrag. Dette betyr nødvendigvis ikke en avgrensning i geografi, men en avgrensning i form av nøkkelområder (dedikerte forbindelser og system) i cyberdomenet som understøtter planlegging, gjennomføring og ledelse av operasjonen best mulig. Eksempelvis vi en deteksjon av fiendens intensjon eller interesse i steg 1 av *Cyber Kill Chain* bidra til økt situasjonsforståelse og mulighet for å handle, gjennom at en avgrensning skaper «...grunnlag for prioriteringer av innhenting, bearbeiding og fordeling av etterretninger» (Andreassen, 2015, s. 247). Dette kan minne om akkurat det som gjøres under lendevurderingen i en landoperasjon, hvor viktig lende defineres.

Situasjonsforståelse etableres gjennom grundige og nøyaktige analyser av tilgjengelig informasjon. Korrekt forståelse av informasjonen er avgjørende for å kunne fatte gode og tidsriktige beslutninger. Men det finnes også kilder til at etterretningen enten blir feil eller at den ikke har noen verdi. Med

cyberdomenets fremvekst har tilfanget av informasjon økt betraktelig. Operasjonsmiljøets omfang vokser, som fører til økt kompleksitet. Utfordringen ligger både i det å få tilgang på relevant informasjon (steg 2 - innhenting), men også i det å kunne prosessere og behandle (steg 3 – bearbeiding) all informasjonen slik at den blir nyttig for operasjonsplanleggingen. Begrensningen ligger nok i stor grad i vår, menneskets, kapasitet til å behandle all data, men heldigvis har vi maskiner, databaser og programvarer til å støtte oss.
Cyberdomenet er som uttalt en jungel av nettverk og maskiner som i liten-, noen-, eller større grad opptrer autonomt. Fordelen med lite autonome system er at det alltid er et menneske som sitter bak og styrer det som skjer. Derigjennom kan sannsynligheten for attribusjon øke, samtidig som en fortsatt har muligheten for å bruke metoder og midler for å skjule egen identitet, som ved bruk av mellomstasjoner og fjernstyrte system (Erichsen & Mathisen, 2015, s. 354). Mer autonome system vil inneholde digitale spor, på samme måte som eksperter på eksplosiver kan spore ulike bomber til en spesifikk bombemaker kan også digitalt utstyr og materiell spores, men det kan være vanskelig å bevise. Likevel viser det seg at attribusjon er mulig også mot større organisasjoner og statssystem, som ved angrepet mot Stortinget i august 2020. Med bakgrunn i etterforskning og analyser gjort av norske sikkerhets- og etterretningstjenester kunne utenriksminister Ine Marie Søreide Eriksen gå ut og attribuere angrepet, og si at det var Russland som stod bak.

Informasjon er utgangspunktet for etterretningen. Etterretning er videre grunnlaget for alle militære operasjoner. En Intelligence Preperation of the Operational Environment (IPOE) prosess må derfor iverksettes så tidlig som mulig i en planprosess fordi den er premissleverandør for den operative planen. Cyberoperasjoner vil kunne være en avgjørende og integrert del av denne prosessen. Både med bakgrunn i de fordelene og mulighetene det gir med tanke på innhenting og distribusjon av informasjon, men også bevisstheten rundt begrensningene og sårbarhetene, egne og motstanderens, som finnes ved bruk av cyberdomenet. NATO sier at cyberoperasjoner må inkluderes i egne etterretningsdoktriner og nytte de samme metodene som i dag for de andre domene (NATO, 2020a, s. 9). Viktigheten av dette er både standardiseringen av militære metoder og prosedyrer, samt sjefens mulighet for å utnytte tilgjengelige midler best mulig og evnen til å agere og handle hurtig i et operasjonsmiljø i stadig endring. Cyberdomenet kan på denne bakgrunn forstås til å videreutvikle utførelsen av operasjonskunsten.

4.5 Informasjon

Som diskutert under kommando og kontroll, manøver, ild og etterretning er informasjon en forutsetning for planlegging, gjennomføring og ledelse av militære operasjoner. Informasjon er grunnlaget for prioriteringer og beslutninger som driver prosesser fremover, uavhengig av nivå.

«Informasjonsoperasjoner (INFOOPS) er en koordinerende funksjon for å samordne alle militære informasjonsaktiviteter som søker å påvirke viljen, forståelsen og kapasitetene hos motstandere, potensielle motstandere og andre målgrupper» (Forsvarsstaben, 2019, s. 153). Det kan være både et offensivt- og defensivt tiltak: «Cyber operations are an integral part of the information function and may support information activities by providing both a vector for deploying information and effects that influence targeted audiences» (NATO, 2020a, s. 9) Cyberdomenet kan i denne sammenheng utnyttes like mye som en formidler eller kanal for å muliggjøre informasjonsoperasjoner, som at informasjonsoperasjoner legger til rette for og muliggjør cyberoperasjoner.

Informasjonsoperasjoner handler om å påvirke viljen til aktørene i operasjonsmiljøet.
Gitt cyberdomenets beskaffenhet er det særdeles godt egnet til å bedrive informasjonsoperasjoner både i og fra. For det første bidrar cyberdomenets rekkevidde og omfang til av informasjon enkelt kan spres over hele verden. Eksempelvis har vi de siste årene sett hvordan terrorgrupper som eksempelvis den islamske stat (IS/ISIL) bruker internett til å spre propaganda, usikkerhet og frykt – de angriper viljer.
For det andre bidrar cyberdomenet til at informasjonen spres utrolig hurtig. En ting er at informasjonen kan deles hurtig mellom sender og mottaker, en annen side er at hendelser og aktiviteter kan deles nesten rett etter at de har inntruffet. På denne måten må en være fleksibel og forberedt på å håndtere oppdukkende situasjoner hurtig.
For det tredje gir domenets oppbygning muligheten for både å skjule seg og manipulere informasjonen som spres. Et nylig eksempel er hvordan Russland, angivelig, under det amerikanske valget i 2016 etablerte motstående grupper på facebook som hadde til hensikt å skape splid internt i USA mellom tilhengere av de to presidentkandidatene. Utfordringen her kan være at mengden informasjon som finnes digitalt gjør at det er vanskeligere å være like kritisk til alt som publiseres, samtidig som at økende oppslutning og fokus også påvirker. Likevel bør de siste årene bidra til at vi nettopp er mer bevisst informasjonen som spres og forholder oss kritiske til det som publiseres.
For det fjerde blir digital informasjon fort mer allment tilgjengelig gjennom at det hurtig oppfattes og spres. Dette gjør også at det er mindre sannsynlighet for at det forsvinner.
Til slutt er tilgjengelighet et avgjørende punkt. På den ene siden er det en fordel at alle som har en computer, en smarttelefon, en radio eller en tv vil være mulig mottakere av informasjon og på denne måten mål i en informasjonsoperasjon. Likevel må ikke mellommenneskelige forhold undervurderes eller overses til fordel for enkelhet og lettvinthet. Mye av vår oppfatning av verden skapes gjennom den informasjonen vi serveres i det digitale domene og vil i så måte kunne påvirke våre handlinger. Tillit bygges over tid, og tillit er en del av viljen. Samtidig er det viktig å tenke på at motstanderen har akkurat samme mulighet som oss i kampen om narrativet. Dette gjør at informasjonsoperasjoner ofte gis en strategisk karakter gjennom at det er stater som gjennomfører informasjonsoperasjoner. Spesielt Kina og Russland er fremtredenen i måten de utnytter cyberdomenet i etterretnings- og

informasjonsoperasjoner (Grzegorzewski & Marsh, 2021). Cyberdomenet brukt på denne måten er med på å knytte operasjonskunsten sterkere til det strategiske nivå, samtidig som det endrer krigens karakter ved å muliggjøre bruken av andre maktmidler enn militærmakten for å nå egne målsettinger. Cyberdomenet muliggjør økt asymmetri i måten krigføringen føres på.

Cyberdomenet brukes til både å formidle og å innhente informasjon. Informasjonsoperasjoner, til forskjell fra etterretning har til hensikt å spre informasjon og kan på denne måten ses på som en effektor. Nedslagsfeltet er mennesket og effekten blir dermed fysisk. Etterretningen samler på sin side inn informasjon for å gjøre den om fra antagelser og forutsetninger til fakta og beslutningsgrunnlag. Likevel legger etterretningen også grunnlaget for hvordan informasjonen kan og bør brukes for å være effektiv opp imot de målsettingene som ønskes nådd. Cyberdomenet forenkler informasjonsoperasjoner gjennom dets utbredelse, samtidig øker det kompleksiteten gjennom at tilfanget av informasjon er så stort. Dette utfordrer kampen om narrative og underbygger viktigheten av operasjonskunstens rolle og viktigheten av å utnytte effektene informasjonen skaper. Samtidig viser denne symbiosen og den tette knytningen mellom strategi og operasjonskunst.

4.6 Understøttelse

I likhet med de andre fellesfunksjonene er også understøttelse avhengig av cyberdomenet. Understøttelse består i henhold til FFOD (2019) av militær ingeniørstøtte, logistikk og sanitet (Forsvarsstaben, 2019, s. 156-172; NATO, 2019a, s. 1-24).

Tradisjonelt er understøttelsen til for å muliggjøre manøver. Ingeniører sørger for at veier er farbare ved at mobilitets fremmende- og hemmende tiltak utføres. De støtter inn på lendevurderinger ved hjelp av militære geologer og de bidrar inn til å sikre miljøer forurenset av enten kjemiske, biologiske, radiologiske eller nukleære (CBRN) stridsmidler. Logistikken handler primært om å ivareta og å opprettholde stridsutholdenheten og kampkraften til egne styrker, gjennom transport, forsyning, vedlikehold og reparasjoner. Saniteten skal redde liv og sørge for å opprettholde kampkraft, gjennom behandling og evakuering av skadd personell. Cyberdomenet endrer ikke viktigheten av dette. Likevel vil funksjonenes tilsynelatende økende avhengighet av det ikke-fysiske domene bidra til økt sårbarhet i utøvelsen av militære operasjoner.

Den teknologiske utviklingen har gitt oss muligheter til å drive mer effektiv understøttelse av operasjoner. Planlegging av disse aktivitetene er avgjørende for å muliggjøre ild og manøver i tid og rom. NATO sin cyberspace doktrine sier at disiplinene som understøtter operasjoner er avhengige av cyberdomenet fordi vi har gjort oss avhengige av det, for å kunne dele informasjon, bestilling av

materiell og medisiner, journalføring og lager-, og beholdningsstatus (NATO, 2020a, s. 10). Selve utførelsen av understøttelsen har ikke nødvendigvis endret seg med cyberdomenet, men militære operasjoners avhengighet av tjenestene cyberdomenet leverer har ført til at det på en siden blir enklere og mer effektivt, men på den annen side også mer sårbart.

Cyberoperasjoner muliggjør egen handlefrihet gjennom å beskytte sårbar infrastruktur som sørger for effektiv understøttelse av operasjoner. På denne måten opprettholdes funksjonelle nettverk og systemer som gjør at understøttelsen av operasjoner kan gjennomføres mest mulig smidig og effektivt. Avdelingene på den fremre delen av stridsfeltet kan relativt enkelt rapportere og meld inn behov for støtte. Uten forbindelsen med bakre elementer vil ikke en styrke kunne opprettholde god stridsutholdenhet over lengre tid. Dersom norske styrker i Finnmark avskjæres fra Sør-Norge, både fysisk og digitalt, vil lokale understøttelsesressurser fortsatt kunne levere tjenester på taktisk nivå, mens på operasjonelt og strategisk nivå vil dette systemet kraftig forsinkes eller i verste fall bryte sammen. Det samme vil skje dersom det er sentrale enheter i Sør-Norge som angripes. Håndtering av risiko kan kun forebygges gjennom nøye planlegging, hvor ressurser for understøttelse av kampstyrker planlegges, men også understøttelse for å etablere, vedlikeholde og om nødvendig gjenopprette forbindelsen i nettverkene. Avgjørende i denne sammenheng er samtidig det tette samarbeidet med sivile aktører (Forsvarsdepartementet, 2014, s. 11). Både for å kunne opprettholde flyt i logistikken og ivaretakelse av personell fordi det er de samme ressursene som i stor grad nyttes både for militære styrker og det sivile samfunn. Cyberdomenet knytter på denne måten fronten enda nærmere det bakre området. Cyberdomenet påvirker i så måte operasjonskunsten gjennom at det må beskytte vår avhengighet av domenet i utøvelsen av operasjoner for å muliggjøre den.

4.7 Styrkebeskyttelse

Styrkebeskyttelse, eller Force Protection (FP) i NATO, er avgjørende for å ivareta sikkerhet og beskyttelse av personell, materiell, utstyr, infrastruktur, operasjoner og aktiviteter. Styrkebeskyttelsestiltak skal bidra til å fatte tiltak som reduserer risiko og øker egen handlefrihet i et operasjonsmiljø (NATO, 2019a, s. 1-25). For å kunne gjøre dette må de ulike fellesfunksjonene gjennom planlegging identifisere egne sårbarheter og anbefale eller iverksette tiltak for å redusere og håndtere risikoene. Siden styrkebeskyttelse skal bidra til å sikre gjennomføringen av oppdragsløsningen må den prioriteres og personellet som gjør disse prosessene må kjenne til styrkene og svakhetene cyberdomenet medfører. Hvis ikke er enkelte risiko- og sårbarhetsanalyser trolig bortkastet.

Cyberdomenet kan anses som en styrkemultiplikator innen styrkebeskyttelse. Militære høyverdimål må beskyttes for å sørge for egen operativ evne. Dette kan være seg forsyningslagre, kritisk teknologi- og kommunikasjonsinfrastruktur, havner, flyplasser, veier etc. Det meste gruppert og plassert i det fysiske domenet på landjorda. Her kan militære styrker gjennom cyberdomenet bidra til å beskytte kritisk infrastruktur og systemer som både det militære og sivile systemet er avhengig av, dette i stede for- eller i tillegg til den fysiske sikkerheten styrker på bakken bidrar med.

Styrkebeskyttelse kjennetegnes gjennom fire koordineringsområder[39]. Disse koordineringsområdene er gjenkjennbare og overførbare for å beskrive og forstå tiltak og handlinger både mot-, i og gjennom cyberdomenet. Dersom det ikke er ressurser til å beskytte alt samtidig, vil operasjonsplanleggingen bunne ut i en prioriteringsliste. Til sammenligning fra fysiske sikringstiltak kan cybersikkerhetstiltak være mer effektivt og mindre resurskrevende. Og i så måte erstatte fysisk tilstedeværelse. Samtidig kan cyberdomenet understøtte fysiske sikringsoperasjoner gjennom overvåkning eller informasjonsinnhenting og derigjennom være en ytterligere styrkemultiplikator (NATO, 2020a, s. 10). Risikoen med styrkebeskyttelsestiltak gjennom eller via cyberdomenet er at den kan virke mot sin hensikt, ved at det øker muligheten for sårbarheter og i så måte gir motstanderen utvidet manøverrom og handlingsalternativer mot egne kritiske sårbarheter. På samme tid kan også fysiske sikringstiltak være med på å beskytte cyberdomenet og cyberressurser. Dette gjøres ved at kritisk infrastruktur i det fysiske laget beskyttes mot fysisk påvirkning av fienden både fra bakken og fra luften, som eksempelvis med bruk av landstyrker, luftvern eller luft- og sjømakt for å nekte en motstander tilgang og muligheten for på påvirke cyberdomenets fysiske lag. Disse måtene å tenke styrkebeskyttelse er rettet mot det fysiske lag eller muliggjøres gjennom det logiske laget i cyberdomenet. Likevel er det viktig å huske på i denne sammenheng, som diskutert tidligere, at selv om det er i det logiske laget cyberoperasjonene muliggjøres kan beskyttelsen ligge like mye i å endre K2 og K2iS struktur, som det å sikre den.

Styrkebeskyttelse i cyberdomenet kan være både defensive cyberoperasjoner og sikkerhetsovervåkning av Forsvarets K2iS. Slik styrkebeskyttelse defineres i NATO og i FFOD handler det om å «...sikre egen handlefrihet og operativ effektivitet» (Forsvarsstaben, 2019, s. 149; NATO, 2020a, s. 4). Cybersikkerhetsovervåkning har til hensikt å «...forebygge, avdekke og håndtere uønskede digitale hendelser», mens defensive cyberoperasjoner er på sin side tiltakene som iverksettes for å forsvare og sikre militære sjefers og styrkers evne og mulighet for å utøve kommando og kontroll (Forsvarsstaben, 2019, s. 126). På samme måte som at overvåkning ikke er en etterretningsoperasjon er ikke cybersikkerhetsovervåkning nødvendigvis en cyberoperasjon, da den ikke alltid fokuserer mot

[39] Styrkebeskyttelse deles inn i fire koordineringsområder: forebyggende sikkerhet, aktive,- og passive tiltak og skadereparasjon/skadebehandling (Forsvarsstaben, 2019, s. 149).

en spesiell aktør, men er en del av daglige driftsrutiner. Likevel er cybersikkerhetsovervåkning en viktig del av den cyberspesifikke operasjonskunsten for å muliggjøre defensive cyberoperasjoner og derigjennom sikre og opprettholde konfidensialiteten, integriteten og tilgjengeligheten i de militære nettverkene. På denne måten kan også ansvars-, og interesseområder i cyberdomenet bedre defineres. I tillegg samarbeider Forsvaret tett innad i totalforsvaret og med allierte styrker, både for å kartlegge-, og motvirke potensielle cybertrusler (Forsvarsstaben, 2019, s. 126). Forebyggende sikkerhet er et fellesansvar for å ivareta systemers operativitet og integritet, i alle domener.

Styrkebeskyttelse som fellesfunksjon bidrar til at cyberdomenets påvirkning på militære operasjoner økes. Fordi det er rimelig å anta at aktører først vil påvirke en motstanders evne for å utøve effektiv kommando og kontroll, derfor er det også virkemidler som understøtter nettopp dette som må prioriteres i et styrkebeskyttelsesperspektiv. Hensikten er å opprettholde egen handlefrihet i cyberdomenet, så vel som i de andre krigføringsdomene. Grensesnittet mellom sivile og militære oppgaver er i denne sammenheng viktig, da militære styrker har ansvaret for å beskytte Forsvarets systemer. Likevel utfordres dette grensesnittet, da militære styrker også i stor grad er avhengig av sivile aktører og sivil infrastruktur for å gjennomføre sine operasjoner.

4.8 Sivilt-militært samvirke

Som oppgaven innleder med og som den har belyst flere steder er forholdet mellom sivile instanser og det militære helt avgjørende for nasjonal sikkerhet også innen cyberdomenet. Staten har voldsmonopol og iverksetter militærmakten ved behov. Politikkens primat og krigsmaktens autonomi er styrende. Men ikke på noe område, som i cyberdomenet, er maktmidlet mer likt og mer symbiotisk mellom det sivile og militære. I cyberdomenet har alle tilgang til den samme slagmarken, og potensielt tilnærmet like forutsetninger for å sloss. Dette forholdet er svært ulikt de andre krigføringsdomene og kan samtidig ses på som en gjensidig styrkemultiplikator.

Sivilt-militært samvirke, Civil Military Cooperation (CIMIC) i NATO, har som fellesfunksjon fokus på alle sivile forhold og anliggende i et operasjonsområde, og hvordan dette påvirker militære operasjoner og operasjonsmiljøet (Forsvarsstaben, 2019, s. 172). Dette innebærer koordinering og samordning av alle aktører i operasjonsområdet, fra sub-taktisk til strategisk nivå og omfatter kjennskap og kunnskap om operasjonsmiljøet, altså gjennom politiske, militære, økonomiske, sosiale, informasjon og infrastruktur (PMESII). Samtidig som det spiller en viktig rolle i å vurdere, analyser og beslutte hvilke maktmidler som bør eller kan nyttes i et operasjonsområde. Eller det kan være som i Norge, hvor Totalforsvarskonseptet står støtt og er avgjørende viktig for at Forsvaret og samfunnet

utnytter fellesressurser på en mest mulig effektiv måte. Dette kjennetegnes fra NATOs helhetlige tilnærming, comprehensive approach.

For militære operasjoner i cyberdomenet innebærer et sivilt-militært samarbeid flere ting. For det første må det etableres forbindelse og planlegges for tilgang til og bruk av sivil kommunikasjonsinfrastruktur. Dette kan medføre økt risiko dersom operasjonen ikke gjennomføres nasjonalt, fordi det betyr at en ikke nødvendigvis vil ha full kontroll over nettverket[ene]. På den annen side vil terrenget i cyberdomenet være gjenkjennbart uavhengig av egen geografiske plassering, som betyr at risikoen kan håndteres gjennom forhåndsplanlagte cybersikkerhetstiltak eller defensive cyberoperasjoner. Denne utfordringen og bevisstheten er samtidig viktig dersom- og når allierte deployerer til Norge enten for å trene eller bidra i et kollektivt forsvar av landet.
For det andre vil et slikt samvirke kunne være enklere enn i eksempelvis landdomenet. Fordi under et utenlandsoppdrag vil et styrkebidrag kunne være avhengig av enten den sivile befolkningen eller sivile ressurser eller myndigheter for å få tilgang på informasjon i enkelte områder. Denne utfordringen finner en i mindre grad i cyberdomenet siden en kan manøvrere tilnærmet fritt og skjult, uten eskorte. Utfordringen kan derimot være juridisk siden man i NATO operasjoner er underlagt internasjonale lover, FN-pakten, menneskerettighetene og krigens-folkerett (NATO, 2020a, s. 19). Samtidig som at offensive-cyberoperasjoner skal være godkjent på politisk nivå. I NATO er det North Atlantic Council (NAC) som godkjenner dette (NATO, 2020a, s. 21). Selv om cyberdomenet er globalt og opererer med mindre tydelige grenser er fortsatt domenet underlagt nasjonal jurisdiksjon innen nasjonale territorielle grenser.
For det tredje betyr et sivil-militært samvirke økt kampkraft i form av flere ressurser som fokuserer innen et felles målbilde og mot en felles effekt. Dette forutsetter derimot grundig og tett koordinering både før og under gjennomføring av operasjonene. I Norge ligger det overordnede ansvaret for offensive- og defensive cyberoperasjoner som kjent hos det operasjonelle nivå, hos henholdsvis sjef Forsvarets operative hovedkvarter og sjef Etterretningstjenesten (Forsvarsstaben, 2019, s. 129). Totalforsvarskonseptet legger til rette for et utvidet samarbeid gjennom etablerte liasonordninger fra de ulike sivile aktørene inn mot Forsvaret for å ivareta et tett og godt samvirke. Som ved nasjonal håndtering av IKT-sikkerhetshendelser hvor E-tjenesten, Nasjonal sikkerhetsmyndighet og Politiets sikkerhetstjeneste koordinerer aktiviteter (Forsvarsstaben, 2019, s. 131). Nasjonal sikkerhetsmyndighet drifter på sin side nasjonalt cybersikkerhetssenter (NCSC), som er «...den nasjonale responsfunksjonen for alvorlige digitale angrep og drifter det nasjonale varslingssystemet for digital infrastruktur (VDI)» (NSM, 2021). Likevel er ikke en prioritering av kapabiliteter og ressurser utenkelig, snarere nødvendig, noe som kan påvirke muligheten for oppdragsløsningen, på enten militær eller sivil side. Fordelen igjen ligger i at ressursene, infrastrukturen og

interesseområdene i stor grad samsvarer og legger grunnlaget og muligheten for gjensidig støtte ved behov.
Til slutt vil det sivil-militære samvirket bidra til å utvikle både militære og sivile operasjoner i- og gjennom cyberdomenet videre. Det bidrar til økt kjennskap og kunnskap på tvers av aktørene, både hva angår situasjonsforståelse og kulturell forståelse, økt forståelse av respektive målsettinger, integrert planlegging og effektiv kommunikasjon gjennom interoperable nettverk som muliggjør samvirke og informasjonsdeling (Forsvarsstaben, 2019, s. 173-174). Alt dette vil bidra til at militære sjefer har flere ressurser å spille på under planlegging, gjennomføring og ledelse av sine operasjoner.

Sivil-militært samvirke inngår i likhet med de andre fellesfunksjonene inn i flere av de militære planprosessene. Samtidig som at skadeomfanget av kinetiske effekter må vurderes opp imot kost-nytte, må også effektene skapt av cyberoperasjoner vurderes. Dersom cyberoperasjoner blir iverksatt for å ta ut sivile mål, som eksempelvis strømforsyninger, vil dette kunne påvirke produksjon og tilgang på potensielt livsnødvendige varer og tjenester. Den umiddelbare effekten vil kanskje oppleves mindre enn ved et nedslag. Derimot vil som nevnt de langvarige effektene være store og påvirke handlefriheten og måloppnåelsen i de andre domene. Og igjen, effekten gjennom cyberdomenet er alltid fysisk som betyr at den vil påvirke måten vi planlegger, gjennomfører og leder operasjoner på. Det vil si at cyberdomenet påvirker utøvelsen av operasjonskunsten gjennom en tettere forankring og tilknytning mot det sivile, noe som er hensiktsmessig gitt domenets karakter og utbredelse. Samtidig gjør denne tette tilknytningen og avhengigheten at operasjonskunsten videre utfordres med hensyn til operasjonsmiljøets økende kompleksitet og omfang. Gitt det at domenet er menneskeskapt vil det alltid være en symbiose mellom den sivile og militære delen av samfunnet. En helhetlig tilnærming til bruk og utnyttelse av cyberdomenet er derfor avgjørende viktig for at strategiske føringer og målsettinger skal kunne omgjøres til taktiske handlinger.

5 Konklusjon

Oppgaven har hatt til hensikt å besvare spørsmålet: *Hvordan påvirker cyberdomenet utøvelsen av operasjonskunst?* Før det konkluderes vil jeg begynne med å svare på om cyberdomenet i det hele tatt påvirker utøvelsen av operasjonskunsten, til det vil jeg svare, ja.

Doktriner, strategier og operasjoner har sin forankring i militærteorien. Det militærteoretiske fundamentet etablerer et grunnlag som skal gi retning for hvordan militære styrker skal anvendes i krig. Det betyr med andre ord at noe er prioritert bort. NATO sin cyberspace doktrine er pr tid utgangspunktet for hvordan også Norge skal planlegge, gjennomføre og lede militære cyberoperasjoner i en fellesoperativ ramme. Men, den er likevel kun veiledende (NATO, 2020a, s. xiii). For hvordan tilnærmer og tilpasser man seg et domene som er menneskeskapt? Og hva har det å si for militære operasjoner i dag og fremover?

Operasjonskunsten vokste frem i en tid hvor krigens karakter var i en voldsom utvikling. Den søkte å «...begrepsfeste og håndtere kompleksiteten som den industrialiserte folkekrigen førte med seg...Operasjonskunsten var den praktiske planleggingen og ledelsen av store kompliserte kampsystem for å nå de strategiske målsettingene innenfor et operasjonsområde...» (Ydstebø, 2012, s. 423-424). En kompleksitet som i dag kan påstås å være vel så stor om ikke større nettopp på grunn av cyberdomenet. Fordi cyberdomenet knytter verden ennå tetter sammen med sin globale utstrekning og tilgjengelighet.

Før operasjonskunsten ble introdusert på første halvdel av 1900-tallet hadde klassiske militærteoretikerne viet både strategi og taktikk mye tid gjennom grundige analyser av krig. Deres tanker lever i beste velgående den dag i dag. Likevel tok Svechin til mele for at noe manglet. Noe som kunne binde sammen strategien og taktikken:

> Studying the methods of conducting an operation is a job for operational art rather than strategy…strategy, which defines its task in the conduct of military operations as combining operations for achieving the ultimate goal, is not only interested in stating the goal of an operation but also makes certain requirements of the methods of achieving it. All branches of the art of war are closely interrelated: tactics takes the steps that make up an operational leap, and strategy points the way. (Svechin, 1927, s. 269)

Dagens komplekse operasjonsmiljø skyldes selvfølgelig flere ting. Denne oppgaven har søkt å vise hvordan cyberdomenet har bidratt til å endre krigens karakter og hvordan vi kan forstå dets påvirkning av operasjonskunsten i rammen av de åtte fellesfunksjonene som er selve rammeverket for planlegging, gjennomføring og ledelse av operasjoner.

Cyberdomenet påvirker utøvelsen av operasjonskunsten spesielt med hensyn til tid og rom. Tidsdimensjonen i cyberdomenet skiller seg fra de fysiske domene i den forstand at det rett og slett er mulig å oppnå et relativt høyere tempo over tid. Dette påvirker på sin side hvordan K2, manøver, ild, etterretning, informasjon, styrkebeskyttelse, understøttelse og sivil-militært samarbeid kan utnyttes og må forstås i rammen av militære operasjoner. Tiden det tar å forflytte seg fra en side av jordkloden til den andre gjennom cyberdomenet er gjort på millisekunder. Dette er ikke kun en fordel for cyberoperasjoner isolert sett, det er også i aller høyeste grad en fordel for de krigførende partene i både land-, sjø-, og luftdomene.

Effektene som skapes i- eller gjennom cyberdomenet er fysiske i sin karakter, selv om de utføres gjennom nettverk og systemer i det ikke-fysiske domenet. Planlegging og gjennomføring av cyberoperasjoner er nødvendigvis ikke mindre tidkrevende, snarere tvert i mot, da de både bør gjennom de samme prosessene som i annenplanlegging, samtidig som de skal synkroniseres og koordineres med operasjoner i det fysiske domenet.

Romdimensjonen endrer seg også med at cyberdomenet som operasjonsmiljø er relativt nytt og menneskeskapt. Det omfatter alle de andre krigføringsdomene, men er samtidig avhengige av de, da infrastrukturen i cyberdomenet går på land, under vann og på luften. Det er også viktig å huske på at det er i det fysiske domenet effektene skapes. Til forskjell fra konvensjonelle kriger er ikke operasjonsområdet like avgrenset og isolert i cyberdomenet. Manøverrommet er utvidet og i tillegg så vil topografien hurtig kunne endre seg. En avgrensning av interesse- og ansvarsområde er derfor også avgjørende i cyberdomenet.
Romdimensjonen bidrar imidlertid til at cyberdomenet som en arena for krig er med på å øke muligheten for- og effekten av asymmetrisk krigføring, gjennom dets utbredelse, tilgjengelighet og rekkevidde. Samtidig som skille mellom fred, krise og krig kan bli vanskeligere å avdekke fordi hva er en krigserklæring i cyberdomenet?
Videre er skillet mellom det sivile og militære, det fremre og bakre operasjonsområde blitt enda mindre eller mer utydelig. Dette utfordrer lederskapet, både sivilt og militært, fordi krig er ikke lenger krig slik vi alltid har oppfattet det, krigen har endret karakter og er tilført ytterligere en dimensjon av kompleksitet. Domenets foreløpige strategiske forankring påvirker derfor utøvelsen av operasjonskunsten.

Cyberoperasjoner vil kreve like mye om ikke mer tid og oppmerksomhet fremover, for at vi skal kunne forstå domenet og utnytte dets potensial fullt ut. Til sammenligning har det tatt århundrer om ikke årtusener å forstå krig slik vi kjenner det i dag. På denne bakgrunn må militærteorier, doktriner, strategi, taktikk og prosedyrer tilpasses og standardiseres. Det må eksistere et begrepsapparat som er

mest mulig likt det vi bruker i dag. Slik at det ikke skapes et skille mellom de fysiske og det ikke-fysiske domene. Det er vist at etterretningsprosessen, koordineringsområdene for styrkebeskyttelse, målbekjempningsprosessen og førende lederskapsfilosofi hvor viljens sentrale posisjon fra manøverteori og manøverkrigføring både kan anvendes for- og integreres i planlegging av cyberoperasjoner. Synergien domenene imellom antas å bare bli tydeligere og tydeligere etter hvert som cyberdomenet blir en mer integrert og naturlig del av militære operasjoner. Selv om cyberoperasjoner er avhengige av et logisk lag for å gjennomføres, er effektene som skapes utelukkende fysiske. Dette betyr at de på en eller annen måte bidrar til og skaper forutsetninger for operasjoner i det fysiske domene.

Krig er på ingen måte et nytt fenomen. Det er forsket på, undersøk og studert så lenge den har eksistert. Det som er sikkert er at det fortsatt vil være en kamp mellom viljer, enten om det skjer fra et tastatur eller fra en skyttergrav. Fremtiden vil fortsette å være preget av teknologisk utvikling og nye revolusjoner innen krigføringen. Kanskje vil maskiner og systemer få menneskelig egenskaper. Uansett, cyberdomenet vil fortsette å påvirke måten vi planlegger, gjennomfører og leder operasjoner på gjennom å utfordre operasjonsmiljøet – det vi må gjøre er å tilpasse oss og utnytte det. Den viktigste måten å tilegne oss kjennskap, kunnskap og kompetanse om cyberdomenet og cyberoperasjoner på er å studere og undersøke det.

Underveis i denne studien har jeg ofte fått ideer og tanker om hvordan oppgaven kunne vært vinklet eller designet annerledes. Derfor vil jeg også dele noen av disse tankene og foreslå mulige problemformuleringer for videre studie av cyberdomenet.

Planlegging, gjennomføring og ledelse av militære operasjoner er Forsvarets primære oppgave. Derfor ville det vært interessant å sett videre på hvordan Norge og Forsvaret planlegger, gjennomfører og leder cyberoperasjoner mer i detalj. Dette kan gjøres ved å sammenligne måten Forsvaret utnytter og opererer i cyberdomenet sammenlignet med andre nasjoner. Enten internt i NATO eller med potensielle motstandere som Russland og Kina.
En annen vinkling vil være å se nærmere på grensesnittet mellom det sivile og militære cyberdomenet. På denne måten kan også samhandlingen i rammen av Totalforsvaret forstås bedre.

Det ville også være interessant å undersøke hvor vidt fordelingen av ansvaret for defensive- og offensive cyberoperasjoner i Forsvaret er hensiktsmessig. Kan det foreksempel være organisert på en annen måte for å bedre være i stand til å planlegge, gjennomføre og lede cyberoperasjoner?

6 Litteraturliste:

Andersen, M. & Ydstebø, P. (2016). Hva er Operasjonskunst? *I Morten Andersen og Geir Ødegaard (red.) (2016). Militære Fellesoperasjoner - En innføring. Side 29 - 42.*

Andreassen, Y. (2015). Etterretning, (I Morten Andersen og Geir Ødegaard (red.) (2015). Militære Fellesoperasjoner - en innføring. s 243-256.).

Art, R. J. (1996). American Foreign Policy And the Fungibility of Force. *Security Studies, Volum 5, no.4 (summer 1996)*(Published by Frank Cass, London.), 7-42.

Ben-Shalom, U. & Shamir, E. (2011). Mission Command between theory and practice: The case of the IDF. *Defense & Security Analysis, 27:2*, 101-117. Hentet fra http://dx.doi.org/10.1080/14751798.2011.578715

Bergh, A. (2020). Påvirkningsoperasjoner i sosiale medier - oversikt og utfordringer. *FFI-rapport 20/01694,* (Forsvarets forskningsinstitutt (FFI)). Hentet fra https://publications.ffi.no/nb/item/asset/dspace:6867/20-01694.pdf

Boyd, J. (1986). Patterns of Conflict. Hentet fra https://www.slideshare.net/noobgank/patterns-of-conflict

Brezins, J. (2014). Russia´s New Generation Warfare in Ukrain: Implications for Latvian Defence Policy. *Policy Paper, no:02. April 2014*(National Defence Academy of Latvia. Center for Security and Strategic Research.).

Clausewitz, C. v. (1976). On War, edited and translated by Michael Howard and Peter Paret, *9th printing edition (1976)*(Princton, NJ: Pincton University).

Clausewitz, C. v. (1984). On War. *I Forsvarets Høgskole kompendium (2018). Væpnet konflikt og doktrineutvikling. MILMA5540, 2018-H.*

Clement, J. (2020). Worldwide digital population as of october 2020. Hentet fra https://www.statista.com/statistics/617136/digital-population-worldwide/

Coaker, W. & Dobson-Keefe, N. (2015). Thinking more rationally: cognitive biases and the Joint Military Appreciation Process, (Department of Defence. Australia).

Conti, G. & Raymond, D. (2017). On Cyber - Towards an Operational Art of Cyber Conflict. *Kopidon press*.

Crowther, G. A. (2017). The Cyber Domain. *The Cyber Defence Review,, Vol 2, No. 3 (Fall 2017), pp 63-78.* Hentet fra https://www.jstor.org/stable/26267386?seq=1#metadata_info_tab_contents

Dalløkken, P. E. (2014). Her er Norges nye panservogn - CV90 MKIII. *Teknisk Ukeblad*. Hentet fra https://www.tu.no/artikler/her-er-norges-nye-panservogn/222995

DSB. (2020). Risikostyring i digitale verdikjeder, (Direktoratet for samfunnssikkerhet og Beredskap (DSB). Rapport fra en arbeidsgruppe ledet av professor Olav Lysne (Lysneutvalget)).

Erichsen, O. v. P. & Mathisen, H. H. (2015). Cyberoperasjoner, (I Morten Andersen og Geir Ødegaard (red.) (2015). Militære Fellesoperasjoner - en innføring. s 345-361).

Forsvaret. (2020). Forsvarets grunnsyn på ledelse.

Forsvarsdepartementet. (2014). Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektiren «FDs cyberretningslinjer». Hentet fra https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf

Forsvarsdepartementet & Justis-og_beredskapsdepartementet. (2018). Støtte og samarbeid - En beskrivelse av totalforsvaret i dag, (Regjeringen, Oslo 8.mai 2018). Hentet fra https://www.regjeringen.no/contentassets/5a9bd774183b4d548e33da101e7f7d43/stotte-og-samarbeid-en-beskrivelse-av-totalforsvaret-i-da.pdf

Forsvarsstaben. (2007). Forsvarets fellesoperative doktrine.

Forsvarsstaben. (2019). Forsvarets Fellesoperative Doktrine, (Forsvarets Høgskole (FHS)/Stabsskolen (FHS/STS), 2019 Oslo).

Frieser, K.-H. (2005). Panzer Group Kleist and the Breakthrough in France, 1940, (I Historical perspectives of the operational art, red. Michael D. Krause og R. Cody Phillips. Washington DC: Center of Military History, United States Army, 2005. s. 169-182).

Gabel, C., R. (1992). The U.S. Army GHQ Maneuvers of 1941. I Menning, Bruce W - Operational Art´s Origins (2005). *Washington, D.C: U.S. Army Center of Military History 1992. pp. 185-194*.

Greenberg, A. (2019). Sandworm - A new area of cyberwar and the hunt for Kremlin´s most dangerous hackers, (Anchor Books, A Division of Penguin Random House LLC, New York).

Grzegorzewski, M. & Marsh, C. (2021). Incorporating the Cyberspace domain: How Russia and China exploit asymmetric advantages in great power competition, (Modern War Institute, At West Point). Hentet fra https://mwi.usma.edu/incorporating-the-cyberspace-domain-how-russia-and-china-exploit-asymmetric-advantages-in-great-power-competition/?fbclid=IwAR3ns7p8WpymdnbfoZfozxOATwoMofsKje6X_Gu3izk3Hd9bxlcG7bBghP4

Gundersen, P. C. (2015). Kommando og Kontroll. *I Morten Andersen og Geir Ødegaard (red.) (2016). Militære Fellesoperasjoner - En innføring. Side 231 -241.*

Heuser, B. (2016). Theory and Practice, Art and Science in Warefare: An Etymonological Note. *I Marston, D. & Leahy, T (2016) (edt.). War, Strategy and History: Essays in Honour of Professor Robert O'Neill, edited by Daniel Marston and Tamara Leahy, published 2016 by ANU Press, The Australian National University, Canberra, Australia.*

Høiback, H. (2012). Militærteoretisk idehistorie. , (I Høiback, H og Ydstebø. P (red.). 2012. Krigens Vitenskap - en innføring i militærteorie. Abstrakt forlag AS. s.78-119.).

Høiback, H. & van Loon, C. (2012). Cyberkrig, oppblåst samband eller en ny arena?

Isserson, G. S. (1932/1936/2013). The Evolution of Operational Art (B, W. Menning, Overs.). G, S. Isserson (Første utg. 1932, Andre utg. 1936), (Combat Studies Institute Press. US Army Combined Arms Center. Fort Leavenworth, Kansas. July, 2013.).

Jacobsen, D. I. (2015). Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode. *Capplen Damm Akademisk, 3.Utgave, 2.Opplag 2016.*

Jacobsen, R. (2015). Forord, (I Morten Andersen og Geir Ødegaard (red.) (2015). Militære Fellesoperasjoner - en innføring).

Johansen, I. (2004). Cyberspace som slagmark - Refleksjoner omkring internett som arena for terrorangrep. *FFI/Rapport-2004/01666,* (Forsvarets forskningsinstitutt).

Johnsen, S. T. & Kveberg, T. (2014). Cyberdomenet, cybermakt og norske interesser. *FFI-rapport 2013/02712,* (Forsvarets Forskningsinstitutt).

Jomini, A. H. (1862). The Art of War (Summary), (Philladelphia, J. R. Lippinscott & Co. 1862).

Karlsen, G. H. (2015). Strategisk kommunikasjon: NATOs modell for informasjon og påvirkning, (I Morten Andersen og Geir Ødegaard (red.) (2015). Militære Fellesoperasjoner - en innføring. s.291-317).

Kuusisto, T., Kuusisto, R. & Roehrig, W. (2015). Situation Understanding for Operational Art in Cyber Operationss. *In Abouzakhar, N. (ed.) Proc of the 14th European Conference on Cyber Warefare and Security ECCWS-2015, Hatfield, UK, 2-3.7.2015, pp 169-178.,* (Academic Comferences and Publishing International Limited Reading, UK 44-118-972-4148.). Hentet fra https://www.researchgate.net/publication/280637915_Situation_Understanding_for_Operational_art_in_Cyber_Operations

Leksikon, S. N. (2015). Moores Lov, (Skrevet av: Bjørn B. Larsen (NTNU)). Hentet fra https://snl.no/Moores_lov

Libicki, M. C. (2016). Cyberspace - In Peace and War. *Naval Institute press, Annapolise, MD 21402.*

Lind, W. S. (1997). Some Doctrinal Questions for the US Army. *Military Review, 1977., Årgang 77*(No 1), 13. Hentet fra https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/425/

McCormick, M. (1997). The New FM 100-5: A returne to Operational Art, (School of Advanced military Studies. United States Army Command and General Staff College. Fort Leavenworth, Kansas). Hentet fra https://apps.dtic.mil/dtic/tr/fulltext/u2/a331274.pdf

Mearsheimer, J. J. (1981). Maneuver, Mobile Defense, and the NATO Central Front. *International Security, Vol. 6, No-3-(Winter 1981-1982), pp 104-122.* Hentet fra http://links.jstor.org/sici?sici=0162-2889%28198124%2F198224%296%3A3%3C104%3AMMDATN%3E2.0.CO%3B2-X

Menning, B. W. (2005). Operational Art´s Origins., (I Historical perspectives of the operational art, red. Michael D. Krause og R. Cody Phillips. Washington DC: Center of Military History, United States Army, 2005. s. 3-21).

MoD. (2016). Joint Doctrine Publication 04 - Understanding and Decision-making, *2nd Edition* (The Development, Cincepts and Doctrine Center. UK Ministry of Defence (MoD), Shrivenham. Swindon, Wiltshire, SN6 8RF).

Morris, L. J., Mazarr, M. J., Hornung, J. W., Pezard, S., Binnendijk, A. & Kepe, M. (2019). Gaining Competitive Advantage in the Gray Zone - Response Options for Coercive Aggression Below the Threshold of Major War, (RAND Corporation, Santa Monica, Calif.).

NATO. (2016a). AJP-2 Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security, *Edition A, Version 2*(NATO Standardization Office (NSO)).

NATO. (2016b). AJP-3.9 Allied Joint Doctrine for Joint Targeting, *Esition A, Version 1*(NATO Standardization Office (NSO)).

NATO. (2017a). AJP-01. Allied Joint Doctrine, *Edition E, Version 1*(NATO Standardization Office (NSO).).

NATO. (2017b). Warsaw Summit Key Decisions, (NATO). Hentet fra https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf

NATO. (2019a). AJP-3. Allied Joint Doctrine for rhe Conduct of Operations, *Edition C, Version 1*(NATO STANDARDIZATION OFFICE (NSO)).

NATO. (2019b). AJP-5. Allied Joint Doctrine for the Planning of Operations., *Edition A, Version 2*(NATO Standardization Office (NSO)).

NATO. (2019c). AAP-06 - NATO Glossery of Terms and Definitions., *Edition 2019*(NATO Standardization Office (NSO)).

NATO. (2020a). AJP 3.20 Allied Joint Doctrine for Cyberspace Operations, *Edition A, Version 1*(NATO Standardization Office (NSO)).

NATO. (2020b). AJP-3.20 Allied Joint Doctrine for Cyberspace Operations, *Edition A. Version 1*(NATO standardization office (NSO)).

NATO. (2021). Allied Command Operations Comprehensive Operations Planning Direktiv (COPD), *Version 3.0*

NSM. (2021). Nasjonalt Cybersikkerhetssenter (NCSC). Hentet fra https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/

Nye, J. S. (2011). The Furure of Power, (Ingram Publisher. New York: Public Affairs, 2011).

Nyeng, F. (2012). Nøkkelbegreper i forskningsmetode og vitenskapsteori, *1*(Vigmostad &Bjørke AS), 9-15.

Orlowski, J. (2020). The Sosial Dilemma. *Netflix,* (Exposure Labs). Hentet fra www.netflix.com

Overkommando, F. (2000). Forsvarets Fellesoperative Doktrine. Del B - Operasjoner, *Første utgave*. Hentet fra https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2381754/FFOD%202000.%20Del%20B%20Operasjoner..pdf?sequence=2&isAllowed=y

Persson, C. P. (2019). Abduksjon: Metoden for å finne den beste forklaringen. *forskning.no,* (© Videnskab.db. Oversatt av Lars Nygaard for forskning.no). Hentet fra https://forskning.no/om-forskning-samfunnsvitenskap/abduksjon-metoden-for-a-finne-den-beste-forklaringen/1317339

Sander, K. (2020). Fire Industrielle revolusjoner. *Estudie.no*. Hentet fra https://estudie.no/fire-industrielle-revolusjoner/

SNL. (2019). William Gibson. *Store Norske Leksikon (SNL)*. Hentet fra https://snl.no/William_Gibson_-_science_fiction-forfatter

Soldal, M. L. (2020). Cybermaktkonkferansen 2020 - Forskning på Cyberoperasjoner, Phd Mass L. Soldal.

Springer, P. J. (2016). Transforming War. I Libicki, Martin C. (2016). Cyberspace in Peace and War.

Stoltenberg, J. (2018). Speech at the Cyber Defence Pledge Conference (Ecole militarie, Paris), (NATO Secretary General). Hentet fra https://www.nato.int/cps/en/natohq/opinions_154462.htm

Stortinget. (2020). IT angrep mot Stortinget.

Strachan, H. (2019). Strategy in theory; strategy in practice. *Journal of Strategic Studies, 42(2).* Hentet fra https://www.tandfonline.com/doi/full/10.1080/01402390.2018.1559153

Svechin, A. A. (1927). Strategy, (Minneapolis: East View, 2004).

Sæveraas, T., E. & Henriksen, K. (2007). Et militært universalmiddel? - Amerikansk «Maneuver Warefare» og norsk doktrineutvikling. *Oslo Files - On defence and security-01/2007,* (Institutt for Forsvarsstudier (IFS). Tollbugt. 10, 0152 Oslo).

Sønstebyfondet. (2021). Hentet fra https://www.no24.no/2021-cyberforsvarerne/

TRADOC. (2017). The Operational Environment and the Changing Character of Futer Warfare. *Small Wars Journal,* (U.S. Army Training and Doctrine Command (TRADOC) G-2 Mad Scientist Initiative). Hentet fra https://smallwarsjournal.com/jrnl/art/the-operational-environment-and-the-changing-character-of-future-warfare

TRADOC. (2018). The U.S Army in Multi-Domain Operations 2028, (Pamphlet 525-3-1). Hentet fra https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf

U.S.Army. (1986). FM 100-5 Operations, (Field Manual No. 100-5. Headquarters, Department of the Army, Washington, DC, 5.May 1986).

U.S.Army. (2017). Army Doctrine Reference Publication No.3-0, (Headquarters, Department of the Army, Washington, DC). Hentet fra https://fas.org/irp/doddir/army/adrp3_0.pdf

U.S.Army. (2019). ADP 6-0 Mission Command - Command and Control of Army Forces, (Headquarters, Department of the Army).

USMC. (1997). MCDP 1 - Warfighting, (Department of the Navy. Headquarters United States Marine Corps. Washington, D.C. 20380-1775). Hentet fra https://www.marines.mil/Portals/1/Publications/MCDP%201%20Warfighting.pdf

Van Hecke, M. L. (2007). Blind Spots. *I Jacobsen, Dag Ingvar (2015). Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode. Capplen Damm Akademisk. 3.Utgave, 2.Opplag 2016,* (New York: Prometheus Books).

Ydstebø, P. (2012). Fellesoperasjoner og Operasjonskunst - militærteoriens praktiske uttrykk, (I Krigens Vitenskap - en innføring i militærteori. Harald Høiback og Palle Ydstebø (red). s. 421-481).