FORSVARET
Forsvarets høgskole

Defensive cyberoperasjoner

Forholdet mellom taktisk og operasjonelt nivå

Gry-Mona Nordli

Masteroppgave

Forsvarets høgskole

vår 2024

Forord

Valg av tema for denne masteroppgaven kan vel sies å ha vært alt annet enn tilfeldig. Etter å ha jobbet mange år i fagfeltet og kjent hvor skoen har trykket, har det vært et privilegium å få tid og tilgang til ressurser for å se nærmere på et tema som ligger hjertet nær.

Jeg vil takke engasjerte respondenter for deres bidrag, jeg har blitt tatt imot med åpne armer hvor enn jeg har henvendt meg, og dette har bare bevist for meg hvor riktig det var å ta tak i denne problemstillingen. Interessen og engasjementet ute blant mine kolleger i cyberfagfeltet er stort, noe som har vært en sterk motivator når arbeidet med oppgaven har vært litt bratt.

Jeg vil også takke en tålmodig arbeidsgiver og kollegaer i Cyberstaben som har tålt mye fravær og holdt ut med mine stadige referanser til masterskrivingen. Takk for armslaget og gode diskusjoner. Jeg må også rette en takk til gode kollegaer og medstudenter for gjennomlesing, gode innspill og moralsk støtte. Ikke minst rettes en stor takk til min veileder Stig Tore Aannø som har utfordret meg faglig samt bidratt med gode innspill og konstruktiv kritikk.

Til slutt en spesiell takk til de på hjemmebane som har holdt ut med meg under studietid både i Oslo og hjemme, det skal bli godt med en ball mindre i lufta fremover.

Gry-Mona Nordli
Brumunddal, mai 2024

Sammendrag

I moderne krigføring er avhengigheten av cyberdomenet stadig mer fremtredende. Både ledelse, kampsystemer og samvirke må fungere, og alle har avhengigheter av et utfordret cyberdomene. Cyberdomenet er for mange fortsatt abstrakt og lite håndgripelig. Selv etter NATOs anerkjennelse som et krigføringsdomene, noe som sidestilte cyberdomenet med land-, sjø-, luft- og romdomenet, hersker det fremdeles mye usikkerhet rundt hvordan krigføring i cyberdomenet skal og bør utøves. Defensive cyberoperasjoner handler ikke kun om å beskytte teknologi, men er tiltak og aktiviteter som skal sikre og forsvare en militær sjefs handlefrihet. Avhengigheter av cyberdomenet innebærer at militære sjefer sine mulighet til å utøve militær kommando, kontroll og kommunikasjon avhenger av effektive defensive cyberoperasjoner.

Denne masteroppgaven utforsker forholdet mellom taktisk og operasjonelt nivå i Forsvaret innen defensive cyberoperasjoner. Gjennom å anvende en kvalitativ forskningsmetode som kombinerer aksjonsforskning og semistrukturerte intervjuer med aktører på taktisk og operasjonelt nivå, utforsker oppgaven hvordan aktørenes mentale modeller påvirker forholdet, og hvordan doktrine kan bidra til en felles tilnærming til defensive cyberoperasjoner som en del av fellesoperasjoner. Analysen bygger på et teoretisk rammeverk som ser cyberdomenet som en innovasjon, og kombinerer militær innovasjonsteori og spredningsteori med teori om mentale modeller. Dette rammeverket bidrar til en forståelse av hvordan aktørene opplever utfordringer i planlegging og gjennomføring av defensive cyberoperasjoner, samt har en forklaringskraft for hvorfor forholdet mellom taktisk og operasjonelt nivå oppleves som uavklart.

Funnene indikerer at aktørene har ulike forståelser av domenet. Det er fortsatt mye usikkerhet knyttet til cyberdomenet, ikke bare i begreper, men også roller ansvar og myndighet. Militære innovasjoner møter motstand i den militære organisasjonens byråkratiske natur, at cyberdomenet oppleves som abstrakt og komplekst er faktorer som bidrar til at spredning av innovasjonen går tregt. Mangelfulle doktriner og manglende operasjonalisering av eksisterende doktriner bidrar til utvikling av ulike mentale modeller på taktisk og operasjonelt nivå. Aktørenes divergerende mentale modeller, og lave bevissthet knyttet til disse, hemmer kommunikasjonen mellom taktisk og operasjonelt nivå. Alle vil det samme, men veien dit ser ulik ut. For Forsvarets evne til å planlegge og gjennomføre effektive defensive cyberoperasjoner er en omforent forståelse, åpenhet og kommunikasjon en nøkkel til suksess. At aktørene er gitt den samme ønskede sluttilstanden, er ikke nødvendigvis det som bidrar til den mest effektive veien til målet.

Summary

In modern warfare, the reliance of cyberspace is increasingly prominent. Both leadership, combat systems, and coordination must function, and are all dependent on a contested cyberspace. Cyberspace remains abstract and intangible for many. Even after NATO's recognition of cyberspace as a warfighting domain, which equated cyberspace with the land, sea, air, and space domains, there is still much uncertainty about how warfare in cyberspace should and ought to be conducted. Defensive cyberoperations are not solely about protecting technology, but are measures and activities aimed at ensuring and defending a military commander's freedom of action. Dependencies on cyberspace imply that a military commander's ability and opportunity to exercise military command, control, and communication depend on effective defensive cyberoperations.

This master's thesis explores the relationship between the tactical and operational levels in the Norwegian Armed Forces within defensive cyberoperations. The qualitative research method combines action research and semi-structured interviews with actors at the tactical and operational levels. The thesis explores how actors' mental models influence the relationship and how doctrine can contribute to a common approach to defensive cyberoperations as part of joint operations.

The analysis is based on a theoretical framework that views cyberspace as an innovation, combining military innovation theory and diffusion theory with theory of mental models. This framework contributes to an understanding of how actors experience challenges in planning and executing defensive cyberoperations and provides explanatory power for why the relationship between the tactical and operational levels is perceived as unclear.

The findings indicate that actors have different understandings of the domain. There is still much uncertainty regarding cyberspace, not only in terminology, but also roles, responsibilities, and authorities. Military innovations encounter resistance due to the bureaucratic nature of the military organization, and the perception of cyberspace as abstract and complex, are factors contributing to the slow diffusion of innovations. Deficient doctrines and the lack of operationalization of existing doctrines contribute to the development of diverging mental models at the tactical and operational level. The actors' diverging mental models and low awareness of these, hinder communication between the tactical and operational level.

Everyone wants the same thing, but the path to get there looks different. For the military's ability to plan and execute effective defensive cyberoperations, a shared understanding, openness, and communication are key to success. The fact that the actors are given the same desired end state is not necessarily what contributes to the most effective path to the goal.

Innholdsfortegnelse

Figuroversikt

Tabelloversikt

1 Innledning

«It is commonly believed that cyber-attacks are the weapon of the future. However, the war in Ukraine proved that this future is already here. Therefore, defense doctrines and international laws must adapt quickly» (Economic security council of Ukraine, 2022, s. 6).
Da Russlands storskala invasjon av Ukraina fant sted 24.Februar 2022 var dette starten på en ny moderne krig i Europa. Timer før de første Russiske stridsvognene krysset grensen inn i Ukraina var krigen i cyberdomenet allerede i gang. 23.februar ble wiper-programvare[1] rettet mot en rekke myndighetsorganisasjoner og kritisk infrastruktur i hele Ukraina (Microsoft, 2022, s. 7). På samme tid ble Russiske cyberoperasjoner rettet mot kommersielle satellittkommunikasjonsnettverk (VIASAT), trolig i den hensikt å ramme Ukrainsk evne til kommando og kontroll under invasjonen (Duguin & Pavlova, 2023, s. 10). Russland har ved flere anledninger siden invasjonen koordinert cyberoperasjoner med bruk av konvensjonelle våpen i den hensikt å ramme ukrainske myndigheter og den ukrainske befolkningen. Disse cyberoperasjonene er formet for å skape kaos og ramme kritisk infrastruktur, samtidig som det reduserer ukrainske myndigheters handlingsrom (Duguin & Pavlova, 2023, s. 9).

Kort tid før invasjonen hadde Ukraina endret lovgivning om databeskyttelse som tidligere ikke tillot offentlige etater å lagre data i offentlig sky. Før denne endringen ble Ukrainas digitale infrastruktur for offentlig sektor utelukkende lagret på servere i Ukraina. Dette gjorde den offentlige informasjonsinfrastrukturen sårbar for artilleri- og missilangrep. På grunn av beslutninger som å flytte kritisk data opp i skyen, hadde Russlands innledende operasjoner rettet mot ukrainsk digital infrastruktur begrenset operativ innvirkning i den innledende fasen av krigen (Microsoft, 2022, s. 5).

Det er mye å lære av krigen i Ukraina, som under arbeidet med denne oppgaven fortsatt pågår for fullt. Kombinasjonen av bruk av kinetiske og logiske virkemidler er et perspektiv mange har ment mye om, men som verden, og spesielt Europa, har hatt liten erfaring med. Den ukrainske forsvarskampen har foregått i alle domener og det er mye erfaring å trekke ut av det Ukraina opplever i cyberdomenet og øvrige krigføringsdomener som har avhengigheter til cyberdomenet. Som eksemplet over viser, vil defensive cyberoperasjoner som former lendet til egen fordel kunne ha en stor effekt. Det lendet som Russiske cyberenheter møtte de første dagene av invasjonen, var ikke det samme lendet de tidligere hadde kartlagt og forventet å møte.

[1] Programvare som er designet for å slette data fullstendig fra en datamaskin eller et annet digitalt lagringsmedium.

Det siste tiåret har vært preget av store endringer, i tiden før og etter den russiske invasjonen av Ukraina i 2014 og Russlands aggressive angrepskrig i Ukraina i 2022 har verden sett gjentatte eksempler på hvilken rolle cyberdomenet kan ha i en modernekrig. Mange ser til Ukraina for å lære av deres erfaringer og utvikle egne defensive kapasiteter for å stå imot fremtidige potensielle trusler og cyberangrep som understøtter russiske målsetninger (Willett, 2022, s. 9).

Siste langtidsplan for Forsvaret, «Forsvarsløftet», peker på at «Forsvaret skal kunne integrere cybersikkerhet og cyberoperasjoner i alle fellesoperasjoner». Videre fremheves det at «Forsvaret skal operere og løse oppdrag i alle domener selv om Forsvaret er utsatt for forstyrrelser, anslag og angrep i det digitale rom» (Prop. 87 S (2023–2024), pargr. 4.4). Dette medfører at Forsvaret må evne å gjennomføre effektive defensive cyberoperasjoner for å opprettholde egen handlefrihet.

1.1 Oppgavens relevans

At cyberdomenet har en rolle i moderne krigføring hersker det liten tvil om. Derimot er det uenighet blant forskere og praktikere om hvilken rolle domenet har og vil ha i en moderne konflikt. Til tross for at det er stor interesse rundt cyberdomenet og mye forskning som foregår innen fagfeltet, er litteraturen om cyberdomenets rolle i militære operasjoner og spesielt defensive cyberoperasjoner svært begrenset.

Cyberdomenet er noe som ikke bare påvirker militære operasjoner, og det vises omfattende interesse i sivil sektor. Mye av det publiserte materialet som omhandler cyberfaget er i stor grad rettet mot policy, strategi og administrativ cybersikkerhet. Litteratur som favner militære operasjoner fokuserer i stor grad mot det som skaper en målbar effekt, de offensive cyberoperasjonene.

Flere gode masteroppgaver skrevet knyttet til cyberdomenet de siste årene, og jeg har hentet inspirasjon fra oppgaver som *Militære operasjoner i cyberdomenet* (Rummelhoff, 2021), *Småstaten Norge – en cyberstormak*t? (Brunstad, 2018) og *Cybersikkerhet i væpnet konflikt* (Prestmo, 2015). Disse oppgavene tar for seg ulike tilnærminger til cyberdomenet i det norske Forsvaret. Oppgaven *Det fellesoperative problemet* (Martinsen, 2021) tar for seg hvorvidt Forsvarets operative hovedkvarter (FOH) er i stand til å lede fellesoperasjoner. Funn fra denne oppgaven har gitt inspirasjon til spissing av min egen problemstilling. I valg av teori er oppgaven basert på funn fra masteroppgaven *Militär innovation som resultat av aktörers mentala modeller av ny teknologi* (Modig, 2020) som fremmer et nytt perspektiv på innføring av cyberforsvar i Sverige og i høy grad kan relateres til min problemstilling.

1.2 Bakgrunn for oppgaven og problemstilling

Siden anerkjennelsen av cyberdomenet som et eget krigføringsdomene har det vært en vedvarende diskusjon om integrering av domenet i militære operasjoner. NATO har samlet allierte villige til å bidra med offensive kapasiteter, og NATOs Cyberdoktrine er utarbeidet (AJP-3.20, 2019). NATO Cooperative Cyber Defence Centre of Excellence har utviklet egne kurs for operasjonsplanleggere, utgitt «Cyber Commanders handbook» (CCDCOE, 2020) samt utgitt to volum av hvordan folkeretten gjør seg gjeldende i cyberdomenet og det tredje volumet er under utvikling (Schmitt, 2013, 2017).

Cyberdomenet fremstår enda som ungt og umodent og det er fortsatt mange problemstillinger å ta tak i. Militære doktriner om cyberoperasjoner er umodne og mangelfulle og det er min påstand at de heller ikke er operasjonalisert i tilstrekkelig grad, ei heller integrert i nevneverdig grad i multidomeneoperasjoner.

Ola Modig og Kent Andersson har studert i hvilken grad militære innovasjonsprosesser påvirkes av mentale modeller for ny teknologi. Denne tilnærmingen har dannet grunnlag for denne oppgaven og spisser deres tilnærming videre inn mot forholdet mellom det taktiske og operasjonelle nivået i det norske Forsvaret. Modig og Andersson sin studie indikerer blant annet at mentale modeller kan både hemme og fremme de militære innovasjonsprosessene, og at å utfordre mentale modeller og synliggjøre divergerende mentale modeller kan bidra positivt (Modig & Andersson, 2022, s. 58–59).

På bakgrunn av dette vil denne oppgaven søke å belyse følgende problemstilling:

> *«Hvorfor oppleves forholdet mellom taktisk og operasjonelt nivå som uavklart i planlegging og gjennomføring av defensive cyberoperasjoner som en del av fellesoperasjoner?»*

Problemstillingen vil søkes besvart på gjennom å belyse to forskningsspørsmål:

Forskningsspørsmål 1: Hvordan påvirker aktørenes mentale modeller og evne til militær innovasjon forholdet mellom taktisk og operasjonelt nivå innen defensive cyberoperasjoner?

Forskningsspørsmål 2: Hvordan kan doktrine bidra til en felles tilnærming til defensive cyberoperasjoner som en del av fellesoperasjoner?

1.3 Avgrensing

Fokus vil være på forholdet mellom taktisk og operasjonelt nivå i Forsvaret. Det er mange faktorer og aktører som har påvirkning på dette forholdet, men i denne oppgaven vil det avgrenses til å fokusere på aktører på taktisk og operasjonelt nivå.
Oppgaven vil også kun fokusere på defensive cyberoperasjoner og vil dermed ikke dekke cyberoperasjoner som helhet, ei heller offensive cyberoperasjoner.

Cyberdomenet i sin helhet er omfattende og komplekst. I det norske Forsvaret er ansvar og myndighet innen cyberoperasjoner fordelt på flere organisasjoner. Etterretningstjenesten som fagmyndighet er ansvarlig for helheten av domenet, mens Cyberforsvaret er delegert fagansvar for den delen som er cyberforsvar og cybersikkerhet. Offensive cyberkapasiteter er definert som en strategisk ressurs, og ansvaret er tildelt etterretningstjenesten (Forsvaret, 2019, pargr. 05122). Integrering av cyberdomenet i Forsvarets fellesoperasjoner vil på sikt inkludere både offensive og defensive kapasiteter. Cyberforsvar er en grunnstein for suksessen av operasjoner i øvrige domener. Oppgaven vil derfor avgrenses til å omhandle integrering av defensive cyberoperasjoner i fellesoperasjoner, og vil dermed ikke ytterligere berøre offensive cyberoperasjoner.

Skriftlige kilder som benyttes i oppgaven er utelukkende offentlig tilgjengelige kilder, dette vil avgrense analysen noe da graderte dokumenter kunne belyst problemstillingen ytterligere.

Oppgaven søker ikke å peke på feil, men heller å belyse utfordringer mellom taktisk og operasjonelt nivå, og vil heller ikke dekke tekniske aspekter av prosessene som omtales.

1.4 Oppgavens struktur

Oppgaven er strukturert i sju hovedkapitler. I dette første kapitlet er bakgrunn og beskrivelse av problemstillingen gjort rede for.

I kapittel 2 vil det gjøres rede for begreper og teori som benyttes videre i oppgaven. Med utgangspunkt i sentral litteratur fra fagområdet vil dette kapittelet redegjøre for hvor Forsvaret står i dag på veien mot integrering av defensive cyberoperasjoner i fellesoperasjoner.

I kapittel tre vil valgt metode for oppgaven beskrives og begrunnes. Forhold knyttet til metodekvalitet vil også belyses i dette kapitlet.

I kapittel fire diskuteres cyberdomenet og defensive cyberoperasjoner som en innovasjon i rammen av Everett M. Rogers fem karakteristikker for en innovasjon. Diskusjonen fortsetter i kapittel fem

«Spredning av innovasjon» hvor datamaterialet vil diskuteres i rammen av Rogers sin innovasjons-beslutningsprosess. Kapittel 6 vil ta for seg mentale modeller og doktrine i lys av funn fra de foregående kapitlene.

I kapittel sju fremlegges konklusjon og svar på problemstilling og forskningsspørsmål.

Avslutningsvis vil det deles noen tanker om mulig videre forskning.

2 Teori

I dette kapitlet vil først det teoretiske rammeverket som benyttes videre i oppgaven beskrives. Deretter vil det gjøres rede for sentrale begreper og utviklingen av cyberoperasjoner, hovedsakelig defensive cyberoperasjoner, i Norge og NATO. Hensikten er å skape et bakteppe for hva defensive cyberoperasjoner er og hvor Forsvaret er i dag i både etablering av cyberdomenet som et eget krigføringsdomene, og i integreringen av defensive cyberoperasjoner i fellesoperasjoner.

Oppgaven fokuserer på forholdet mellom taktisk og operasjonelt nivå i planlegging og gjennomføring av defensive cyberoperasjoner. Dette forholdet er analysert i rammen av militær innovasjonsteori, spredningsteori og aktørenes mentale modeller. Disse vil kort gjøres rede for nedenfor.

2.1 Teoretisk rammeverk

Endring er aldri enkelt, spesielt utfordrende kan det være i organisasjoner som er bygget opp etter faste rutiner og faste mønstre. Max Weber studerte byråkrati, og han argumenterte for at kjernen i byråkratier er orden, rutine og repetisjon, noe som skulle tilsi at de er bygget for å motstå endring eller innovasjon (Rosen, 1991, s. 2). Stikkordene orden, rutine og repetisjon er noe de fleste i en militær organisasjon vil kunne kjenne seg igjen i. Militære organisasjoner kan sies å være enda mer motstandsdyktig mot endring. Som Oberst John Mitchell fra den britiske hæren så direkte artikulerte det «Ikke i noe yrke er frykten for innovasjon så stor som i hæren» (Mitchell, 1838, s. 14). Mitchell baserte dette utsagnet på den argumentasjonen at offiserer starte sin karriere i forsvaret i en alder der de ikke former stort av egne meninger, og kommer inn i et system der de følger ordrer og den etablerte rutinen. De får sin oppvekst i en organisasjon som i stor grad styrt av en fastsatt struktur og kultur som vil være vanskelig å endre på senere i livet (Mitchell, 1838, s. 14).

Innovasjon som begrep benyttes ofte i dagligtalen om noe nytt og fremtidsrettet. «Innovasjon er å iverksette noe nytt som skaper verdi for innbyggerne og samfunnet».(Meld. St. 30 & (2019–2020), pargr. 3.1.1). En innovasjon er noe som individet anser som nyskapende, enten det er en idé, praksis eller gjenstand. At det anses som innovativt trenger ikke bety at det er noe helt nytt, men kan være noe en aktør har ny kunnskap om, nye tanker, eller nylig har besluttet å implementere (Rogers, 2003, s. 12). I offentlig sektor kan innovasjon referere til en ny tjeneste, et produkt, en prosess, organisasjonsstruktur eller måte å kommunisere på, enten det er helt nytt eller innebærer betydelige endringer (OECD & Eurostat, 2018).

Militær innovasjon refererer til introduksjon av nye ideer, konsepter, teknologier, eller taktikker som forbedrer en militær organisasjon sin operative evne. Stephen Rosen og Adam Grissom er begge prominente forskere innenfor militær innovasjon og selv om ingen av dem gir en direkte og tydelig definisjon av begrepet er de begge tydelige på at det innebærer en endring i operasjonell praksis som medfører en økning i militær effektivitet (Grissom, 2006, s. 907; Rosen, 1991, Kapittel 1). Militær innovasjon kan omfatte utvikling og implementering av nye våpensystemer, taktiske doktriner, organisatoriske strukturer eller operasjonelle strategier. Basert på dette vil innføringen av cyberdomenet i Forsvaret betraktes som en militær innovasjon.

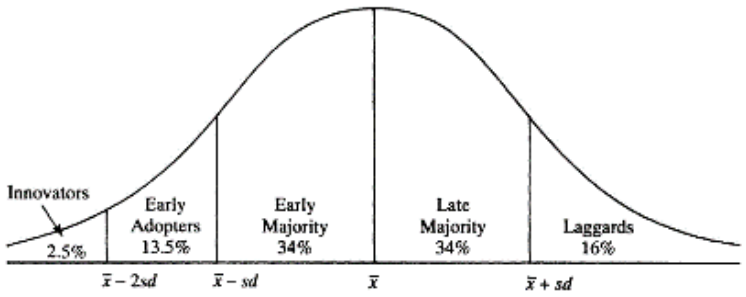
Innovasjon av ulik art vil skje av ulike årsaker selv innenfor samme organisasjon. Ulike organisasjoner vil også håndtere innovasjon forskjellig (Rosen, 1991, s. 12). Måten innføringen av cyberdomenet og defensive cyberoperasjoner er gjennomført på i Forsvaret er av stor betydning for dagens praksis, og data fra oppgavens respondenter vil analyseres i rammen av Rodgers spredningsteori. Rogers definerer innovasjon som en ide, praksis eller objekt som oppfattes som nytt av et individ eller en enhet, mens spredning (diffusjon) er «prosessen hvor en innovasjon er kommunisert gjennom visse kommunikasjonskanaler over tid til medlemmene av et sosialt system» (2003, s. 12, 2003, s. 5).

Rogers identifiserer at ulike innovasjoner kan ha svært ulike tidshorisonter for å nå en utbredt adopsjon. Han trekker frem at innovasjoner som oppfattes å ha større relativ fordel og kompatibilitet, mindre kompleksitet samt er etterprøvbare og observerbare, vil bli vedtatt raskere enn andre innovasjoner. Disse fem egenskapene er de viktigste egenskapene til innovasjoner for å forklare adopsjonshastighet (2003, s. 15–16).

«Relativ fordel (relative advantage) er i hvilken grad en innovasjon oppfattes som bedre enn ideen den erstatter. Kompatibilitet (compatibility) er i hvilken grad en innovasjon oppfattes å være i samsvar med eksisterende verdier, tidligere erfaringer og behov hos potensielle brukere. Kompleksitet (complexity) er i hvilken grad en innovasjon oppleves som vanskelig å forstå og bruke. Etterprøvbarhet (trialability) er i hvilken grad en innovasjon kan eksperimenteres med. Observerbarhet (observability) er i hvilken grad resultatene av en innovasjon er synlige for andre. «Jo lettere det er for enkeltpersoner å se resultatene av en innovasjon, jo mer sannsynlig er det at de tar den i bruk» (Rogers, 2003, s. 15–16).

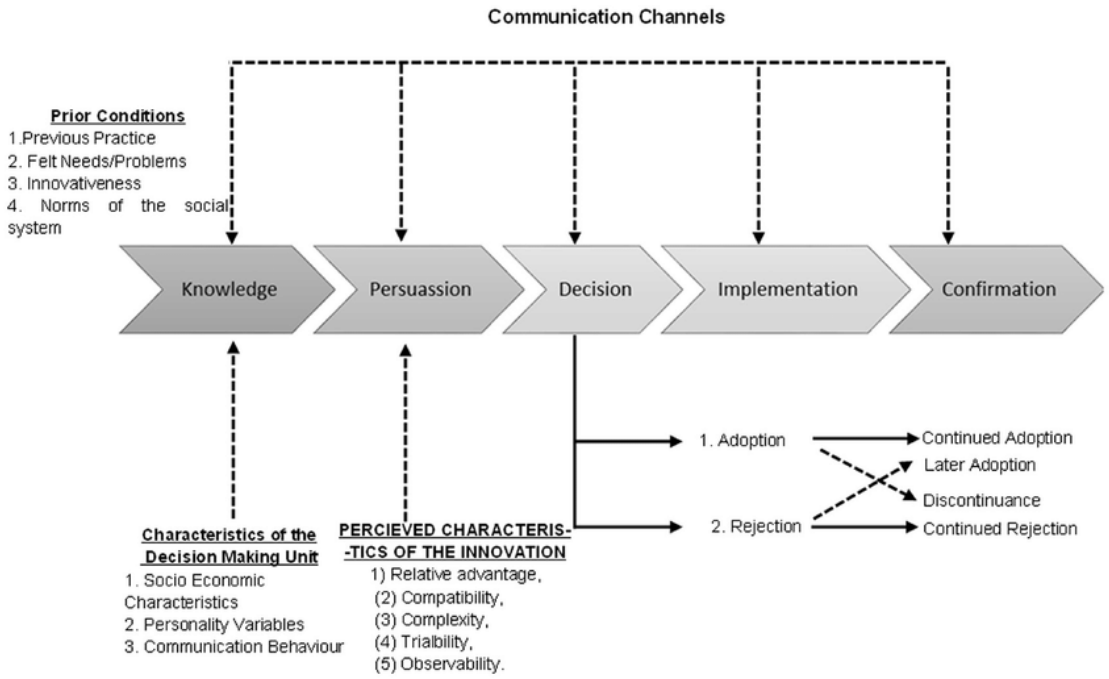
Rogers kategoriserer også aktørene i et innovasjonsmiljø basert på hvor tidlig de tar i bruk en innovasjon. Innovatører (innovators) er de første til å omfavne en ny idé, de har god teknisk forståelse og evner å håndtere høy grad av usikkerhet, eksperimentere og prøve ut nye ting. De

utgjør vanligvis en liten andel av befolkningen, men har en viktig rolle i å lansere nye ideer. Tidlige tilpasningsdyktige (early adopters) er også tidlig ute med å akseptere ideer, men er mer forsiktige og observerer innovatørene før de tar beslutninger. Denne gruppen utgjør en større andel av befolkningen enn innovatørene. Tidlig majoritet (early majority) representerer en betydelig del av befolkningen som aksepterer en innovasjon før gjennomsnittet, mens sen majoritet (late majority) er skeptiske til endring og aksepterer innovasjonen kun når den blir normen. Etternølere (laggards) er de siste til å omfavne en ny idé, de misliker endringer og ser ofte til hvordan ting er gjort tidligere. De utgjør den delen av befolkningen som sist aksepterer innovasjonen (Rogers, 2003, s. 282–285). Figur 2-1 illustrerer hvordan fordelingen av de fem aktørkategoriene følger en S-formet kurve som viser adopsjonstakten over tid.



Figur 2-1 Kategorier av aktører i et innovasjonsmiljø (Rogers, 2003, fig. 7–3)

Rogers forslår også en modell som identifiserer fem steg i en innovasjons-beslutningsprosess. Denne modellen beskriver hvordan aktører og organisasjoner tar beslutninger om å akseptere eller avvise innovasjoner. Som figur 2-2 viser, består denne modellen av stegene kunnskap, overtalelse, beslutning, implementering og bekreftelse (2003, s. 170).



Figur 2-2 Modell av de fem stegene i Innovasjons-beslutningsprosessen (Rogers, 2003, s. 170)

Steget kunnskap er når aktøren blir først kjent med innovasjonen, og lærer om dens funksjon. Overtalelse er der aktøren vurderer fordelene og ulempene ved innovasjonen og vurderer dens relevans og nytteverdi. Beslutning er når aktøren tar et valg om å akseptere eller avvise innovasjonen. Implementering skjer når aktøren tar en innovasjon i bruk. Bekreftelse er der aktøren søker støtte for en innovasjonsbeslutning som allerede er tatt, men kan omgjøre beslutningen dersom det kommer frem motstridende meldinger om innovasjonen. Aktører i denne settingen vil kunne være individer og/eller organisasjoner (Rogers, 2003, Kapittel 5).

Oppfattelsen av en innovasjon vil variere mellom de ulike aktørene i det sosiale systemet. For å bedre forstå hva som påvirker forholdet mellom taktisk og operasjonelt nivå vil det videre i oppgaven analyseres hvordan aktørenes mentale modeller påvirker deres forhold og deres evne til militær innovasjon, herunder implementering av defensive cyberoperasjoner som en del av fellesoperasjoner.

Mentale modeller kan ses på som interne prosesser hvor mennesker forstår omverdenen gjennom å konstruere modeller av den (Johnson-Laird, 1983, s. 4). Eller som Peter Senge mer direkte formulerer det «Mentale modeller er inngrodde antakelser, generaliseringer eller tankebilder; de påvirker både hvordan vi oppfatter verden og hvordan vi handler» (Senge, 1991, s. 14).

Dette utledes videre av filosofen Charles Sanders Peirce som beskriver deduksjon, en metode for å resonere som undersøker tingenes tilstand, danner et diagram (mental modell) av tilstanden og

oppfatter relasjoner som ikke fremgår spesifikt. For deretter gjennom mentale eksperimenter, fastslå at relasjonene alltid vil bestå i en grad og deres sannsynlige sannhet (Peirce, 1960, pargr. 66). I tråd med Peirce sin teori, mente Psykologen Kenneth Craik at dersom mennesker lager små interne modeller av virkeligheten for deretter å mentalt teste ut ulike handlemåter basert på egen kunnskap og erfaring, vil de kunne bruke dette til å agere på en bedre måte på fremtidige hendelser (Craik, 1967, s. 61). Peirce og Craik omtales som opphavsmenn for det som i dag innen kognitiv psykologi omtales som mentale modeller.

Mentale modeller benyttes for analyse av aktører på taktisk og operasjonelt nivå sin oppfattelse av defensive cyberoperasjoner som militært relevant. For oppgaven vil det derfor være hensiktsmessig å se til teorier om felles mentale modeller. Felles mentale modeller refererer til felles forståelse, kunnskap og oppfatninger som enkeltpersoner i en gruppe eller et team deler om en bestemt oppgave, mål eller situasjon som setter de i stand til å koordinere og tilpasse deres handlinger (Cannon-Bowers et al., 1993, s. 228).

Modig og Andersson har studert om aktører som deler lignende strategiske kulturer implementerer ny teknologi for militære formål ulikt. Resultatene de kom frem til viser at å tilstrebe felles mentale modeller av en teknologi, bidrar i større grad til nøyaktighet i militær innovasjon enn hva vurdering av strategisk kultur gjør. Studien konkluderer også med at beslutningstakere bør være bevisst forming av mentale modeller i kapasitetsutvikling. De mentale modellene kan bidra til å både hemme og fremme militær innovasjon, men prosessen drar mest sannsynlig nytte av at de mentale modellene blir utfordret (Modig & Andersson, 2022, s. 58–59).

2.2 Militære doktriners rolle

Ved innføring av nye krigføringsdomener kan måten krigføring gjennomføres på endres. Grunnleggende endringer vil potensielt kreve endringer i doktrine. I dette avsnittet vil det derfor kort gjøres rede for hva doktrine er, og hvilke doktriner som beskriver cyberoperasjoner.

NATO definerer doktrine som “Fundamental principles by which the military forces guide their actions in support of objectives. It is authoritative but requires judgement in application” (NATO, 2021b, s. 44).

FFOD stadfester at doktriner formidler militære erfaringer, definerer begreper og bidrar til standardisering av terminologi (Forsvaret, 2019, pargr. 01008). Doktriner vil legge grunnlaget for videre utvikling av fagområder gjennom konsepter, håndbøker og veiledninger.

Harald Høiback har forsket på militære doktriner i lang tid. Han argumenterer for at en god doktrine inneholder tre viktige elementer; teori, kultur og autoritet. Han hevder at doktriner trenger et element av teori som forklarer årsaken til anbefalinger eller krav som fremstilles i doktrinen. Videre må kulturelle hensyn inkluderes for å gi effekt, doktrinene må skrives på en måte som gjør at den favner det intenderte publikummet. Til slutt fremlegger han at enhver doktrine trenger en form for autoritet om den skal etterfølges, skal doktrinen være relevant må brukerne ha kjennskap til den og respektere den (Høiback, 2016). Høiback konkluderer også i sin bok Understanding Military Doctrine: A Multidisciplinary Approach med at doktrine kan benyttes både som ledelsesverktøy, endringsverktøy og læringsverktøy (2013).

I fortsettelsen er det to sentrale doktriner som omtales, AJP[2] 3.20, *Allied Joint Doctrine for Cyberspace Operations*, også omtalt som «Cyberdoktrinen», og *Forsvarets fellesoperative doktrine* (FFOD). AJP 3.20 er NATO doktrinen for planlegging, gjennomføring og vurdering av cyberoperasjoner i allierte fellesoperasjoner og bidrar til en viss grad til definering av begreper og standardisering (AJP-3.20, 2019). Doktrinene er en del av NATOs operasjonsarkitektur og underbygger AJP-3, *Allied Joint Doctrine for the Conduct of Operation*s (NATO, 2019).

FFOD ble sist gang revidert i 2019, og tok inn begreper fra AJP 3.20. FFOD stadfester og standardiserer begreper som benyttes i tilknytning til cyberdomenet, men går ikke i dybden på hvordan begreper skal forstås og omsettes i praksis. AJP 3.20 og FFOD er i liten grad operasjonalisert innenfor defensive cyberoperasjoner, og det finnes foreløpig ingen norsk doktrine for cyberoperasjoner eller defensive cyberoperasjoner. Når operasjonalisering av doktriner er mangelfull vil det være en risiko for at begreper tolkes ulikt og de underliggende prosessene på de ulike nivåene i Forsvaret utvikles i ulike retninger. Hensikten med doktrine er å skape felles mentale modeller hvor doktrinen vil fungere som et referansepunkt.

2.3 Utvikling av cyberdomenet

Cyber, Cyberspace, Cyberdomenet

«Cyberdomenet skiller seg fra andre domener ved at det er menneskeskapt, delvis ikke fysisk og ikke geografisk avgrenset» (Forsvaret, 2019, pargr. 05116). I tillegg er cyberdomenet et menneskeskapt domene hvor sivile og militære aspekter er tett sammenknyttet og kan i mange tilfeller være vanskelig å skille (Brantly, 2016, s. 1). Domenet med sin komplekse natur oppleves også som svært

[2] Allied Joint Publication

abstrakt og lite håndgripelig. «Cyberspace is the ultimate abstract realm, in which goals are achieved not by pushing matter around in space, but by manipulating intangible symbols and patterns» (Pinker, 2018, s. ii).

Bruken av begrepet cyber har siden dets opprinnelse vært omdiskutert og ulike tolkninger har oppstått. Begrepet «cyber» ble første gang benyttet av den amerikanske matematikeren Norbert Wiener i hans bok «Cybernetics: Or Control and Communication in the Animal and the Machine». Etymologisk stammer ordet «cyber» fra det greske ordet kybernetes, som betyr styrmann eller navigatør (Wiener, 1948).

William Gibson introduserte første gang begrepet «cyberspace» i sin novelle «Burning Chrome» fra 1982 for å referere til en datagenerert virtuell virkelighet (Gibson, 1982). Begrepet ble imidlertid ikke populært før Gibson igjen benyttet begrepet i romanen «Neuromancer», som også er den mest hyppig benyttede referansen til opprinnelsen av begrepene cyber og cyberspace (Gibson, 1984).

Bruken av begrepet cyberspace fra science-fiction litteraturen ble adoptert, og utover 1970 og 1980-tallet ble prefikset «cyber» knyttet til datamaskiner og det digitale domenet. Siden den gang har bruken av «cyber» blitt utvidet til å dekke et bredt spekter av digitale og datateknologiske konsepter. En studie identifiserte opp til 28 ulike definisjoner av «cyberspace» (Kramer et al., 2009).

Å finne en ensartet definisjon vil være krevende da tolkning av begrepet ofte er avhengig av kontekst og hvilket miljø det benyttes i. Bare i Norge benyttes ulike begreper og tolkninger i både norske offentlige utredninger, Forsvaret og Akademia. Denne variasjonen i bruk av begreper og definisjoner fremhever viktigheten av tydelighet i hvilken tolkning som benyttes i ulike studier og arbeidsgrupper. «Senior leaders do not always use the same lexicon- or use the same lexicon for different phenomena» (Smeets, 2022, s. 62). Som Smeets peker på, vil det kunne brukes samme ord om ulike fenomener noe som vil gjøre det vanskelig å gjennomføre sammenligninger på tvers av organisasjoner og nasjoner. Dette medfører også at komparative studier på cyberfeltet kan ha en grad av feilmargin basert på tolkninger av begreper og hvordan trusselen forstås.

Denne oppgaven benytter definisjoner stadfestet av NATO og Forsvaret. Allied administrative publication nr 6 (AAP-6)[3] definerer cyberspace som «Det globale domenet som består av all sammenkoblet kommunikasjon, informasjonsteknologi og andre elektroniske systemer, nettverk og

[3] AAP-6, er NATOs ordbok for militære termer og definisjoner (NATO, 2021b). Denne er grunnlaget for NATOs policy, doktriner og konsepter.

deres data, inkludert de som er atskilte eller uavhengige, som behandler, lagrer eller overfører data» (NATO, 2021b).

Forsvarsdepartementets cyberretningslinjer omtaler cyberdomenet som «Fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data. Synonym: Det digitale rom» (Forsvarsdepartementet, 2014). Mye har skjedd innen utviklingen av cyberdomenet siden retningslinjene ble utgitt i 2014, og denne definisjonen skraper kun i overflaten av hva som i dag ligger i begrepene cyberdomenet og det digitale rom. Forsvaret benytter definisjoner fastsatt i FFOD fra 2019:

> «Cyberdomenet er menneskeskapt, har global utbredelse og vokser raskt. Det består av informasjons- og kommunikasjonsteknologi og andre elektroniske systemer, de nettverk som knytter systemene sammen og informasjonen som behandles, lagres og overføres i nettverkene, herunder også systemer som er uavhengige av eller adskilt fra resten av nettverket» (Forsvaret, 2019).

FFODs definisjon av cyberdomenet fraviker ikke fra retningslinjene, men går mer i dybden og følger i større grad ordlyden fra NATO sin definisjon. I *FDs cyberretningslinjer* omtales «cyber» som et prefiks, mens i FFOD er det valgt å benytte begrepet frittstående og cyberdomenet benyttes fremfor NATOs begrep «cyberspace» (Forsvaret, 2019, s. 229; Forsvarsdepartementet, 2014, pargr. 1.4).

NATO benytter begrepet «cyberspace», norske myndigheter benytter i stor grad begrepet «det digitale rom», mens Forsvaret benytter begrepet «cyberdomenet». Felles for disse tre begrepene med tilhørende definisjoner, er at de omtaler domenet som sammenkobling av informasjons- og kommunikasjons teknologi, sammenkoblede nettverk og deres data. Mens NATO og FFOD går videre i å omtale domenet som globalt, og presiserer at definisjonen omfatter også systemer som ikke er sammenkoblet med øvrige nettverk. Videre vil begrepet «cyberdomenet» benyttes.

Cyber commander er et begrep som benyttes om Sjef Etterretningstjenestens delegerte myndighet for cyberoperasjoner. Begrepet i seg selv er ikke definert i verken AJP 3.20 eller FFOD. Sjef Etterretningstjenestens myndighet er synliggjort i FFOD som en koordinerende myndighet i den hensikt å sikre at «defensive cyberoperasjoner ikke kommer i konflikt med offensive cyberoperasjoner eller annen etterretningsaktivitet» (Forsvaret, 2019, pargr. 05122). Selv ikke i *Cyber commanders handbook* er det definert, utover at Cyber command omtales som den viktigste myndigheten for cyberoperasjoner (CCDCOE, 2020, s. 25). Sjef Etterretningstjenestens rolle som

Cyber commander omtales i *Konsept for nasjonale militære cyberoperasjoner* uten at begrepet defineres (Forsvaret, 2020).

Innenfor fagområdet er det en stor variasjon i bruk av begreper, dette kan føre til utfordringer når det kommer til samarbeid mellom ulike miljøer, og spesielt i fremskaffelsen av en felles situasjonsforståelse. Manglende standardisering og en felles tolkning av begreper kan føre til forvirring og misforståelser mellom ulike organisasjoner, nasjoner og miljøer. Cyberdomenet er svært dynamisk og teknologien utvikles raskt. I møte med stadig nye trusler må organisasjoner og deres prosesser også utvikles i høyt tempo, og dette vil skje uavhengig i mangelen på en felles standard. Dette vil kunne føre til at noen organisasjoner vil være lenger fremme i utviklingen, noe som kan ytterligere komplisere kommunikasjon og samarbeid. I møte med et komplekst trusselbilde vil en felles situasjonsforståelse være av stor viktighet. Manglende felles forståelse av grunnleggende begreper kan føre til misforståelser og feilaktige slutninger og beslutninger. Dette kan være spesielt problematisk under samarbeid og informasjonsdeling, hvor det er avgjørende å ha en enhetlig forståelse av begreper for å håndtere truslene effektivt. Når definisjoner og tolkninger av cyberdomenet divergerer vil dette kunne bidra til å øke avstanden, og komplisere viktig samarbeid mellom aktører fra ulike sektorer og miljøer.

Cyberdomenet i NATO

Selv om NATO alltid har beskyttet sine kommunikasjons- og informasjonssystemer, var det ikke før i 2002 under NATO toppmøtet i Praha at cyber ble satt på NATOs politiske agenda, og alliansens ledere ble enige om å styrke deres evner til beskyttelse mot cyberangrep (NATO, 2002, pargr. 4f). Under toppmøtet i Riga i 2006, ble behovet for samarbeid om deling av informasjon og etterretning for å beskytte vitale informasjonssystemer fremhevet (NATO, 2006, pargr. 24).

Estland, som på det tidspunktet var ett av NATOs nyeste medlemsland, ble i 2007 rammet av omfattende cyberangrep som lammet offentlige og private institusjoner (Russel, 2014, Kapittel 4). I kjølvannet av dette angrepet ble NATOs forsvarsministre enige om utarbeidelse av NATOs første Cyber Defence Policy (NATO, 2007, pargr. 17).

Estland hadde ved inntreden i Alliansen utarbeidet et konsept for et kompetansesenter innen cyberforsvar. De omfattende angrepene på Estland i 2007 ble en vekker for NATO og allierte. Samtidig viste konflikten mellom Russland og Georgia hvordan storstilte cyberangrep kunne kombineres med en konvensjonell militær invasjon (Russel, 2014, Kapittel 5). Dette viste Alliansen at cyberangrep hadde et stort potensial for å bli en viktig del av krigføring i fremtiden. NATO besluttet å

gi full akkreditering til Cooperative Cyber Defence Centre of Excellence (CCDCOE) som ble etablert i 2008 i Tallinn, Estland (*CCDCOE*, 2023).

Til tross for at Alliansen over de neste årene stadig innså det økende omfanget og konsekvensene av cyberangrep for nasjonal og NATOs sikkerhet og stabilitet, var det ikke før 2012 at cyberforsvar ble introdusert i NATOs forsvarsplanleggingsprosess (NATO, 2012, pargr. 49).

2014 var en viktig milepæl for utvikling av cyberforsvar i NATO. Under toppmøtet i Wales ble en ny cyber-policy vedtatt. I denne anerkjenner de allierte at cyberforsvar er en av NATOs kjerneoppgaver og en del av det kollektive forsvaret av Alliansen. Dette innebar at et cyberangrep på en alliert kunne være grunnlag for å påberope NATOs artikkel 5[4]. I den samme policyen anerkjente NATOs medlemsnasjoner også at folkeretten gjelder i cyberdomenet (NATO, 2014, pargr. 72 og 73).

Den neste store milepælen kom under NATO toppmøtet i Warszawa i 2016, der allierte statsoverhoder anerkjente cyberdomenet som et operasjonsdomene.

> «We agreed in Wales that cyber defence is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea" (NATO, 2016, pargr. 70).

Dette var et steg man ønsket skulle forbedre NATOs evne til å beskytte og gjennomføre operasjoner samtidig som handlefriheten ble opprettholdt i alle domener. Videre var det ønskelig med en ytterligere integrering av cyberdomenet i operasjonsplanlegging. I tillegg forpliktet de allierte seg gjennom Cyber Defence Pledge[5] til å prioritere styrking av cyberforsvar av nasjonale nettverk og kritisk infrastruktur (NATO, 2016, pargr. 70).

Under NATOs toppmøte i Brussel i 2018 bekreftet NATOs statsoverhoder NATOs defensive mandat, og deres besluttsomhet om å ta i bruk alle alliansens evner for å blant annet møte hele spekteret av cybertrusler. Dette inkluderer bruk av offensive cyberkapasiteter gjennom Sovereign cyber effects, provided voluntarily by Allies (SCEPVA)[6]. Cyberspace Operations Centre (CyOC) ble opprettet i den

[4] Artikkel i NATO traktaten om kollektivt forsvar, denne innebærer at et angrep mot ett eller flere medlemsland i NATO betraktes som et angrep mot alle medlemslandene.
[5] NATO Cyber Defence Pledge er et initiativ som ble lansert av NATO for å styrke medlemslandenes evne til å beskytte seg mot cybertrusler samt styrke NATOs kollektive forsvar gjennom et mer robust cyberforsvar. Medlemslandene forplikter seg til å investere ressurser for å oppfylle disse målene.
[6] Et rammeverk gjør det mulig for NATOs medlemsland på frivillig basis å bidra med offensive cyberkapasiteter til understøttelse av NATOs operasjoner og misjoner.

hensikt å bidra til situasjonsforståelse og for å koordinerer NATOs operative aktivitet i og gjennom cyberdomenet (NATO, 2018, pargr. 20).

Etter hvert som cybertruslene mot Alliansens sikkerhet tiltar i kompleksitet og hyppighet brukes et stadig tydeligere språk for å fremheve NATOs besluttsomhet til å møte hele spekteret av trusler i cyberdomenet. Gjennom NATOs toppmøter i de senere årene er NATO stadig tydeligere på at alliansen må aktivt avskrekke, forsvare seg mot og møte hele spekteret av cybertrusler til enhver tid – i fredstid, krise og konflikt – og på politisk, militært og teknisk nivå. Alliansen anerkjenner også at virkningen av betydelige, ondsinnede cyberaktiviteter kan, under visse omstendigheter, betraktes som et væpnet angrep (NATO, 2021a, pargr. 32).

I erkjennelsen av behovet for å motta støtte raskt, ble det ved siste NATO-toppmøtet i Vilnius i 2023, besluttet etablering av Virtual Cyber Incident Support Capability (VCISC). Dette skal på frivillig basis, og ved bruk av nasjonale ressurser, bidra til å bygge og øve en virtuell evne for rask reaksjon, og støtte nasjonale skadebegrensende tiltak som svar på omfattende ondsinnede cyberaktiviteter (NATO, 2023a, pargr. 66).

Utvikling av Cyberdomenet i Norge

Norge har fulgt utviklingen av cyberdomenet i NATO tett, og Norge har både signert Cyber defence pledge og ratifisert[7] NATOs Cyberdoktrine[8]. Utviklingen av defensive cyberoperasjoner i Forsvaret har pågått over flere tiår. I 2003 kom Norges første nasjonale strategi for digital sikkerhet (Handelsdepartementet, 2003) og i 2007 kom *Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010* (Justis- og politidepartementet et al., 2007). Den nasjonale strategien for digital sikkerhet har i lys av utviklingen av det stadig endrede trusselbildet vært gjennom revisjoner i 2012 og i 2019 (Fornyings-, administrasjons- og kirkedepartementet, 2012; Justis- og beredskapsdepartementet & Forsvarsdepartementet, 2019a). I 2019 ble strategien ytterligere styrket med en tiltaksplan og *Nasjonal strategi for digital sikkerhetskompetanse* (Justis- og beredskapsdepartementet, 2019; Justis- og beredskapsdepartementet & Forsvarsdepartementet, 2019b).

Begrepet informasjonssikkerhet dreide seg på tidlig 2000-tallet i hovedsak om å beskytte systemer og informasjon behandlet på disse systemene mot brudd på konfidensialitet, integritet og tilgjengelighet (Justis- og politidepartementet et al., 2007). *FDs cyberretningslinjer* ble utgitt i 2014, og var de første

[7] Innebærer at en stat folkerettslig forplikter seg til å overholde den aktuelle avtalen
[8] AJP 3.20 Allied Joint Doctrine for cyberspace operations

retningslinjene som tok for seg cyberterminologien (Forsvarsdepartementet, 2014). Disse retningslinjene er ikke revidert siden og er fortsatt gjeldende. Med retningslinjene ble det også en større tydelighet i oppgavene tildelt Cyberforsvaret innen defensive cyberoperasjoner (i retningslinjene definert som computer network defence). 2012 ble et vendepunkt for Forsvaret da Stortingsproposisjon 73 – «Et forsvar for vår tid» ble lagt frem. Denne fastslo at «Evnen til å bevare handlefrihet i det digitale rom har både en defensiv og en offensiv dimensjon som kan være utslagsgivende i militære operasjoner» (Prop. 73 S (2011-2012), pargr. 5.6). Det ble også fremhevet at «Forsvarssektoren skal kunne ivareta både defensive og offensive cyberoperasjoner som del av en fellesoperativ tilnærming» (Prop. 73 S (2011-2012), pargr. 10.4).

I anerkjennelsen av at Forsvaret skal være i stand til å håndtere cyberoperasjoner som rammer Forsvarets egne systemer ble det også vedtatt å styrke egen evne til å håndtere dette nye domenet og Forsvarets avdeling som da var kjent som Informasjonsinfrastruktur (INI) endret navn til Cyberforsvaret, og ble opprettet som egen driftsenhet i Forsvaret (Prop. 73 S (2011-2012), pargr. 7.8.3).

I 2015 kom rapporten fra Digitalt sårbarhetsutvalg (Lysneutvalget) som omhandlet digitale sårbarheter i det norske samfunnet (NOU 2015:13, 2015). I oppfølgingen av rapporten til Lysneutvalget kom i 2017 stortingsmeldingen «IKT-sikkerhet – et felles ansvar», den første stortingsmeldingen utelukkende viet til digital sikkerhet. Denne gir status på oppfølging av anbefalinger til tiltak fra Lysneutvalget (Meld. St. 38 (2016–2017)). I 2017 kom også Norges internasjonale cyberstrategi som tar for seg Norges strategiske prinsipper innen cybersikkerhet (Utenriksdepartementet, 2017).

I 2019 kom den per nå sist reviderte nasjonale strategien for digital sikkerhet (Justis- og beredskapsdepartementet & Forsvarsdepartementet, 2019a). Som en del av strategien ble Norge også fullverdig medlem av CCDCOE og ansatte en norsk representant ved senteret (Justis- og beredskapsdepartementet & Forsvarsdepartementet, 2019b, nr. 23).

En økt digitalisering av samfunnet, økte sårbarheter, komplekse verdikjeder og kompetente trusselaktører driver utviklingen av strategier, retningslinjer og doktriner. De strategiske dokumentene er på plass, men retningslinjer fra 2014 og strategier fra 2017 er langt fra relevante nok for det som kreves for å holde tritt med et høyst komplekst og dynamisk trusselbilde. I Forsvaret har fagmyndighet og ansvar blitt fordelt mellom Etterretningstjenesten og Cyberforsvaret, men

rammeverket for håndtering og koordinering er mangelfullt. Videre i denne oppgaven vil det gås nærmere inn på hvordan dette påvirker Forsvarets evne til å lykkes med defensive cyberoperasjoner.

Cyberoperasjoner og Defensive Cyberoperasjoner

I Norge ble defensive cyberoperasjoner først offisielt definert gjennom Forsvarsdepartementets «Cyberretningslinjer» (Forsvarsdepartementet, 2014). Senere har *Forsvarets fellesoperative doktrine* (Forsvaret, 2019) tatt inn begrepet og det er senere beskrevet ytterligere i *Konsept for defensive cyberoperasjoner* (Cyberforsvaret, 2022).

FDs cyberretningslinjer starter med å definere cyberoperasjoner som synonymt med datanettverksoperasjoner og operasjoner i det digitale rom. Cyberoperasjoner defineres som «tiltak som gjennomføres i datanettverkene for å påvirke motstanders datanett og beskytte eget nett» (Forsvarsdepartementet, 2014, s. 5–6). Det som i retningslinjene omtales som computer network defence (CND) og computer network attack (CNA), er tidlige begreper benyttet om det som i dag er kjent som defensive- og offensive cyberoperasjoner. «Computer Network Defense er å anse som en defensiv aktivitet som skal sikre handlefrihet i egen informasjonsinfrastruktur, til tross for offensive aktiviteter fra en motstander» (Forsvarsdepartementet, 2014, s. 6). Computer network attack anses i retningslinjene som offensive aktiviteter og gjennomføres normalt i en motstanders nettverk, «Computer Network Attack har til hensikt å redusere eller hindre en motstanders evne til å utnytte cyberdomenet til egne operasjoner» (Forsvarsdepartementet, 2014, s. 6).

Siden NATOs AJP 3.20 ble publisert i 2019 har norske offentlig dokumenter i større grad benyttet definisjoner stadfestet i denne. Dette innebærer blant annet at begrepene computer network defense og computer network attack i praksis er erstattet med nye begreper.

NATO definerer cyberoperasjoner som «handlinger i eller gjennom cyberdomenet i den hensikt å opprettholde egen og vennlig handlefrihet i cyberdomenet, eller å skape effekter for å oppnå militære mål» (NATO, 2021b). Denne definisjonen er satt sammen av definisjonene for det som utgjør cyberoperasjoner, defensive og offensive cyberoperasjoner. Defensive cyberoperasjoner, ofte forkortet DCO, er «Handlinger i eller gjennom cyberdomenet for å bevare egen og vennlig handlefrihet i cyberdomenet» (NATO, 2021b). Offensive cyberoperasjoner, ofte forkortet OCO, utgjør siste del av definisjonen «Handlinger i eller gjennom cyberdomenet som skaper effekter for å oppnå militære mål» (NATO, 2021b).

I Forsvaret benyttes hovedsakelig definisjonen fra FFOD. Denne definerer cyberoperasjoner som «militære eller strategiske handlinger som foregår i eller gjennom cyberdomenet for å sikre egen

handlefrihet, og ramme fienden for å oppnå militære eller strategiske målsettinger» (Forsvaret, 2019, pargr. 05106). Defensive cyberoperasjoner defineres som:

> «Tiltak og aktiviteter i den hensikt å sikre og forsvare en militær sjefs evne og mulighet til å utøve militær kommando, kontroll og kommunikasjon gjennom å beskytte egne informasjonssystemer. Tiltakene har til hensikt å hindre eller stoppe cyberangrep, redusere skaden og håndtere konsekvensene av et angrep» (Forsvaret, 2019, pargr. 05112).

NATO omtaler cybersikkerhet som «anvendelse av sikkerhetstiltak for beskyttelse av kommunikasjon, informasjon og andre elektroniske systemer, og informasjonen som lagres, behandles eller overføres i disse systemene med hensyn til konfidensialitet, integritet, tilgjengelighet, autentisering og sporbarhet» (AJP-3.20, 2019; NATO, 2021b, s. 4). FFOD omtaler defensive cyberoperasjoner som en del av cybersikkerhet sammen med sikkerhetsovervåking og er en «ønsket tilstand hvor kommunikasjons- og informasjonssystemer kan motstå påvirkninger i cyberdomenet som kan kompromittere konfidensialiteten, integriteten og tilgjengeligheten til digitale tjenester og den informasjon som lagres, behandles eller overføres av disse systemene» (Forsvaret, 2019, s. 229). Forsvarets definisjon av cybersikkerhet er i tråd med NATO, men FFOD går noe lenger i å sette cybersikkerhet i en operativ kontekst gjennom å utdype en hensikt om å sikre at militære styrker opprettholder handlefrihet og operativ evne (Forsvaret, 2019, pargr. 05111).

Cybersikkerhet, selv om det er en viktig del av fellesoperasjoner, vil ikke omtales videre, men omtales for å bidra til økt forståelse av begrepsbruk. Offensive cyberoperasjoner er beskrevet i den hensikt å gi et bilde på hva cyberoperasjoner som helhet er og hvilken relasjon det har til defensive cyberoperasjoner, videre vil det kun være defensive cyberoperasjoner som omtales.

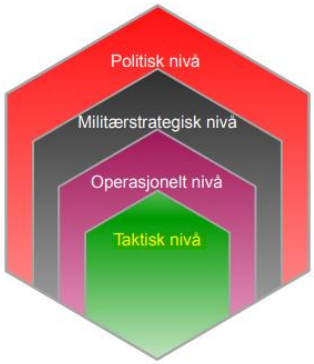
Som tidligere omtalt er ikke *FDs cyberretningslinjer* ikke oppdatert siden de ble skrevet i 2014 og er derav ikke endret siden AJP 3.20 ble ratifisert. Begrepene som stadfestes i retningslinjene er utdaterte og bidrar til ulik begrepsbruk internt i Forsvaret. Definisjonene som kommer frem i retningslinjene, har også et snevrere omfang enn de begreper som i dag benyttes i AJP 3.20 og FFOH. Der cyberretningslinjene fokuserer på beskyttelse av egne nettverk og påvirkning på en motstanders datanettverk, har både NATO og Forsvarets doktriner i større grad tatt inn over seg de operasjonelle konsekvensene av cyberdomenet. Begge doktrinene fremhever opprettholdelse av egen handlefrihet som kjernen i begrepet. FFOD har også et noe videre perspektiv på cyberoperasjoner enn NATO definisjonen. Der NATO kun omtaler opprettholdelse av handlefrihet i cyberdomenet, har Forsvaret et større perspektiv på å sikre egen handlefrihet uten å avgrense til cyberdomenet. Det som er felles for doktrinene og retningslinjene er at alle tydeliggjør av cyberoperasjoner kun omhandler aktivitet som

foregår i cyberdomenet (AJP-3.20, 2019, s. 4; Forsvaret, 2019, pargr. 05106; Forsvarsdepartementet, 2014, s. 6).

2.4 Fellesoperasjoner

Da problemstillingen fokuserer på defensive cyberoperasjoner som en del av fellesoperasjoner er det nyttig i fortsettelsen å se på hva fellesoperasjoner er og hvordan defensive cyberoperasjoner doktrinært er beskrevet som en del av fellesoperasjoner.

I en hierarkisk kommandokjede blir politiske ambisjoner blir omdannet til militære operasjoner, der hvert nivå har sine spesifikke roller og ansvarsområder i prosessen. Det politisk-strategiske nivået utvikler strategiske mål og ambisjoner, som blir overført til det militærstrategiske nivået. Det operasjonelle nivået utarbeider operasjonsplaner med konkrete oppdrag for taktiske styrker. FFOD definerer de fire kommandonivåene som vist i figuren: politisk, militærstrategisk, operasjonelt og taktisk (Forsvaret, 2019, pargr. 01007, 2019, pargr. 02081).



Figur 2-3 Kommandonivåer (Forsvaret, 2019, pargr. 02081).

NATO beskriver strategisk nivå som der en nasjon eller gruppe av land bestemmer nasjonale eller multinasjonale sikkerhetsmål og deployerer nasjonale, inkludert militære, ressurser for å nå dem (SHAPE, 2021, pargr. 1.11). Videre beskrives operasjonelt nivå som nivået som linker de militærstrategiske målsettingene til taktiske operasjoner innenfor et felles operasjonsområde (AJP-01, 2017, pargr. 1.24; NATO, 2019, pargr. 1.1). FFOD forklarer operasjonskunst og fellesoperasjoner som omsetting av strategiske mål og ambisjoner til taktiske handlinger (Forsvaret, 2019, pargr. 01006). NATO definerer taktisk nivå som der aktiviteter, slag og engasjementer planlegges og utføres for å oppnå militære mål tildelt taktiske enheter (SHAPE, 2021, pargr. 1.11).

Staber i militære organisasjoner ofte organisert i en funksjonell inndeling ut fra hvilke fagområder som dekkes. På operasjonelt nivå benyttes betegnelsen Joint (J) og de ulike fagfunksjonen omtales

som J1 til J10. J1 håndterer personell og administrasjon, J2 etterretning, J3 er ansvarlig for operasjoner, J4 logistikk, J5 håndterer planer og policy, J6 har ansvar for samband og informasjonssystemer, J7 øving og trening, J8 håndterer ressurser og økonomi, J9 ivaretar sivilt-militært samarbeid og til sist er J10 ansvarlig for prosjekter og utvikling (AJP-3, 2019, pargr. A.3-A.12; Forsvarets stabsskole, 2010, s. 47–50).

På operasjonelt nivå gjennomføres plan- og beslutningsprosesser i ulike tidshorisonter. Pågående operasjoner og operasjoner på mellomlang sikt håndteres av J3, mens utvikling, oppdatering og revisjon av planer håndteres av J5 (Forsvaret, 2019, pargr. 07051).

Ved Forsvarets operative hovedkvarter (FOH) gjennomføres beslutningsprosesser i den hensikt å synkronisere og samordne innsatsen, dette gjøres gjennom et stridshjul, eller en beslutningssløyfe som er et verktøy for å sikre nødvendig koordinering på tvers av fagområder og funksjoner. Beslutningssløyfen består av en rekke arbeidsgrupper og beslutningsmøter som følger en tidsmessig syklus. I disse møtene søkes det å opprettholde tempo i operasjonene samt fange opp eventuelle avvik i forhold til den gjeldende planen for deretter å gjøre korrigerende tiltak (Andersen & Ødegaard, 2016, s. 412, 2016, s. 446). Cyber working group (CyWG) er FOHs arbeidsgruppe for cyberoperasjoner som inngår i hovedkvarterets beslutningssløyfe (Cyberforsvaret, 2022, s. 26). Gruppen ledes av J6 cybersikkerhet og har deltagere fra de taktiske kommandoene og Etterretningstjenesten.

En fellesoperasjon defineres i FFOD som «En operasjon der elementer fra minst to forsvarsgrener deltar og der graden av samhandling er styrt fra et operasjonelt nivå» (Forsvaret, 2019, s. 232). NATO definerer «Allied Joint operations» som «An operation carried out by forces of two or more NATO nations, in which elements of more than one service participate» (NATO, 2021b, s. 10) og stadfester at «NATO recognizes that military success relies on a joint effort, usually with components and other force elements brought together under a unified command structure» (AJP-01, 2017, pargr. 4.1).

Å lede operasjoner fra fellesoperativt nivå er krevende. For å lede fellesoperasjoner kreves en grunnleggende forståelse for taktikken, samtidig som perspektivet må holdes på et operasjonelt nivå. Operasjonsmiljøet og avhengigheter må forstås (Vego, 2015, s. 63).

I Forsvarssjefens fagmilitære råd fra 2023 fastslås det at «Forsvaret skal gjennomføre fellesoperasjoner, som betyr at innsats fra styrker i alle domener må samordnes for å skape utfordringer for motstanderen» (Forsvaret, 2023, s. 30). Videre erkjennes det i det fagmilitære rådet at operasjonsmiljøet er i utvikling. Trusselbildet kombinert med introduksjon av nye domener som

cyberdomenet og rommet stiller nye krav til en helhetlig tilnærming og evne til å operere på tvers av alle domener. Dette krever konseptuelle endringer og det fagmilitære rådet løfter frem NATO sitt konsept for multidomeneoperasjoner (Forsvaret, 2023, s. 30).

En definisjon av et domene kommer frem verken fra NATO doktriner eller FFOD. Den mest nærliggende definisjonen er av operasjonsmiljøet som beskrives å bestå av «fysiske og ikke-fysiske domener, elementer, faktorer og betingelser som må forstås for å bruke stridsmidler, beskytte en styrke eller løse et oppdrag» (AJP-3, 2019, pargr. C.1; Forsvaret, 2019, pargr. 02008). NATO fastslår at innenfor NATO strukturen er det fem operasjonsområder; Land, sjø, luft, rom og cyber og omtaler disse videre som domener, uten beskrive sammenhengen mellom begrepene operasjonsområde og domene (NATO, 2023b). I FFOD omtales de fysiske stridsfeltene land, sjø, luft- og verdensrommet, og de ikke-fysiske stridsfeltene; informasjonsmiljøet, det elektromagnetiske spektrum og cyberdomenet som deler av operasjonsmiljøet, heller ikke i FFOD utdypes koblingen mellom stridsfelt og domener (Forsvaret, 2019, pargr. 02008)

Multidomene operasjoner er en videreutvikling av dagens fellesoperasjoner som i større grad tar inn over seg krigføringsdomener utover de tradisjonelle land, sjø og luft domenene. Der dagens fellesoperasjoner defineres med deltagelse fra minst to forsvarsgrener, legger MDO som en forutsetning at alle domener i større grad er til enhver tid samordnet. Dette er ytterligere definert i Prop 87 s;

> «MDO er en logisk videreutvikling av fellesoperasjoner til en mer domeneorientert tilnærming som søker å samordne militære og ikke-militære innsatser og aktiviteter for å oppnå rettidige og synkroniserte effekter og endringer som understøtter sikkerhets- og forsvarspolitiske målsettinger» (Prop. 87 S (2023–2024), pargr. 1.2.2)..

Cyberoperasjoner som en del av fellesoperasjoner er omtalt i FFOD, men utover å stadfeste at cyberoperasjoner og støtten til forsvarsgrenene koordineres av operasjonelt nivå gjennom den fellesoperative planprosessen, er det lite i FFOD som sier noe om hvilken rolle defensive cyberoperasjoner har eller kan ha i en fellesoperasjon (Forsvaret, 2019, pargr. 05127). *Konsept for defensive cyberoperasjoner* går lenger i å beskrive viktigheten av at defensive cyberoperasjoner samordnes og synkroniseres som en del av fellesoperasjoner, men også i dette konseptet er tilnærmingen overordnet og utdyper i liten grad hvordan defensive cyberoperasjoner i praksis kan understøtte fellesoperative målsettinger (Cyberforsvaret, 2022, Kapittel 9). Domeneorienteringen MDO bringer med seg legger i større grad til rette for en tettere integrering av cyberdomenet i operasjoner på alle nivåer.

2.5 Oppsummering

I dette kapitlet er det pekt på utfordringer med å implementere endringer i organisasjoner preget av faste rutiner, som byråkratiske og militære strukturer. Videre defineres innovasjon som implementering av noe nytt som skaper verdi, og militær innovasjon som endringer i operasjonell praksis for å øke militær effektivitet. Teksten bruker Everett M. Rogers' teori om spredning av innovasjon for å utforske hvordan innovasjon sprer seg og hvordan aktørenes mentale modeller påvirker deres evne til militær innovasjon, spesielt innen defensive cyberoperasjoner.
I kapittelet belyses også bruken og definisjoner av cyberdomenet i militære og NATO-kontekster. Videre redegjøres det for utviklingen av cyberdomenet i NATO og Norge, med fokus på etablering av doktrine og retningslinjer for defensive cyberoperasjoner. Avslutningsvis defineres kommandonivåene i Forsvaret, fellesoperasjoner og Multi-domene operasjoner.

3 Metode

En grundig metodebeskrivelse bidrar til transparens og åpenhet rundt forskningsprosessen. I dette kapitlet vil det derfor redegjøres for forskningsdesignet som er valgt for å svare på problemstillingen og forskningsspørsmålene. Det vil i dette kapitlet redegjøres for hvordan empiri er samlet inn og behandlet på en måte som ivaretar oppgavens validitet og reliabilitet (Jacobsen, 2015, s. 16). Metodetilnærmingen i arbeidet med oppgaven følger en stegvis prosess for strukturering av datamateriale. Først valg av forskningsdesign og innhentingsmetode, deretter utvalg av respondenter, utforming av tabletop og intervjuguide, innsamling av data, og til slutt kategorisering av datamateriale og analyse. Avslutningsvis vil jeg i dette kapitlet dele noen refleksjoner rundt hvordan valg av metode potensielt styrker eller svekker oppgavens reliabilitet og validitet

3.1 Metodisk tilnærming

Til forskjell fra de tradisjonelle domenene finnes det ikke årtier med erfaringer fra verken fredstid eller krise og krig i cyberdomenet. I Forsvaret finnes det lite dokumenterte erfaringer fra innføring av cyberdomenet og hvilke erfaringer som er gjort de årene siden defensive cyberoperasjoner ble en del av fellesoperasjoner. I denne oppgaven vil jeg derfor ta en eksplorerende, eller utforskende tilnærming for å finne svar på problemstillingen. Denne fremgangsmåten har til hensikt å utdype områder det finnes lite kunnskap om. En eksplorerende tilnærming er derfor godt egnet for oppgaver hvor det ikke er en omforent forståelse av fagområdet (Creswell & Creswell, 2023, s. 110; Jacobsen, 2015, s. 64).

For å svare på problemstillingen vil det benyttes et kvalitativt undersøkelsesopplegg som kombinerer aksjonsforskning og individuelle intervjuer. Ved kombinering av disse to metodene vil de sterke sidene ved én tilnærming kunne kompensere for svakheter ved den andre. På denne måten vil problemstillingen kunne belyses fra flere perspektiver og bidra til et mer helhetlig bilde av fenomenet som undersøkes (Jacobsen, 2015, s. 121, 174).

Jeg vil dermed kunne avdekke mer informasjon om hvordan defensive cyberoperasjoner gjennomføres i dag, samtidig som respondentens svar åpner for nye perspektiver og refleksjoner rundt hvordan de opplever dagens situasjon.

Kvalitativt forskningsdesign

I kvalitativ forskning kan ulike tilnærminger benyttes for å fremskaffe data, ofte benyttes metoder som intervju, dokumentanalyse og observasjon (Jacobsen, 2015, s. 157). Et kvalitativt undersøkelsesopplegg med åpne individuelle intervjuer er valgt som primærkilde for datainnsamling.

«Kvalitative studier gjør det mulig for forskere å forstå mennesker og deres handlinger. For å få inngående kjennskap til menneskets tanker og handlinger er deltakerperspektivet ofte det beste» (Granlund & Andersen, 2010, s. 71). Tematikk knyttet til cyberdomenet og defensive cyberoperasjoner er kompleks, og aktører på ulike nivåer kan sitte inne med svært ulike perspektiver. Det er ønskelig med åpen dialog for å få frem mulige friksjonsområder mellom taktisk og operasjonelt nivå, da kreves nærhet og tillitt mellom forsker og respondenter. I følge Jacobsen er kvalitativ metode godt egnet dersom oppgaven skal søke å få frem nyanserte beskrivelser og avklare uavklarte forhold knyttet til temaet (2015, s. 133).

Aksjonsforskning

En grunnleggende målsetning med aksjonsforskning er at den skal bidra til å skape kunnskapsutvikling og konkrete løsninger på aktuelle problemer (Levin, 2017, s. 35). I denne oppgaven vil det benyttes aksjonsforskning for å sammen med de som utøver faget, skape en forståelse av hvor Forsvaret står i dag i utøvelsen av defensive cyberoperasjoner.

Aksjonsforskning er en tilnærming som fokuserer på å løse praktiske problemer og skaper endringer i virkelige situasjoner gjennom en syklisk prosess av planlegging, handling, observasjon og refleksjon (Zuber-Skenitt, 1993, s. 45). I denne oppgaven vil kun deler av prosessen inkluderes, endring vil ikke innføres for å evaluere utfallet slik full syklus legger opp til. I søken etter svar på problemstillingen er

det hensiktsmessig å identifisere hvor Forsvaret står i dag og hvordan mentale modeller og doktrine kan påvirke dette. Det vil derfor potensielt identifiseres enkelte tiltak som kan skape den ønskede endringen, men oppgaven vil ikke strekke seg så langt i prosessen som til implementering og evaluering av disse tiltakene.

Aksjonsforskning som forskningsmetode har utviklet seg i mange retninger, og definisjonen av hva det er varierer mellom forskere og ulike konteksten hvor aksjonsforskningen finner sted. Felles for disse varierende definisjonene er at de har fokus på involvering av deltagerne, fremskaffelse av kunnskap og et mål om å oppnå sosial endring (Masters, 1995).

Videre i denne oppgaven vil følgende definisjon benyttes: «aksjonsforskning er samfunnsforskning utført av en gruppe som inkluderer en aksjonsforsker og medlemmer av en organisasjon, et fellesskap eller et nettverk som søker å forbedre deltakernes situasjon» (Greenwood & Levin, 2006).

Målet med aksjonsforskning er å generere kunnskap som ikke bare forstås, men også brukes til å føre til positiv endring eller forbedring i en bestemt kontekst. Problemstillingen for denne oppgaven er eksplorerende og vil søke å belyse noen av de utfordringene Forsvaret står ovenfor i utøvelsen av defensive cyberoperasjoner. Det anses derfor som hensiktsmessig å benytte et undersøkelsesopplegg som legger til rette for identifisering av disse utfordringene.

Aksjonsforskningen ble gjennomført i form av to tabletop-øvelser, en for en taktisk kommando, og en for operasjonelt nivå. En tabletop-øvelse er en uformell, diskusjonsbasert øvelse der en gruppe diskuterer sine roller og responser ved en situasjon som presenteres i form av øvingsscenarier med en eller flere hendelser. Tabletop-øvelse som verktøy er valgt på bakgrunn av dens effektive måte å kartlegge prosesser og hvordan deltagerne vurderer situasjonen uten at forskeren styrer utfallet ved ledende spørsmål. Metoden bidrar også til læring for deltagerne og har dermed også en positiv effekt for undersøkelsesenheten.

3.2 Datainnsamling

I dette avsnittet vil det redegjøres for hvordan datainnsamlingen ble gjennomført og hvilke vurderinger som ligger til grunn for utvalg av respondenter.

Valg av kilder

Respondenter i tabletop-øvelsene og intervjuene utgjør den primære datakilden i oppgaven. I valg av respondenter var det ønskelig med et bredt tverrsnitt av personell som jobber med defensive cyberoperasjoner som en sentral del av sine arbeidsoppgaver. Det var også ønskelig med

perspektiver fra personell som jobber med den faglige og konseptuelle utviklingen. FFOD stadfester at «Defensive cyberoperasjoner gjennomføres av Cyberforsvaret under kommando av SJ FOH, koordinert gjennom Cyberforsvarets operasjonssenter» (Forsvaret, 2019, pargr. 05122). Personell sentrale i denne prosessen fra både taktisk og operasjonelt nivå var derfor viktige å inkludere.

Defensive cyberoperasjoner gjennomføres i Forsvaret kun av en liten gruppe mennesker og det er få som har reell erfaring med denne type operasjoner. Selv om det er Cyberforsvaret som er delegert ansvar for gjennomføringen, vil øvrige taktiske styrkesjefer ha en viktig rolle, avhengig av hvor en cyberhendelse rammer. Det ble derfor vurdert som nyttig å inkludere en taktisk kommando som ikke har defensive cyberoperasjoner som primæroppgave. Uten at det er gjennomført en dyptgående analyse av kompetanse og modenhetsnivået innen cyberdomenet i de ulike taktiske kommandoene, kan det sies at nivået er svært varierende. Enkelte taktiske kommandoer har satt ressurser på å kurse opp eget personell samt inkludere cyberdomenet i eget planverk. Andre taktiske kommandoer har fortsatt en svært lav bemanning på fagområdet. Cyberdomenet har i disse organisasjonene ofte blitt nedprioritert, og har foreløpig en svært liten rolle i avdelingens planverk. For å benytte respondenter med gode forutsetninger til å reflektere rundt egen avdelings bidrag ble det valgt en taktisk kommando som har fremhevet seg i implementeringen av cyberdomenet i avdelingens operative planverk og organisasjon.

Som en viktig aktør i planlegging og gjennomføring av defensive cyberoperasjoner er deltagelse fra CyWG vurdert som sentral. FOH ved J6, sitter med et særskilt ansvar for denne gruppen i tillegg til å være koblingen inn mot hovedkvarteret i saker som angår cyberdomenet. Det var derfor naturlig at utvalget også omfattet personell fra FOH J6.

Cyberforsvaret som spydspissen innen Forsvarets utvikling, planlegging og gjennomføring av defensive cyberoperasjoner er en sentral del av oppgaven. Kunnskap og erfaring fra både konseptutvikling og planlegging og gjennomføring av operasjoner som dette personellet kan bidra med er nødvendig for oppgavens validitet og reliabilitet.

Tabletop-øvelse

Som en del av aksjonsforskningen er deltagelse fra respondentene en grunnleggende forutsetning. En taktisk kommando og en ad-hoc variant av FOHs CyWG, gjennomførte derfor hver sin tabletop-øvelse. Scenario for øvelsen ble utformet med støtte fra personell ved Cyberforsvarets Cybersikkerhetsavdeling. Disse har tidligere erfaring fra tjeneste knyttet til den taktiske kommandoen som skulle øves, og har erfaring med hvilke hendelser som er realistiske og kan ha

operative konsekvenser. Det var et mål i øvelsen å belyse dialogen mellom taktisk og operasjonelt nivå, derfor var det viktig med et scenario med konsekvenser ut over hva den rammede avdelingen selv kunne håndtere.

Kort tid etter øvelse GRAM[9] høsten 2023, da hendelser og erfaringer fra øvelsen fortsatt var friskt i minnet, ble første tabletop-øvelse gjennomført for den taktiske kommandoen. Etter øvelsen ble det også gjennomført individuelle intervjuer av respondentene. Disse har bidratt i utvikling av avdelingens operasjonsplaner, og inngår i avdelingens cybergruppe som samles ved mistanke om cyberhendelser som rammer avdelingen.

Andre tabletop-øvelse ble gjennomført under et arbeidsmøte i regi av FOH J6. Flere taktiske kommandoer var representert med personell som til vanlig inngår i CyWG. Tabletop-øvelsen ble gjennomført som en del av arbeidsmøtet. Det ble også her gjennomført individuelle intervjuer med enkelte av deltagerne fra operasjonelt nivå.

Første tabletop-øvelse ble innledet ved at den taktiske kommandoen presenterte sitt operative planverk og deres tilnærming til cyberdomenet. Deretter innledet jeg selve øvelsen med en scenario-presentasjon. Scenarioet illustrerte en situasjon tett knyttet opp mot Forsvarets pågående og fremtidige operasjoner. Scenario definerte et konkret oppdrag avdelingen skulle løse som en del av en fellesoperasjon. Deretter presenterte jeg deltakerne for en serie av hendelser som rammet subtaktisk nivå, hvor kritiske systemer ble satt ut av spill, og operativ evne kunne potensielt bli kritisk redusert om feilen ikke ble identifisert og utbedret. Hendelsene var utformet på en slik måte at det innledningsvis ikke fremgikk tydelig at dette var forårsaket av et cyberangrep. Gruppen diskuterte deretter hendelsesforløpet og kom frem til videre anbefalinger til håndtering, mens jeg observerte og noterte. Situasjonen i øvelsen eskalerte gjennom fremlegging av flere detaljer i hendelsesforløpet etter hvert som diskusjonen gikk fremover. Avslutningsvis ble deltagerne presentert med alle detaljene og den tiltenkte målsettingen med angrepet. Øvelsen ble avsluttet med refleksjon rundt hendelsen og hvordan gruppen tolket data de ble presentert med, og hvordan de selv opplevde relevansen av diskusjonen knyttet til det aktuelle cyberangrepet og andre tilsvarende situasjoner forårsaket av cyberhendelser. Med de potensielle konsekvensene for den taktiske styrkesjefens evne til å understøtte Sjef FOH, og kritisk reduksjon av FOHs handlefrihet ble det identifisert behov for å løfte hendelsen til operasjonelt nivå gjennom CyWG.

[9] Forsvarets årlige fellesoperative kommandoplassøvelse (CPX) for operasjonelt og taktisk nivå.

Dette la grunnlaget for den neste gjennomføringen av tabletop-øvelsen. Under gjennomføringen var 13 deltagere fra 6 ulike taktiske kommandoer og FOH J6 til stede. Øvelsen ble innledet med en kort introduksjon om masteroppgavens problemstilling og hensikt. Videre ble scenario og hendelsesforløp presentert av en av deltagerne fra den første tabletop-øvelsen, som ble gjennomført for en taktisk kommando. Vedkommende fungerte også som ordstyrer i tabletop-øvelsen for CyWG.

Data fra disse to gjennomføringene ble notert for hånd og videre renskrevet på PC uten gradert innhold. Refleksjoner jeg gjorde meg underveis i tabletop-øvelsene ble inkludert i de renskrevne notatene i egne avsnitt for bruk i den videre analysen og drøftingen.

Erfaringene fra tabletop-øvelsene var delte. Den taktiske kommandoen fremsto som svært interessert i å både lære, diskutere og bidra i oppgaven. Respondentene reflekterte over scenariet som ble lagt frem og deres egen rolle i denne settingen. Gjennomføringen for CyWG var noe mer avmålt da gruppen var større, varierte mer i kompetanse og bakgrunn, og besto av flere respondenter som ikke var delaktige i diskusjonen. Det var gode tilbakemeldinger på scenariet og tabletop-øvelse som verktøy for egen læring og diskusjon, men det fremkom langt mindre refleksjoner rundt egen rolle.

Intervjuer

Respondenter til intervju ble valgt ut blant deltagere i tabletop-øvelsene, samt nøkkelpersonell i Cyberforsvaret og FOH J6. Bakgrunn og erfaring blant respondentene var svært variert. Det ble inkludert personell fra flere ulike våpengrener, ulik erfaring og alder for å dekke et større spenn. Totalt ble åtte respondenter intervjuet for oppgaven.

Samtlige intervjuer ble gjennomført ansikt til ansikt, dette ble vurdert som mest hensiktsmessig for å skape tillit og får mest mulig refleksjoner og personlige oppfatninger fra respondentene. Intervjuene ble gjennomført på ulike steder da jeg reiste til respondentene og gjennomførte intervjuer i fortsettelsen av tabletop-øvelsene.

Intervjuene ble innledet med en presentasjon av bakgrunnen for masteroppgaven. Deretter ble respondentenes bakgrunn presentert med fokus på deres erfaring med defensive cyberoperasjoner. Dette bidro til en verifisering av respondentenes relevans for oppgaven, og for å få praten i gang i intervjusettingen. Samtlige respondenter leste og signert samtrykkerklæringen før intervjuet startet.

Intervjuene ble gjennomført semistrukturert, der respondentene i størst mulig grad snakket selv. Samtlige respondenter var svært positive til å stille til intervju, og fremsto som ivrige etter å dele sine

refleksjoner om temaet for oppgaven. En veiledende intervjuguide ble benyttet for å holde respondentene i gang, denne ble ikke delt i forkant av intervjuene. Intervjuguiden ble justert noe underveis i de ulike intervjuene da ikke alle spørsmål var relevante for samtlige respondenter (Se vedlegg C). Notater og lydopptak fra intervjuene ble renskrevet og transkribert før den videre analysen startet.

Skriftlige kilder

Data innhentet fra respondenter gjennom aksjonsforskning og kvalitative intervjuer utgjør den primære datakilden for oppgaven. Dette grunnlaget alene vil være noe tynt da det kreves mer kontekst for å tolke og forstå datagrunnlaget. Det er derfor benyttet sekundærkilder i arbeidet med utforming av problemstilling og tolking av data. Det finnes lite eksisterende litteratur om Forsvarets implementering av cyberdomenet og om hvordan integreringen av defensive cyberoperasjoner planlegges og gjennomføres. Dette er til dels reflektert i gradert planverk som Arctic Guard (strategisk nivå), Joint Guard (operasjonelt nivå) og Guard-planverket for taktisk nivå. Dette planverket holder for høyt graderingsnivå for inkludering i oppgaven. Det var derfor nødvendig å søke etter sekundærdata i åpne kilder. Det er viktig å bemerke at disse ikke nødvendigvis er direkte rettet mot de forskningsspørsmål som søkes å svare ut i denne oppgaven, men kan bidra til en forståelse av kontekst og de utfordringer som belyses. Disse kildene kan være preget av visse skjevheter, farget av andre forskeres perspektiver eller interesser (Jacobsen, 2015, s. 170–171).

Litteratursøk er gjennomført i Forsvarets høgskole sitt digitale bibliotek (Oria) og Forsvarets tilgjengelige databaser for å identifisere relevante kilder. I tillegg har det vært hensiktsmessig å se på utviklingen av cyberdomenet i Norge og i NATO gjennom offentlige dokumenter som Forsvarssjefens fagmilitære råd, Langtidsplaner for Forsvaret og NATOs kommuniké de siste ti-årene. Som nevnt i innledningen er det også hentet inspirasjon til oppgaven samt identifisert gode kilder gjennom arbeidet tidligere masterstudenter har gjort. Referanselister i andre masteroppgaver og forskningsartikler er benyttet for å identifisere relevante kilder.

3.3 Analyse

I kapittel 2 ble det gjort rede for teori som danner bakteppet, samt det teoretiske rammeverket som danner grunnlaget for kategorisering og analyse av det innsamlede datamaterialet. Videre i dette avsnittet vil det beskrives hvordan datamaterialet er brutt ned og kategorisert.
Jeg har valgt å benytte tematisk analyse for å bearbeide og analysere datagrunnlaget. Analyseprosessen er gjennomført i seks steg: (1) Bli kjent med datamaterialet, (2) generere

innledende koder, (3) søke etter temaer, (4) kontroll av temaer opp mot kodene, (5) definere og navngi temaer og (6) Utarbeidelse av drøftingen (Braun & Clarke, 2006, s. 87).

Ved kvalitative intervjuer er idealet at intervjuer skrives ut i sin helhet både for å forenkle analyseprosessen, men også for å muliggjøre at fortolkninger kan valideres gjennom å ettergå rådataen. Såkalte tykke beskrivelser som inneholder så mye detaljer som mulig, vil også tilrettelegge for en god og stringent analyse (Jacobsen, 2015, s. 202–205). Lydopptak ble derfor transkribert manuelt i sin helhet.

Gjennom å lytte til lydopptak og transkribere for hånd ble jeg godt kjent med materialet. Siden datainnsamlingen foregikk over noe tid, gikk jeg tilbake og lyttet og leste tidligere intervjuer. Allerede under datainnsamlingen var det enkelte temaer som skilte seg ut som noe som opptok respondentene, og gikk igjen i samtlige intervjuer. Disse observasjonene ble notert underveis.

Dette bidro videre til utvikling av de kodene jeg benyttet for å søke gjennom datamaterialet. Avsnitt som svarte til de ulike kodene ble klippet ut, merket med respondentkode (R1-8) eller tabletop-øvelse (T1-2) og samlet under en overskrift for hver kode.

Disse avsnittene ble deretter systematisert og kategorisert, kategoriene ble samlet i egne dokumenter for hvert tema. Etter hvert som kategoriene falt på plass gikk jeg gjennom datamaterialet på nytt for å verifisere at alle relevante utsagn om disse kategoriene var med videre i analysen. Jeg tegnet deretter flere skisser hvor jeg satte kategoriene opp mot hverandre og det begynte å bli klart at temaene korresponderte godt med innovasjons-beslutningsprosessen. Jeg fikk dermed et rammeverk for å sette kategoriene i en logisk rekkefølge. Tabell 3.1 viser korrelasjonen mellom innovasjons-beslutningsprosessen og temaene utledet gjennom analysen (Rogers, 2003, s. 170).

Tabell 3-1 Korrelasjon av Rogers' Innovasjons-beslutningsprosess og utledede temaer

Innovasjons-beslutningsprosess	**Kunnskap**	**Overtalelse**	**Beslutning**	**Implementering**	**Bekreftelse**
Tema fra datamaterialet	Kompetanse	Kompetanse blant beslutningstakere	Ledelse	Prosess	Evaluering

I siste steg ble disse temaene med tilhørende utdrag fra datamaterialet drøftet opp mot den relevante teorien for å svare ut oppgavens problemstilling.

Hvordan teorien benyttes i oppgaven

Hensikten med oppgaven er å belyse hvorfor forholdet mellom taktisk og operasjonelt nivå oppleves som uavklart i planlegging og gjennomføring av defensive cyberoperasjoner som en del av fellesoperasjoner. Dette vil det søkes å finne svar på ved hjelp av de to forskningsspørsmålene:

F1: Hvordan påvirker aktørenes mentale modeller og evne til militær innovasjon forholdet mellom taktisk og operasjonelt nivå innen defensive cyberoperasjoner?

F2: Hvordan kan doktrine bidra til en felles tilnærming til defensive cyberoperasjoner som en del av fellesoperasjoner?

Jeg vil drøfte datamateriale i konteksten av Everett M. Rogers' spredningsteori og fem karakteristikker for innovasjoner for å belyse hvordan disse påvirker adopsjonsraten av cyberdomenet og defensive cyberoperasjoner som en innovasjon. Videre vil jeg benytte spredningsteorien, og drøfte datagrunnlaget i rammen av Rogers' fem steg for en innovasjons-beslutningsprosess (Se Figur 2-2). Denne modellen operasjonaliseres gjennom at den brytes ned i temaer som benyttes som kategorier i analysen av datamaterialet (ref. tabell 3.1).

Teori om mentale modeller vil benyttes for å belyse hvorvidt felles eller divergerende mentale modeller fremmer eller hemmer evnen til å drive defensive cyberoperasjoner som en del av fellesoperasjoner. Mentale modeller vil også benyttes kombinert med militær innovasjonsteori som en forklaringsmodell i den hensikt å tolke aktørenes oppfatning og forståelse av forholdet mellom taktisk og operasjonelt nivå. Avslutningsvis vil jeg se mot militær doktrine og hvilken rolle denne har og kan ha.

3.4 Metodekvalitet

Innsamling av kvalitativ data kan foregå gjennom flere metoder, som individuelle eller fokusgruppe intervju, observasjon eller dokumentundersøkelse. Valgt metode for datainnsamling vil kunne ha en innvirkning på dataenes validitet. Metoden som benyttes kan påvirke resultatene gjennom begrensninger i innsamlingen eller forskerens fortolkning av dataen (Jacobsen, 2015, s. 145–146).

Undersøkelsesopplegget som er benyttet i denne oppgaven, søker å tilfredsstille krav om validitet (gyldighet) og reliabilitet (troverdighet) (Jacobsen, 2015, s. 16).

Jeg har i undersøkelsesopplegget inkludert aksjonsforskning. Morten Levin identifiserer fire variabler som er sentrale for god kvalitet på aksjonsforskningen. Disse er «bred lokal deltakelse, kontroll av forutinntatthet, samarbeid mellom flere forskere og systematiske data om endringsprosessen» (Levin, 2017, s. 35).

Validitet

Med validitet menes at empirien, eller dataen skal være gyldig og relevant, det vil si om det faktisk gir svar på den problemstillingen og de forskningsspørsmålene oppgaven søker å finne svar på. Den interne gyldigheten innebærer at det finnes dekning for mine konklusjoner i dataen som ligger til grunn, mens ekstern gyldighet er hvorvidt funnene er overførbare til andre sammenhenger og dermed kan generaliseres (Jacobsen, 2015, s. 17, 2015, s. 228).

For å være sikker på at dataen jeg har samlet inn faktisk svarer på problemstillingen har jeg justert på intervjuguiden underveis i tråd med de endringer som ble gjort i problemstillingen. I ett tilfelle har jeg også gått tilbake til en respondent for å få en bedre utdyping innenfor den nye retningen problemstillingen tok.

Generalisering har ikke vært et mål i seg selv da jeg har studert et smalt felt innenfor en spesifikk kontekst. Enkelte funn vil være gjeldende for forholdet mellom taktisk og operasjonelt nivå i andre kontekster også, men dette har ikke vært et mål og er heller ikke vurdert i oppgaven. Aksjonsforskning som samfunnsforskning mottar sterke kritikker for den manglende muligheten for å generalisere forskningsresultatene. Resultatene er ofte sterkt knyttet til spesifikke kontekster og er preget av deltagernes unike perspektiver og kompetanse. Ved gjennomføring av en tilsvarende tabletop-øvelse med andre deltagere og en annen setting, vil potensielt få andre utfall.

Fagmiljøet i Forsvaret som arbeider med defensive cyberoperasjoner er svært lite. Til tross for at tilnærmingen i liten grad legger til rette for generalisering, vil det være naturlig at flere av Forsvarets avdelinger og taktiske kommandoer, står ovenfor mange av de samme utfordringene. Det vurderes derfor som hensiktsmessig å benytte denne tilnærmingen. Selv om den ikke vil la seg generalisere til andre land og andre miljøer, vil det allikevel kunne tillate en viss generalisering innenfor det avgrensede miljøet i Forsvaret. Tett korrelasjon mellom funn i oppgaven og Everett M. Rogers forskning indikerer også en større grad av generaliserbarhet enn hva jeg innledningsvis hadde forventet.

Til tross for kritikk av aksjonsforskning som samfunnsvitenskapelig metode vurderes den som hensiktsmessig for å søke svar på problemstillingen for denne oppgaven. Mangel på muligheter for generalisering anses som mindre relevant i den kontekst oppgaven skrives. Et fagmiljø med engasjerte respondenter taler også til fordel for deres deltagelse i oppgaven.

Ved bruk av aksjonsforskning i undersøkelsesdesignet er det en viss fare for at data som innhentes ikke er relevant for problemstillingen. Gjennom å ta liten styring under tabletop-øvelsene og gi stort spillerom for fri diskusjon hadde jeg liten kontroll over hvilken retning diskusjonen tok. Det var derfor viktig med et realistisk og relevant scenario som trigget den problemstillingen jeg ønsket å belyse. Dette ble ivaretatt gjennom støtte til utarbeidelse av tabletop-øvelsen fra personell med god kjennskap til fagområdet og erfaring med tabletop-øvelser. Jeg sparret med flere kollegaer for å finpusse scenarioet. Deltagerne i øvelsen kjente ikke innholdet før selve gjennomføringen.

For å sikre kvalitet i aksjonsforskningen må forskningsstrategien være transparent, det må være mulig for andre å ettergå arbeidet som er gjennomført (Levin, 2017, s. 36). Ved forskning på et snevert fagområde, som cyberoperasjoner i Forsvaret, vil det være en hårfin balanse mellom transparens og prinsippet om å bevare respondentenes anonymitet. I små fagmiljøer er det vanskelig å bevare anonymiteten, og det vil kunne gå på bekostning av transparens. Det er ikke identifisert hvilken taktisk kommando som deltok i tabletop-øvelsene, både for å bevare deltagernes anonymitet, men også av graderingshensyn. Detaljgraden av scenario for tabletop-øvelsen gjengis i oppgaven med et minimum av detaljer av gradering- og sensitivitetshensyn. Det vurderes allikevel at metoden er hensiktsmessig og at empiri fra øvelsen er relevant for å gi den kunnskap og innsikt som kreves for å svare på problemstillingen.

For å understøtte observasjoner fra aksjonsforskningen er denne supplert med individuelle intervjuer både av deltagere fra tabletop-øvelsene og av andre relevante respondenter. På denne måten kan empiri fra de to tilnærmingene skape en større bredde og dybde i forståelsen av problemstillingen. Kombinering av data på denne måten kan bidra til å øke validiteten til undersøkelsene (Jacobsen, 2015, s. 138–139).

Reliabilitet

At oppgaven bør tilfredsstille krav om reliabilitet, eller troverdighet, betyr at undersøkelsene gjennomført er til å stole på, og at det er gjennomført på en måte som gir tillit til resultatene (Jacobsen, 2015, s. 17). Min strategi for å ivareta reliabiliteten i oppgaven har vært å dokumentere i så stor detalj som mulig de stegene som er gjennomført i undersøkelsene (Creswell & Creswell, 2023,

s. 215). Der det har vært mulig er det gjennomført lydopptak, disse lagres til forskningsprosjektet er avsluttet. Alle lydfiler er transkribert manuelt og deretter gjennomgått for å avdekke eventuelle feil.

Mangel på objektivitet kan også være en utfordring i gjennomføring av aksjonsforskning da forskeren selv vil bli en deltagende part. Som en kombinasjon av å være den som innfører en endring og samtidig være forsker, må det være en sterk bevissthet rundt egen rolle og mulig påvirkning på empirien (Jacobsen, 2015). Å forske på egen praksis kan være krevende da det er hensiktsmessig å holde empirien fri for egne fordommer og forutinntatthet. For å redusere mitt eget fotavtrykk i er det gjort et bevisst valg om at jeg ikke deltar i diskusjonen eller er deltagende utover å legge frem dilemmaer for diskusjon. Tabletop-øvelsene ble gjennomført som en åpen, ikke-deltagende observasjon for å registrere adferden og avdekke hvordan gruppene vil handle i gitte situasjoner. Dette har en svakhet i at det ikke gir rom for å observere hva den enkelte deltager opplever eller hva de mener. For å ivareta observasjonenes reliabilitet suppleres derfor tabletop-øvelsene med intervjuer av deltagerne for å fange opp deres subjektive meninger, deres opplevelse av situasjonen og generelle refleksjoner (Jacobsen, 2015, s. 166–167).

Respondentene i både tabletop-øvelser og intervjuer er anonymisert. Respondentenes anonymitet gir rom for en større grad av åpenhet og fritt talerom. Samtidig er dette en svakhet da det vanskeliggjør etterprøvbarheten av funnene. Den vurderingen jeg som forsker har gjort i analyse og fortolkning av empirien vil kunne farges av hvordan jeg kjenner respondentenes stilling, kompetanse og erfaring. Enkelte respondenters bakgrunn vil medføre at deres uttalelser kan veie tyngre enn andre respondenter uten samme grad av kompetanse og erfaring. Anonymisering av deltagere vil derfor kunne svekke oppgavens troverdighet da leseren ikke gis det samme grunnlaget for å vurdere de funnene jeg er kommet frem til. Leseren gis heller ikke mulighet til å vurdere relevansen av den taktiske kommandoen som ble valgt ut til å gjennomføre en tabletop-øvelse da denne også er anonymisert. Cyberfagfeltet er lite og ved å kun identifisere hvilken avdeling som har deltatt vil i stor grad identifisere respondentene.

Begge gjennomføringene av tabletop-øvelser ble gjennomført på område godkjent for HEMMELIG. Dette medførte at lydopptak ikke var mulig og notater ble skrevet for hånd. Etter gjennomføringen fikk jeg mulighet til å be om gjentakelse eller utdyping der jeg ikke hadde fått gode nok notater. At tabletop-øvelser og enkelte intervjuer ikke er tatt opp på lydfil eller transkribert i sin helhet vil svekke tilgangen på rådata og detaljgraden i mine notater er derfor viktig.

Intervjuer ansikt-til-ansikt legger til rette for en bedre flyt i samtalen og åpenhet mellom intervjuer og respondent. Min rolle som forsker i denne settingen, kan ha en påvirkning på resultatet. I et

intervju gjennomført på denne måten vil intervjueffekten være en faktor som må tas med i vurderingen (Jacobsen, 2015, s. 148). Dette er en av utfordringene med å forske på et tema der en selv er tett på problemstillingen. Jeg har tatt et tydelig standpunkt til at jeg ikke hadde noen rolle i intervjuene utover å sette rammene, lytte og observere. Dette ble også formidlet til respondentene ved starten av intervjuet for å unngå usikkerhet.

Enkelte intervjuer ble gjennomført i lokaler godkjent for HEMMELIG og det ble ikke benyttet lydopptaker. Det ble vurdert som hensiktsmessig at respondentene kunne uttale seg fritt uavhengig av graderingsnivå, og graderte kommentarer ble senere utelatt fra renskrevne notater. I de intervjuene hvor lydopptaker ble benyttet ble respondentene informert om dette og oppfordret til å indikere dersom de ønsket å gå inn på gradert informasjon. Ved disse tilfellene ble lydopptaket satt på pause til respondenten gikk tilbake til ugradert informasjon.

Uten lydopptak av samtlige intervjuer vil det ikke være mulig med komplett transkripsjon av alle intervjuene, og enkelte utsagn som ikke er notert kan går tapt. Det vil heller ikke være mulig å sitere alle respondentene da notatene er i stikkordsform. Det er også en risiko ved denne fremgangsmåten at utsagn kan misforstås i analysen da det vil være mindre kontekst tilgjengelig enn der det finnes en komplett transkripsjon.

Forskerens rolle og egne refleksjoner

Underveis i arbeidet med oppgaven ble problemstillingen og forskningsspørsmålene omformulert. Dette ble gjort både for å gjøre spisse problemstillingen, men også for å gjøre problemstillingen mer forskbar. Problemstilling og forskningsspørsmålene ble endret etter at de første intervjuene var gjennomført. For å bevare konsistens i intervjuene ble det ikke gjort større endringer i intervjuguiden, men noe av dataen som ble innsamlet var ikke lenger relevant for oppgaven og ble utelatt i analysen.

Å forske på egen praksis kan ha både sine positive og negative sider. Ved å ha en nærhet til respondenter og til organisasjonene som undersøkes er det, spesielt i et smalt fagfelt som defensive cyberoperasjoner, svært nyttig å ha god kjennskap til personer både for å finne det rette utvalget, men også for å få mest mulig ærlige svar. Det er også en stor fordel å forstå sjargongen og «stammespråket» som benyttes for å kunne forstå og fortolke dataen med høy grad av troverdighet (Jacobsen, 2015, s. 56).

På den andre siden kan det være utfordrende å ha for høy grad av nærhet til problemstillingen. Personer og organisasjoner som undersøkes skal i minst mulig grad farges av min egen

forutinntatthet og personlige meninger. Etter å ha jobbet innenfor fagområdet i mange år er det vanskelig å legge vekk egne meninger og ha et åpent sinn for hva respondentene uttrykker. I tillegg er det lett å la seg rive med av respondentenes resonnementer da jeg selv har god kjennskap til utfordringene de står i, og det kan være vanskelig å holde seg nøytral og ha et kritisk blikk på datagrunnlaget (Jacobsen, 2015, s. 57). Etter å ha tjenestegjort i Cyberforsvaret i en årrekke vil potensielt også respondentene betrakte meg som en representant for Cyberforsvaret selv om jeg i denne settingen tilstreber å ha en nøytral rolle som forsker. Dette vil kunne prege det datamaterialet jeg samler inn, da respondentene i større grad kan vinkle sine svar inn mot Cyberforsvaret og Cyberforsvarets operasjonssenter (CDOC) sin rolle.

Etter å ha jobbet innenfor fagmiljøet i mange år, er det vanskelig å finne respondenter som både er relevante for oppgavens problemstilling, og som jeg ikke allerede har en relasjon til. Min opplevelse av arbeidet med oppgaven har vært at respondenter har vært svært forståelsesfulle for denne problemstillingen og har i liten grad gått inn i diskusjoner med meg, men heller snakket fritt og åpent om egne erfaringer. Det var også viktig å ta så liten rolle som mulig i gjennomføringen av tabletop-øvelsene. I frykt for å fremstå som en som forsøker å kontrollere eller evaluere mine kollegaer, var det enklere å ha en rolle som ren observatør. Spesielt i tabletop-øvelsen for CyWG var det viktig for meg å ta et steg tilbake, og ved å ikke være endringsagenten var det også mulig å ikke bli med i diskusjonen. Dette valget har jeg vært svært fornøyd med i etterkant, da respondenten som tok denne rollen gjorde dette på en svært god måte som også tilførte øvelsen en større grad av realisme.

Erfaringer etter gjennomførte intervjuer er at selv om intensjonen var god med stor bredde i kompetanse og erfaring blant respondentene, så er det er liten variasjon mellom respondentenes uttalelser. De yngste og mest uerfarne berørte de samme temaene som de mest erfarne, om enn noe mindre utfyllende.

Etiske avveiinger

Ved forskning på egen praksis er det flere etiske avveiinger forskeren må ta hensyn til. «Samfunnsvitenskapelige undersøkelser har konsekvenser, både for dem som blir undersøkt og for samfunnet» (Jacobsen, 2015, s. 45). Etter å ha jobbet innenfor cyberfagfeltet i 15 år er det vanskelig å bevare min nøytralitet som forsker. Dersom jeg ikke har et bevisst forhold til dette vil det kunne innebære at jeg tar med meg mine egne erfaringer og oppfatninger som kan påvirke kvaliteten på innsamling av data og analysen.

Konfidensialitet og anonymitet står sentralt i kvalitativ forskning, og ved mindre utvalg vil det være større muligheter for å identifisere respondentene (Jacobsen, 2015, s. 49–50). Dette er søkt ivaretatt gjennom at respondentenes identitet ikke er nedtegnet, men kun tildelt koder. Avdeling er heller ikke gjengitt i oppgaven da det vil være mulig å identifisere enkeltpersoner dersom dette gjøres kjent. Navn og avdeling fremkommer ikke i lydfiler eller notater. Samtlige deltagere har signert på samtykkeerklæring hvor de er gitt informasjon om formålet med oppgaven, hva deltakelsen vil innebære, og hvilke rettigheter de har. Godkjenning for bruk av respondenter er også innhentet fra deres ledere.

Analyse og fortolkning av innsamlet data vil innebære en reduksjon av detaljer. Idealet om fullstendig gjengivelse vil aldri kunne oppnås, men tilstrebes (Jacobsen, 2015, s. 52). For å sikre best mulig gjengivelse av innsamlet data har jeg så langt det har latt seg gjøre tatt notater og lydopptak fra all interaksjon med respondenter.

Undersøkelsene er gjennomført etter godkjenning fra Sikt (Vedlegg A) og Forsvaret, dette inkluderer å anonymisere dataene og sørge for at sensitive opplysninger ikke blir identifisert.

4 Cyberdomenet og defensive cyberoperasjoner som innovasjon

I Everett M. Rogers' teori om spredning av innovasjoner beskrives karakteristikker for typiske innovasjoner som påvirker hvor raskt innovasjonen adopteres. De fem viktigste karakteristikkene er relativ fordel, kompatibilitet, kompleksitet, etterprøvbarhet og observerbarhet. Disse karakteristikkene bidrar til å forklare hvorfor noen innovasjoner sprer seg raskt, mens andre møter motstand eller tar lang tid å bli adoptert (Rogers, 2003, s. 15–16). I dette kapitlet vil cyberdomenet og defensive cyberoperasjoner (DCO) som militær innovasjon diskuteres i lys av disse fem karakteristikkene.

4.1 Relativ fordel

«Relativ fordel er i hvilken grad en innovasjon oppfattes som bedre enn det den erstatter» (Rogers, 2003, s. 229). Forskere på spredningsteori fremmer at relativ fordel er en av de sterkeste karakteristikkene ved en innovasjon som kan forutse adopsjonsraten til innovasjonen. Dersom innovasjonen har en relativ fordel, vil dette påvirke adopsjonsraten positivt (Rogers, 2003, s. 233).

Den relative fordelen av cyberdomenet kommer i liten grad frem i Forsvarets normative dokumenter. Den hierarkiske strukturen i den militære organisasjonen gjør det utfordrende for unge befal og offiserer å nå frem til beslutningstakere. Denne utfordringen kombinert med at innovatører og tidlig tilpasningsdyktige innen cyberforsvar ofte er personell med høy teknisk kompetanse som gjerne jobber på lavere nivå, indikerer at disse vil ha lav påvirkningskraft. De med best kjennskap til faget har en mindre grad av innvirkning på innføringen av domenet. På teknisk nivå, der det gjerne er en flatere struktur, er dette mindre problematisk. Utfordringene kommer i større grad frem når det skal settes i en militær kontekst og håndteres på taktisk og operasjonelt nivå. Doktriner som FFOD og AJP 3.20 er skrevet som overordnede dokumenter, uten en tydelig plan for hvordan DCO i praksis skal innføres på de ulike nivåene. Dette medfører et gap fra politisk og strategisk nivå, og ned til subtaktisk/teknisk nivå. Uten en operasjonalisering av doktrinene vil det være utfordrende å skape en forståelse av den relative fordelen.

DCO tilfører fellesoperasjonene en ny dimensjon som dekker et område som kan få alvorlige konsekvenser for gjennomføringsevnen. Cyberdomenet og DCO erstatter i utgangspunktet ingen annen innovasjon som den relative fordelen kan måles mot. Det er heller en videreutvikling fra det som er kjent som forebyggende sikkerhet og spesielt informasjonssikkerhet.

En innføring av cyberdomenet og DCO tilfører en ny og fleksibel tilnærming til ivaretakelse av den militære sjefens handlingsrom. Det nye mulighetsrommet gir en fordel utover administrativ sikkerhet gjennom en mer helhetlig og fleksibel tilnærming. I anerkjennelsen av cyberdomenet som et krigføringsdomene gis dette en større grad av militært tilsnitt og en tilnærming som er kjent for militært personell som planlegger og gjennomfører fellesoperasjoner. Dette er et mulighetsrom som fortsatt er i mindre grad utnyttet i Forsvaret. Prosessene er i også mindre grad utformet i fellesskap mellom taktisk og operasjonelt nivå. Det mangler kunnskap på begge nivå og prosessene på operasjonelt nivå mangler en tydelig integrering av perspektiver fra cyberdomenet. Dette indikerer at det er et uutnyttet potensial og den relative fordelen er lav. Adopsjonsraten er lavere enn dens potensiale. Cyberdomenet kan betraktes som en forebyggende innovasjon. Dette er en type innovasjon hvor aktørene aksepter innovasjonen basert på at den potensielt kan bidra til at uønskede hendelser ikke inntreffer. Ved denne formen for innovasjon er aktørenes motivasjon til å implementere innovasjonen lav (Rogers, 2003, s. 176). At cyberdomenet er innført som en forebyggende innovasjon understøtter ytterligere at det vil være en lavere spredningen enn andre innovasjoner (Rogers, 2003, s. 233).

Delkonklusjon

Gjennom å utnytte det fulle potensialet av innovasjonens relative fordel vil Forsvaret potensielt lykkes i større grad med integreringen av defensive cyberoperasjoner i fellesoperasjoner. Med et bevisst forhold til innføring av innovasjonen og en plan for innovasjons-beslutningsprosessen vil den relative fordelen bli tydeligere, og spredningen av innovasjonen vil kunne gå raskere.

4.2 Kompatibilitet

«Kompatibilitet er i hvilken grad en innovasjon oppfattes til å være i tråd med eksisterende verdier, erfaringer og behov» (Rogers, 2003, s. 240). Dersom en innovasjon oppfattes som kompatibel, vil dette ha en positiv innvirkning på adopsjonsraten.
Forsvaret har gode prosesser for planlegging og gjennomføring av operasjoner, dette er noe både FOH og taktiske kommandoer er gode på, men håndteringen av cyberrelaterte hendelser inngår ikke i disse prosessene slik hendelser fra andre domener gjør. Ansvaret for DCO ved FOH er derimot mer eller mindre i sin helhet lagt over på J6. J3 og J5 som har ansvar for operasjoner og planer, er i stor grad fraværende i planlegging og gjennomføring av DCO samt oppdatering av fellesoperativt planverk innen cyberdomenet. Kunnskapen om cyberdomenet er lav på operasjonelt nivå utover fagspesialister på J6. Uten å forstå domenets innvirkning på fellesoperasjoner settes håndtering ut til 6'er miljøer[10] fremfor de som er bedre rustet til å forstå militære operasjoner. J6 skal bidra som fagekspert og rådgiver inn i planprosesser, men i stedet er det opp til dem å lede.

Det er i stor grad manglende kunnskap om cyberdomenet i en militær kontekst og som en del av militære operasjoner på operasjonelt nivå. DCO har grodd frem fra et sikkerhetsperspektiv av personell med hovedsakelig sikkerhetsbakgrunn. Dette bidrar til at overgangen fra tekniske data til militære operasjoner ikke er sømløs. Operasjonelt nivå får et detaljfokus som ikke er hensiktsmessig på deres nivå. Taktisk nivå mangler også kompetanse for å omsette data til operasjonelle vurderinger. Dette medfører at aktørene i liten grad evner å se det store bildet. Kompatibiliteten med kjente normer og prosesser oppleves som lav. Dette påvirker adopsjonsraten negativt.

Delkonklusjon

En idé som er uforenlig med verdiene og normene i et sosialt system, vil ikke bli tatt i bruk like raskt som en innovasjon som er kompatibel (Rogers, 2003, s. 240). For at personell på taktisk og operasjonelt nivå, skal forstå cyberdomenet og evne å bidra konstruktivt inn i DCO kreves det en

[10] G6 (Hæren/HV), A6 (Luftforsvaret), N6 (Sjøforsvaret) og J6 (FOH)

doktrinetilnærming som beskriver omsetting av teknisk data til et språk om er allment forstått i militære organisasjoner.

Uten kunnskap og kompetanse er det vanskelig å ha en enhetlig tilnærming til en problemstilling. Divergerende mentale modeller vanskeliggjør samhandlingen og aktørene snakker potensielt forbi hverandre. Innovasjon i byråkratiske militære organisasjoner er vanskelig nok i utgangspunktet, og innenfor cyberfaget vil det være vanskelig å få med beslutningstakere om cyberoperasjoner fremstilles som noe annerledes, som krever en annen tilnærming. Dersom beslutningstakere og personell med stor innflytelse i stor grad sorterer under sen majoritet og etternølere vil det være utfordrende å nå frem for minoriteten som i tillegg ikke er godt nok inkludert i prosessene på operasjonelt nivå.

4.3 Kompleksitet

«Kompleksitet er i hvilken grad en innovasjon oppleves som relativt vanskelig å forstå og bruke» (Rogers, 2003, s. 257).
Cyberdomenet skiller seg fra øvrige domener både gjennom at det er menneskeskapt, men også at det er svært abstrakt for folk flest. Å omsette data fra subtaktisk og teknisk nivå, til informasjon som gir merverdi på taktisk og operasjonelt nivå, krever kunnskap om cyberdomenet og militære operasjoner og en evne til å sammenstille denne kunnskapen. Cyberdomenet er i liten grad integrert i Forsvarets nivådannende utdanning, og kunnskapen blant Forsvarets personell som ikke jobber med cyberdomenet som en av sine primæroppgaver oppleves som generelt lav. Beslutningstakere på alle nivåer har i liten grad kunnskapen som kreves for å ta perspektiver fra cyberdomenet inn i nødvendige prosesser.

Det er et stort behov for å fylle på med kompetent personell, men det er ingen steder å hente dette personellet fra. Å utdanne personell og gi de den erfaring som kreves tar tid, og det krever at personellet er motivert. Det finnes per i dag ingen klar karriereretning for de som ønsker å spesialisere seg i cyberoperasjoner. Våpengrenenes karriere- og tjenesteplaner gjenspeiler ikke innføringen av cyberdomenet. Cyberdomenet ble således ved innføringen ikke sidestilt med øvrige domener i praksis. Kombinert med at roller, ansvar og myndighet er utydelig og lite definert fremstår kompleksiteten i utfordringene innovasjonen medbringer som høy.

> «Å skape en felles visjon omfatter evnen til å avdekke de felles bildene av fremtiden som fremmer ekte innsatsvilje og deltagelse snarere enn lydighet. Når de mestrer denne disiplinen, lærer ledere hvor uproduktivt det er å prøve å diktere en visjon, uansett hvor mye de selv brenner for den» (Senge, 1991, s. 15).

Etablering av cyberdomenet både som et begrep og som et krigføringsdomene medfører endringer i doktrine. Domenet bringer med seg et omfattende begrepsapparat som er lite gjenkjennbart fra operasjoner i de tradisjonelle domenene land, sjø og luft. Aktørenes mentale modeller bygget på tidligere erfaringer fra andre domener og dette preger deres tilnærming til cyberdomenet. Uten en felles tilnærming og en felles forståelse av konsekvenser for fellesoperasjoner vil avstanden mellom de mentale modellene blant viktige aktører kunne øke. Manglende kommunikasjon vil påvirke forholdet mellom taktisk og operasjonelt nivå og deres evne til å ha en felles tilnærming til DCO.

Delkonklusjon

Kompleksiteten av en innovasjon påvirker adopsjonsraten negativt. Desto mer kompleks en innovasjon synes å være, desto lavere er adopsjonsraten (Rogers, 2003, s. 257).

Kunnskapen i Forsvaret om cyberdomenet og DCO fremstår som generelt lav. Det mangler kunnskap og kompetanse på alle nivåer. Der hvor kunnskapen om domenet finnes er det en lav evne til å omsette det i praksis i en militær kontekst.

Rogers' spredningsteori er en kommunikasjonsteori som går langt i å forklare hva som påvirker tempoet i spredning av innovasjoner. I Innovasjons-beslutningsprosessen er også kommunikasjonskanalene en gjennomgående faktor. Hvordan budskapet formidles påvirker hvordan innovatørene kan lykkes med å få med seg sen majoritet og etternølere. Skal taktisk og operasjonelt nivå lykkes med å planlegge og gjennomføre effektive DCO er det tydelige indikasjoner på at de bør snakke samme språk, skape en felles forståelse og ikke minst kommunisere med hverandre.

Den høye graden av kompleksitet innføringen av cyberdomenet som et krigføringsdomene medfører, resulterer i en negativ påvirkning på adopsjonsraten og tempoet går ned.

4.4 Etterprøvbarhet

"Etterprøvbarhet er i hvilken grad en innovasjon kan eksperimenteres med i begrenset omfang" (Rogers, 2003, s. 258). Innovasjoner som kan testes før de tas i bruk har ofte en raskere adopsjonsrate.

Etterprøvbarheten i cyberdomenet er reservert noen få. Det krever grunnleggende forståelse for det tekniske håndverket i tillegg til militære operasjoner, det bør også være en evne til å sette dette sammen på en hensiktsmessig måte. De med teknisk forståelse har ofte i mindre grad forståelse for militær anvendelse, og de med god kompetanse på militære operasjoner har i mindre grad kunnskap om cyberdomenet.

På teknisk nivå er mulighetene store for eksperimentering gjennom eksempelvis virtuelle testarenaer. På taktisk og operasjonelt nivå har den tekniske eksperimenteringen liten betydning, dette understøttes også av Rogers' som fremmer at etterprøvbarheten er viktigere for innovatørene og de tidlig tilpasningsdyktige (Rogers, 2003, s. 258).

Øving og trening i cyberdomenet og med innvirkning fra cyberdomenet på fellesoperasjoner gjennomføres, men skal læringen være valid bør øvelsene holde høy kvalitet og utfordre taktisk og operasjonelt nivå med dilemmaer relevant for deres nivå. Tekniske øvelser er relativt enkle å få til, men det krever mer kompetanse for å få frem taktiske og operasjonelle dilemmaer.

Delkonklusjon

Cyberdomenets innvirkning på fellesoperasjoner bør øves. Øvelsene bør gå ut over tekniske utfordringer som kun skaper dilemmaer på lavere nivå. Skal taktisk og operasjonelt nivå lære, og skal de kunne øve realistisk bør det legges mer fokus på å skape gode øvelser som skaper dilemmaer som treffer beslutningstakere på flere nivåer. Etterprøvbarhet i cyberdomenet er krevende utover teknisk nivå. Dette medfører at den positive innvirkningen på adopsjonsraten uteblir.

4.5 Observerbarhet

«Observerbarhet er i hvilken grad resultatene av en innovasjon er synlige for andre» (Rogers, 2003, s. 258). Desto mer synlig effekten av innovasjonen er for andre, jo høyere er adopsjonsraten. Cyberdomenet som en forebyggende innovasjon og noe som er abstrakt for folk flest, medfører lav synlighet. Synligheten i samfunnet for øvrig er høy. Der er reduksjon av risiko for alvorlige cyberhendelser tydelig relatert til sikkerhet og profitt. I en militær kontekst er det lavere synlighet og effektene er mer krevende å se. Tap av handlefrihet i cyberdomenet er enklere å måle når det faktisk inntreffer, men dersom et effektivt cyberforsvar evner å forhindre dette er effekten lite observerbart utover teknisk nivå. Gode øvelser som fremmer læring, bidrar til økt kunnskap og kan også bidra til økt observerbarhet av cyberdomenet som innovasjon.

Delkonklusjon

Gjennom militære operasjoner er det ønskelig å oppnå militære effekter som understøtter den militære målsettingen, DCO gjør også dette, men effektene er vanskelige å se og dermed også vanskelig å måle. Det som er vanskelig å se er også vanskelig å forstå, og adopsjonsraten for cyberdomenet og defensive cyberoperasjoner i fellesoperasjoner blir negativt påvirket.

4.6 Oppsummering

I spredningsteori beskriver Rogers fem karakteristikker av innovasjoner. Karakteristikkene relativ fordel, kompatibilitet, kompleksitet, etterprøvbarhet og observerbarhet bidrar til å forklare adopsjonsraten for innovasjoner.
Implementeringen av cyberdomenet i Forsvaret og integrering av defensive cyberoperasjoner i fellesoperasjoner oppleves å gå langsomt. Flere faktorer knyttet til disse karakteristikkene bidrar tildelt til en årsaksforklaring. Den relative fordelen ved cyberdomenet og DCO er lite kommunisert og forstått i Forsvaret, dette påvirker adopsjonsraten negativt. Kompatibiliteten av innovasjonen vil oppleves som lav der kunnskapen om domenet er lav- At tilnærmingen til cyberdomenet avviker fra etablerte prosesser, bidrar ytterligere til en lavere adopsjonsrate. Cyberdomenet skiller seg fra de øvrige domenene på flere måter og den tekniske naturen og abstraksjonsnivået av domenet bidrar til en økt kompleksitet og adopsjonsraten påvirkes negativt. Etterprøvbarheten i cyberdomenet er også lav, noen få har kunnskap og kompetanse til å drive testing og eksperimentering, som igjen påvirker adopsjonsraten negativt. Av de samme årsaker er også observerbarheten lav, ved lav synlighet av effekt påvirkes også adopsjonsraten negativt.

Ut fra Rogers fem karakteristikker som påvirker adopsjonsraten av en innovasjon er det klare indikasjoner på at cyberdomenet og defensive cyberoperasjoner vil ha en lav adopsjonsrate i Forsvaret. Dette peker på at det er hensiktsmessig å ta tak i disse utfordringene og arbeide for å øke forståelsen, kompatibiliteten, tilgjengeligheten, og synligheten for å oppnå en mer effektiv integrering og implementering av cyberdomenet og DCO.

5 Innovasjons-beslutningsprosessen

I foregående kapittel ble det belyst hvilken innvirkning fem ulike karakteristikker ved cyberdomenet og defensive cyberoperasjoner har på adopsjonsraten av cyberdomenet og defensive cyberoperasjoner som innovasjon. Innovasjons-beslutningsprosessen, foreslått i Rogers' teori om spredning av innovasjoner (figur 2-2), beskriver stegene aktører går gjennom når de adopterer en ny innovasjon. Stegene er ikke nødvendigvis lineære, og aktørene kan bevege seg frem og tilbake mellom dem, avhengig av ulike faktorer som tilbakemeldinger, erfaringer og endringer i omstendigheter. Innovasjons-beslutningsprosessen gir en ramme for å forstå hvordan innovasjoner blir adoptert og spredt over tid (2003, s. 170).
De fem stadiene kunnskap, overtalelse, beslutning, implementering og bekreftelse vil i dette kapitlet danne rammen for analyse og diskusjon av datamaterialet. Temaer utledet fra datamaterialet korrelerer med disse fem stadiene som vist i tabell 3.1.

Respondenter er tildelt tilfeldige nummer og omtales som R1-8, mens tabletop-øvelse for taktisk nivå omtales som T1 og tabletop-øvelse for CyWG omtales som T2.

5.1 Kunnskap - Kompetanse

Kunnskapsfasen i innovasjons-beslutningsprosessen starter i det aktørene får kjennskap til innovasjonens eksistens (Rogers, 2003, s. 171). Cyberdomenet har utviklet seg over tid og eksisterte i realiteten flere år før domenet ble formelt definert som et krigføringsdomene. I Forsvaret er det personellet som jobber spesifikt med cyberfaget hovedsakelig personell med primæroppgaver innenfor tradisjonell sambandsplanlegging. Problemstillinger knyttet til cyberhendelser delegeres i stor grad til personell innenfor 6'er miljøet.
Blant respondentene i oppgaven er det et gjennomgående tema at kompetansen er samlet hos noen få. Én respondent mener at FOH legger forholdene til rette for at Cyberforsvaret skal ta tak i DCO, men at Cyberforsvaret per i dag ikke er i stand å gjøre det. Mye sendes direkte ned til Cyberforsvarets cybersikkerhetssenter (CSS), som sitter på den tekniske ekspertisen, men som mangler erfaringen med hva som er behovet på operasjonelt nivå. Innovatører og tidlig tilpasningsdyktige innenfor et så tekniske preget fagfelt som cyberdomenet utgjør, vil ofte være de yngre teknologisk kunnskapsrike i organisasjonen. Som det også påpekes fra en annen respondent med lang erfaring i faget, har dette personellet stort sett bakgrunn og utdanning fra informasjonssikkerhet og forebyggende sikkerhet. Selv om denne bakgrunnen kan gi en solid teknisk forståelse og en grunnleggende kunnskap om cyberdomenet, er det lite i dette karriereløpet som setter personellet i stand til å forstå domenet i en militær kontekst, eller omsette sin kunnskap til et nivå som forstås av personell på taktisk og operasjonelt nivå. Respondenten utdyper videre at dette personellet er på ingen måte uegnet til å drive med DCO, men må skoleres innen militære operasjoner og krigføring. At personellet har denne type sikkerhetsbakgrunn, vil være en faktor som medfører at fokuset dreies mot cybersikkerhet og mer tradisjonell IKT-sikkerhet fremfor militære operasjoner, herunder DCO.

> «Domenet i seg selv definerer hva vi trenger av kompetanse. Det er ikke dumt å forstå hvordan teknologien fungerer, men det er bare én dimensjon» (R6).

Hvorvidt kompetansen er til stede i Forsvaret for å drive effektive DCO er det divergerende oppfatninger om blant respondentene. En respondent trekker frem at forståelsen av DCO i fellesskapet er for lav. Flere respondenter mener at kompetansen ikke er til stede og at med unntak av den tekniske ekspertisen enkelte fagmiljøer i Cyberforsvaret sitter på, er kompetansen lav. En respondent mener på sin side at kompetansen er til stede på individnivå, basert på kursdeltagelse i inn- og utland, men at vi som fellesskap ikke evner å omsette den ervervede kompetansen til praksis i

en militær kontekst. Det påpekes at det norske Forsvaret har en unik mulighet for å utdanne personell gjennom Cyberingeniørskolen[11], men at dette dekker kun deler av behovet.

Det fremkommer også, gjennom T1, at det i den taktiske kommandoen ikke finnes personell med «cyber» i stillingsbeskrivelsen. Dette er en problemstilling som er gjennomgående i Forsvaret. Med unntak av Cyberforsvaret er det lite synliggjort hvilket personell som har oppgaver innenfor cyberdomenet. Personell som spesialiseres i fagfeltet representerer hele bredden fra Forsvarets våpengrener, og har ingen egen fagsjef. Det utvikles ingen egne kompetanseplaner eller karriereplaner for befal og offiserer innen cyberfagfeltet.

Et fåtall av kurs som tilbys innenfor fagområdet tilbys av militære aktører. En stor andel av kursing utover Forsvarets nivådannende utdanning gjennomføres hos sivile aktører. Disse kursene når i stor grad ut til personell som allerede jobber innenfor fagfeltet. I Forsvaret i dag tilbys kun ett kurs innen planlegging av cyberoperasjoner i regi av Etterretningstjenesten i samarbeid med Cyberforsvaret. Nivådannende utdanning i Forsvaret gjennomføres for både befal og offiserer. I begge søylene er cyberdomenet i svært liten grad en del av denne utdanningen. Alle respondentene adresserer behov for utdanning, kurs og trening innenfor cyberfeltet.

> «Uansett hvilken Krigsskole man går, må man få undervisning i cybermakt» (R6).

Skal spredning av en innovasjon lykkes er kunnskap en grunnleggende faktor. Uten denne er det liten sannsynlighet for at innovasjonen kommuniseres og forstås nok for å skape et troverdig beslutningsgrunnlag (Rogers, 2003, s. 171–179). Kunnskap om cyberdomenet når ikke ut til de store massene. All den tid cybermakt ikke inkluderes i nivådannende utdanning vil ikke befal og offiserer som tjenestegjør i stillinger utenfor 6'er miljøer gis den grunnleggende forståelsen som kreves for å drive fellesoperasjoner eller overgangen til MDO som favner alle domener. Prosedyrer og prosesser som utvikles på taktisk og operasjonelt nivå vil potensielt ekskludere cyberperspektiver all den tid det ikke eksisterer en grunnleggende forståelse av cyberdomenets innvirkning på øvrige domener.

Som en av respondentene bemerker, må kadetter uavhengig av hvilken krigsskole, lære mer om Forsvarets tilgjengelige maktmidler. Veien for å oppnå dette går gjennom kunnskap. Som vedkommende også uttrykker «prosedyrer uten kunnskap det er litt skummelt» (R6).

Respondenten fremhever også at kompetansen på taktisk og operasjonelt nivå er kommet langt på vei. Det pekes på ulike årsaker, men fremheves at en bevisstgjøring knyttet til konflikter i vår samtid,

[11] Profesjonsutdanningen som tilbys av Forsvarets høgskole. Skolen gir bachelorgrad i elektrofag med fordypning telematikk i tillegg til grunnleggende befalsutdanning.

som for eksempel Ukraina har hatt stor betydning. Etterretninger om cybertrusler er blitt bedre, noe som potensielt bidrar til en bedre forståelse på flere nivåer.

> «Det som gjenstår, er kompetansen hos de som jobber med det. Den er basert på skolegang de har fått tidligere hvor cyberdomenet var kanskje bare noe interessant som noen andre jobbet med. Så mangler man kanskje både ord og begrep og i hvert fall den praktiske forståelsen for hvordan dette gjennomføres» (R6).

Her trekkes også frem en problematikk som flere av respondentene har reflektert over, og som også har kommet tydelig frem gjennom tabletop-øvelsene. Bruken og forståelsen av ord og begreper er svært varierende. Selv om AJP 3.20 og FFOD definerer DCO hersker det ulike oppfatninger om hva dette faktisk er og skal være. Ulike aktører legger ulike meninger i begreper. Et teknisk språk farger også dialogen mellom aktørene og terminologi som ikke lett lar seg oversette til legmannstermer benyttes i stor grad. Selv internt i CyWG fremkommer det at respondentene opplever at de snakker forbi hverandre i forhold til forståelse av ord og begreper.

Kurs som tilbys innenfor cyberfaget treffer i stor grad kun de som allerede har dette som en primæroppgave eller som et interessefelt. Dette medfører at andre fagområder ikke øker sin forståelse av cyberdomenet og hvordan de må forholde seg til cybertrusselen. Gjennom felles øvelser er det muligheter for å nå ut til en større del av Forsvaret, og bruke disse arenaene for læring. Som en av respondentene nevner, er dette et område vi ikke har god nok kunnskap til å utnytte godt nok. Vi blir gående i en ond sirkel av at personell med liten erfaring blir satt til å utarbeide øvingsscenarioer. Dette medfører at øvelsene ikke treffer de nivåene som har behov for å øve.

> «Vi må øve på de vanskelige tingene sånn at fellesprosessene tar tak i det og skjønner hvordan man må tilnærme seg det. Hvis ikke blir det bare en IKT-greie på nytt» (R4).

Det oppleves også til stadighet at cyberdomenet får liten prioritet i større øvelser. Cyberforsvaret blir i større fellesøvelser satt i en skvis gjennom at de har leveranser til både egne styrker og til styrkene som spiller fienden. Dette medfører at CDOC som skulle vært navet i håndtering av cyberhendelser og gjennomføring av DCO blir stående i en situasjon hvor det ikke er hensiktsmessig å delta i et cyberspill. I de tilfellene hvor det faktisk spilles cyberrelaterte hendelser blir læringen fra disse øvelsene kunstige når det gjelder hvordan taktisk og operasjonelt nivå opererer i det daglige.

Det er bred enighet om at FOH har et potensiale i å inkludere cyberdomenet mer i øvelser og at dette ikke kan kun handle om tekniske problemstillinger. Cyberoperasjoner handler om å skape en effekt, og ikke nødvendigvis kun i cyberdomenet, effekten som ønskes oppnådd er gjerne i det fysiske domenet. Problemstillinger hvor det har skjedd noe som får en effekt utenfor cyberdomenet vil bidra som en øyeåpner for mange. Øvingsscenarioene bør være realistiske for at Forsvaret skal kunne trene

realistisk, og som det trekkes fram fra en respondent på taktisk nivå, så er det ikke nødvendig å trekke ut støpselet for å få en effekt som krever oppmerksomhet fra operasjonelt nivå. At cyberrelaterte hendelser ikke spilles fullt ut i fellesoperative øvelser fremstår som basert på en misforståelse av at datasystemer må gå ned for at det skal ha en effekt.

Delkonklusjon

Kunnskap er et sentralt element i militær innovasjonsteori, men det er klare utfordringer knyttet til å utnytte kunnskapen i en hierarkisk militær organisasjon. For å fremme innovasjon i en militær organisasjon må det først og fremst finnes kunnskap om innovasjonen. At cyberdomenet er anerkjent som et krigføringsdomene hersker det liten tvil om, men hva dette innebærer er det knyttet mye usikkerhet til. Ulike aktører på taktisk og operasjonelt nivå er prinsipielt enige i at kompetanse innenfor fagfeltet er en mangelvare i Forsvaret, men det er ulike oppfatninger av hvilken kompetanse som mangler og hvordan den skal benyttes. At aktørene fremviser felles observasjoner i tilnærmingen til kompetanse betyr ikke nødvendigvis at de deler en felles mental modell. Mennesker med ulike mentale modeller kan observere det sammen fenomenet, men oppleve og beskrive de ulikt (Senge, 1991, s. 179).

Selektiv oppfatning defineres av Rogers til å være tilbøyeligheten til å tolke kommunikasjonsmeldinger i tråd med ens eksisterende holdninger og tro. Individer unngår normalt å utsette seg for meldinger om en innovasjon med mindre de ser et behov for innovasjonen. Selv om aktøren eksponeres for slike meldinger, vil dette ha liten effekt, med mindre innovasjonen oppleves som relevant og i tråd med egen forutinntatthet (Rogers, 2003, s. 171). Dersom Forsvarets personell ikke gis den kunnskapen som kreves for å påvirke deres mentale modell til å innbefatte at cyberdomenet har en relativ fordel, vil adopsjonsraten være lav. Sen majoritet og etternølere vil i liten grad oppfatte kommunikasjonsmeldinger om cyberdomenets relevans om kunnskapen om domenet ikke heves gjennom utdanning, kursing og øving. En felles tilnærming i Forsvaret til karriere- og kompetanseplaner for personell med oppgaver innenfor defensive cyberoperasjoner vil bidra til felles forståelse og større grad av en felles mental modell.

5.2 Overtalelse – Kompetanse beslutningstakere

> «Cyber som enhver annen prosess vil jo møte på de samme utfordringer som andre prosesser, det må prioriteres, det må være konkrete tiltak, det må være konkrete utfall og noen må ta en beslutning» (R4).

Når en aktør har fått kunnskap om en ny innovasjon vil det formes en holdning til denne innovasjonen, og dette gjøres i det neste steget av innovasjons-beslutningsprosessen som kalles

overtalelse. I dette steget vil aktørene forme en mening om at de anser innovasjonen som noe positivt eller ikke. I dette steget søker aktørene mer informasjon om innovasjonen og bestemmer seg for hvilken informasjon som anses som troverdig (Rogers, 2003, s. 174).

I fortsettelsen av det tidligere omtalte kunnskapssteget, vil det i dette avsnittet fokuseres på kompetansen hos beslutningstakere.

> «Vi må få lederne på banen» (R7).

Gjennom både de individuelle intervjuene og tabletop-øvelsene har beslutningstakerne sin rolle vært et gjennomgående tema. Flere av respondentene har påpekt vanskelighetene med å informere beslutningstakere på en måte som gjør at budskapet oppfattes og forstås. Å omsette teknisk informasjon som gir effekt på operasjonelt nivå er krevende og det er tydelig at det kreves en bearbeiding av data mellom nivåene. Her har taktisk nivå, og spesielt CDOC en nøkkelrolle.

Én respondent erkjenner at det er umulig å presentere et beslutningsgrunnlag som er helt sikkert, det vil være mangler i det som legges frem for beslutning, men det vil være nok for å fatte en beslutning. Dette er det hensiktsmessig at beslutningstakerne forstår, og de bør gis en god nok forståelse av cyberoperasjoner til at de er trygge nok til å fatte beslutninger selv på tynt grunnlag. Som respondenten selv sier:

> «Beslutninger er slik at skal du vente til noe er 100% sikkert, så trengs det ingen beslutning. Du må ta beslutninger på et uoversiktlig grunnlag noen ganger. Det er det som er ledelse» (R7).

«Vi lærer best av erfaring, men får aldri direkte erfare konsekvensene av mange av våre viktigste beslutninger» (Senge, 1991, s. 29). Øvelser trekkes av flere respondenter frem som en arena hvor beslutningstakerne bør komme på banen. De bør gis opplæring og øves på å operere i et utfordret cyberdomene, samtidig som de bør gis kunnskap nok om fagområdet til at de er i stand til å forme egne meninger og ta beslutninger selv på et tynt grunnlag. Igjen fremheves viktigheten av å øve riktig og utarbeide gode øvingsscenarioer som utfordrer beslutningstakere på både taktisk og operasjonelt nivå. Tabletop-øvelser og bruk av fellesoperative arenaer trekkes frem som enkle grep som kan bidra til økt kompetanse hos beslutningstakerne. Tilbudet bør tilgjengeliggjøres, men de bør også motiveres til å delta. Flere respondenter uttrykker en misnøye med hvordan cyberdomenet blir håndtert, eller ikke håndtert, av ledere på ulike nivåer. Respondentene legger frem eksempler på hvor det gjennomføres tiltak i form av seminarer og kurs hvor ledelsen uteblir.

> «Cyber må bli noe som ikke lenger er valgfag» (R7).

Signaleffekten for hvilke holdninger Forsvarets ledelse viser til cyberdomenet trekkes også frem av respondenter fra både taktisk og operasjonelt nivå, og de stiller seg kritiske til kombinasjonen av flere faktorer. At sjef Cyberforsvaret fikk endret grad fra Generalmajor til Brigader, at de i 2023 også ble fratatt flere millioner i budsjettet, og at ledere ved FOH som stiller i ulike arbeidsgruppemøter ikke stiller i CyWG, er med på å bidra til at cyberfagfeltet oppleves som nedprioritert blant beslutningstagere. Dette gir en sterk signaleffekt ut i hele sektoren. Det er på overtalelsesstadiet at den generelle oppfatningen av innovasjonen utvikles. Dersom beslutningstakere på taktisk og operasjonelt nivå ikke gis nødvendig kunnskap om cyberdomenet vil dette sterkt påvirke den oppfatningen som dannes om domenet (Rogers, 2003, s. 176). Som en av respondentene pekte på, vil manglende ekspertise innenfor håndtering av cyberrelaterte hendelser og trusler, kunne medføre at selv små hendelser får betydelige konsekvenser. Beslutninger tatt på sviktende grunnlag, eller manglende beslutninger kan føre til en overreaksjon eller en overdreven forsiktighet som kan føre til unødvendig nedleggelse av aktiviteter som igjen gir trusselaktøren en meget god uttelling for noe som krever lav innsats.

Dersom dette er slik cyberdomenet oppfattes blant beslutningstakere i Forsvaret vil dette påvirke evnen til å lykkes med DCO. Om cyberdomenet oppleves som påtvunget gjennom policy og doktrine, vil det uten kunnskap og forståelse av domenets rolle og innvirkning på fellesoperasjoner få en sterkt negativ påvirkning på adopsjonsraten av innovasjonen, eller på Forsvarets evne til å integrere DCO som en del av fellesoperasjoner. Det vil også være svært utfordrende å nå ut i resten av Forsvaret, samt å få med den sene majoriteten og etternølerne dersom ikke ledere på alle nivåer har en positiv tilnærming til implementering av cyberdomenet, og kan bidra til å prioritere og ressurssette etter behov.

Den hierarkiske strukturen i Forsvaret, kombinert med krav til bredde i utdanning og erfaring, gjør det krevende for yngre befal og offiserer å få gjennomslag for sine innovative forslag. Det tar tid før de får den nødvendige innflytelsen og posisjonen til å kunne gjennomføre større endringer i organisasjonen.

Delkonklusjon

Blant respondentene fremstår det som om deres oppfatning av beslutningstakere på alle nivåer i Forsvaret er sammenfallende. Deres oppfattelse og holdninger til beslutningstagernes evne til å fatte gode beslutninger knyttet til cyberrelaterte utfordringer, bidrar til å forme en felles mental modell på tvers av taktisk og operasjonelt nivå. De mentale modellene som formes av beslutningstakerne som

omtales, vil med svært stor sannsynlighet avvike fra de mentale modellene som kommer frem hos personell med høy kompetanse og erfaring fra cyberdomenet.

Rosen påpeker at militære organisasjoner er bygget opp på en måte som gjør det utfordrende for yngre befal og offiserer å drive frem militær innovasjon i fredstid. Den hierarkiske strukturen i organisasjoner som Forsvaret, innebærer at det vil gå tid før disse har avansert høyt nok opp til å ha den nødvendige innflytelsen for å ha nok påvirkningskraft til å gjennomføre større endringer. En annen del av denne utfordringen er også at dette personellet ofte er spesialisert innenfor et smalt fagfelt og dermed ikke tilfredsstiller de kravene Forsvaret setter for personell som skal avansere til de stillingene hvor de er i en posisjon til å ha en påvirkningskraft. Militære organisasjoner kan være konservative og foretrekke kandidater med en mer tradisjonell bakgrunn (Rosen, 1991, s. 20–21).

5.3 Beslutning – Ledelse

«Beslutningssteget i innovasjons-beslutningsprosessen finner sted når aktørene involverer seg i aktiviteter som leder til en beslutning om innovasjonen skal aksepteres eller avvises» (Rogers, 2003, s. 177). Dersom en innovasjon aksepteres, innebærer dette en beslutning om å ta innovasjonen i bruk.

«God situasjonsforståelse innenfor land-, sjø-, luft- og cyberdomenet er nødvendig for å sikre et rettidig og godt beslutningsgrunnlag» (Prop. 151 S (2015–2016), pargr. 1.4.3). Forsvarets grunnsyn på ledelse trekker også frem situasjonsforståelse, situasjonstilpasning og troverdighet blant de grunnleggende forutsetningene for god og effektiv ledelse (Forsvarsstaben, 2020, s. 14). Disse to dokumentene fremhever begge situasjonsforståelse i cyberdomenet, men ingen påfølgende ledelsesprodukter beskriver hva dette innebærer. Som adressert i forrige avsnitt er kompetansen hos beslutningstakerne viktig for effektiv utøvelse av DCO. Ledere bør settes i stand til å ta gode beslutninger basert på det grunnlaget de presenteres for. Kompleksiteten i cyberdomenet er høy, det krever kunnskap for å forstå domenets innvirkning på militære operasjoner. At teknisk personell som sitter tett på håndverket har en god forståelse av de teknologiske utfordringene gir liten operativ effekt om dette ikke omsettes på et språk som beslutningstakere forstår.

Føringer knyttet til cyberdomenet gis gjennom en rekke ulike ledelsesprodukter. Hovedsakelig forholder taktisk nivå seg til det operative planverket og oppdrag som gis gjennom Joint Guard. I tillegg til dette er de også pålagt å forholde seg til en rekke bestemmelser[12] og instrukser[13] som også

[12] Cybersikkerhetsbestemmelser
[13] FDs cyberretningslinjer

legger føringer innen samme fagfelt. På toppen av dette kommer også de doktriner[14] og konsepter[15] som ligger til grunn. Respondenter fra taktisk nivå opplever at det operative planverket ikke er dekkende for deres daglige operasjoner. Totalen av konsepter, bestemmelser og instrukser gjør det uklart og uoversiktlig hva som er gjeldende og hva som legger føringer for aktiviteten. Det hersker også en usikkerhet knyttet til hvilke kommandoforhold som gjelder ved igangsetting av en defensiv cyberoperasjon. Det oppleves som uklart hvem som igangsetter og hvem som har hvilke roller gjennom prosessen. For de taktiske kommandoer som ikke selv har myndighet til å igangsette en DCO, er deres rolle ikke beskrevet og de er usikre på i hvilken grad de blir involvert.

Det hersker også en usikkerhet rundt hvilken sjef som eier risikoen. Dersom et system er kompromittert fremstår taktisk nivå som usikre på sin rolle og hvilken myndighet deres styrkesjef sitter med. Fra operasjonelt nivå kommer det frem en formening om at det er rammet sjef som eier problemet, men det reflekteres i liten grad over om problemet eies av FOH dersom hendelsen har konsekvenser for fellesoperasjoner. Gjennom T1 og T2 kommer det tydelig frem at disse ulike oppfatningene ikke er adressert i dialogen mellom aktørene, og de snakker i stor grad forbi hverandre uten at kjernen i problemet tas tak i. Flere respondenter trekker også frem usikkerhet rundt hvem som skal lede prosessene. Fra taktisk nivå opplever de at oppdrag kommer fra operasjonelt nivå med svært varierende detaljgrad, dette medfører utfordringer med å forstå hvilken type informasjon FOH har behov for, hva de skal med det, og ofte er intensjonen bak oppdragene ikke kjent for taktisk nivå.

> «FOH må rett og slett velge hvilket detaljnivå de ønsker å lede på, i ene øyeblikket graver de seg ned i detaljene, mens i det neste ønsker de ikke å ta i de mer overordnede tingene» (R4).

Respondenter på taktisk nivå opplever at det til stadighet kommer nye oppdrag og føringer fra FOH uten at de har vært involvert i prosessen, og det er uklart hva man kan forvente fra operasjonelt nivå.

Halvparten av respondentene mener at FOH per i dag ikke er i stand til å lede DCO. Dette begrunnes med blant annet at FOH sin rolle og ansvar ikke er tydeliggjort og at det oppleves at ansvar dyttes nedover. Én respondent poengterer også at det ikke er enighet om hva DCO egentlig er, og at uten å ha en omforent tilnærming til hva det innebærer vil det ikke være mulig å gjennomføre effektive cyberoperasjoner. Selv om doktriner og konsepter er på plass bidrar ikke dette til klarhet i hvordan DCO skal ledes. Flere av respondentene mener FOH kunne vært i stand til å lede DCO dersom de

[14] AJP 3.20 Allied Joint Doctrine for cyberspace operations og Forsvarets fellesoperative doktrine (FFOD)
[15] Konsept for nasjonale militære cyberoperasjoner, Forsvarets CIS konsept og Konsept for defensive cyberoperasjoner

hadde tatt tak i det og hatt et ønske om å ta ledelse. Det uttrykkes fra flere en usikkerhet rundt hvorfor FOH ikke tar denne lederrollen. Det pekes blant annet på FOHs ledelseskonsept, personlige egenskaper eller ressurser som flere mulige årsaker.

> «Hva de på FOH skal lede på, er avhengig av deres forståelse av hvordan FOH leder andre operasjoner. Det må være likt» (R8).

Fra taktisk nivå er det flere respondenter som er tydelige på at cyberdomenet ikke bør behandles som noe spesielt. Dersom Forsvaret skal oppnå en reell integrasjon av DCO i fellesoperasjoner bør cyberdomenet tilnærmes på samme måte som øvrige domener hos FOH.

Usikkerhet er et gjennomgående uttrykk som benyttes i forhold til FOH sin lederrolle i DCO. Deres ledelse av CyWG trekkes også frem som en faktor. Øvrige prosesser og arbeidsgrupper har en tydelig ledelse fra FOH sin side, mens i CyWG fremstår lederskapet som veldig uklart og forholdet mellom aktørene er ikke diskutert.

Selv om respondenter fra taktisk nivå i stor grad utviser misnøye med ledelse av aktiviteter som berører cyberdomenet, oppleves det ikke som at dette stammer fra manglende vilje, men heller manglende forståelse og avklaringer. Enkelte respondenter trekker også frem taktisk nivå sitt ansvar i å skape gode beslutningsgrunnlag og presentere informasjon som gir godt nok grunnlag for gode beslutninger, selv av beslutningstakere med liten til ingen kompetanse om cyberdomenet.

Som omtalt i avsnitt 2.3, er ikke begrepet Cyber commander definert. Sjef Etterretningstjenesten er gitt den koordinerende myndigheten for cyberoperasjoner, men hvordan dette skal utøves i praksis er ikke beskrevet i FFOD (Forsvaret, 2019) eller *Konsept for defensive cyberoperasjoner* (Cyberforsvaret, 2022). Samtlige respondenter peker på at denne rollen er uklar og det fremkommer tydelig at det er forventninger fra både taktisk og operasjonelt nivå til at Etterretningstjenesten i rollen som Cyber command/Cyber commander skal ta en viss grad av ledelse i den fellesoperative prosessen.

> «Rollen med å koordinere som Cyber commander har, opplever jeg ikke at er en lederrolle, men heller at de er til stede for å følge med på hva vi andre driver med» (R8).

Respondentene peker i stor grad på at dette er verken en rolle de opplever at Etterretningstjenesten eller FOH tar. I tillegg fremstår ansvarsforholdet uklart all den tid ingen tar ledelse. Det hersker også ulike oppfatninger blant respondentene om hvem som har myndighet til å beslutte en DCO. De fleste respondentene mener at både CDOC og FOH kan beslutte, mens FFOD definerer at utførelsen ligger hos Cyberforsvaret, mens kommandoen ligger hos FOH (Forsvaret, 2019, pargr. 05125). Selv blant

respondenter fra Cyberforsvaret hersker det usikkerhet knyttet til hva fagansvar for defensive cyberoperasjoner faktisk innebærer, og hva dette betyr i deres forhold til operasjonelt nivå. I T1 var respondentene klare på at fra andre taktiske kommandoer utover CDOC ligger det ingen myndighet for å beslutte en DCO, de har kun mulighet til å anmode eller anbefale igangsetting. Prosessen for dette eksisterer ikke, og CyWG pekes på som eneste arena for å løfte en slik type anmodning. Cyber commanders rolle i dette fremstår for respondentene som meget uklar og det savnes involvering fra Etterretningstjenesten. Selv fra operasjonelt nivå oppleves forholdet til Cyber commander som uavklart og vanskelig. Det mangler tydelige retningslinjer og roller, ansvar og myndighet fremstår som veldig uklart. Selv om alle respondentene savner involvering fra Cyber commander fremheves det også fra operasjonelt nivå at en sterkere involvering også ville ytterligere problematisert samvirke i fellesoperasjoner, da FOH og Etterretningstjenesten har ulike tilnærminger til operasjoner.

Selv om *Konsept for nasjonale militære cyberoperasjoner* (Forsvaret, 2020) dekker enkelte av disse forholdene, oppsummerer en av respondentene det på denne måten:

> «Vi har en Cyber Commander som har et visst ansvar, også har vi Sjef FOH med et ansvar og Sjef Cyberforsvaret har et ansvar. Det er litt fragmentert og rart, og ingen vet helt hvem som bestemmer hva» (R4).

Delkonklusjon

Rosen argumenterer for at innovasjon ikke bare er et resultat av tilfeldige idéer eller teknologiske fremskritt, men snarere et bevisst initiativ ledet av respekterte og kompetente ledere. Disse lederne tar initiativ til å formulere en helhetlig strategi som omfatter både tenkemåter og organisasjonsstrukturer for å fremme innovasjon (Rosen, 1991, s. 21). I Forsvaret er ledere ikke gitt denne muligheten om å velge å ta i bruk eller forkaste cyberdomenet som et krigføringsdomene. Politiske beslutninger og ratifisering av NATO-doktrine fratar ledere på operasjonelt nivå denne muligheten. Det de da står igjen med er hvordan de går frem for å best mulig integrere defensive cyberoperasjoner i fellesoperasjoner. Politiske beslutninger, FFOD og AJP 3.20 er i liten grad operasjonalisert i Forsvaret. Det finnes ingen egen nasjonal doktrine som omhandler cyberoperasjoner, og rollen som Cyber commander er uklar og ikke definert. Dette preger samvirket mellom taktisk og operasjonelt nivå som opplever at ingen helt vet hvem som skal gjøre hva og resulterer i manglende felles forståelse og tilnærming til de utfordringene som dukker opp.

Evnen til å lede defensive cyberoperasjoner fremstår som det området som splitter taktisk og operasjonelt nivå mest. Aktørene har lav bevissthet om både sammenfallende og divergerende oppfatninger av situasjonen, og de ender opp med en form for pekelek der taktisk nivå forventer

ledelse fra operasjonelt nivå, mens operasjonelt nivå forventer at taktisk nivå tar mer ansvar selv. At Cyber commander rollen er utydelig tilfører ytterligere forvirring og gjør dialogen mer komplisert. De mentale modellene som skapes på taktisk og operasjonelt nivå knyttet til ledelse av defensive cyberoperasjoner er i stor grad divergerende.

5.4 Implementering – Prosess

Rogers definerer implementeringssteget som den perioden der en innovasjon blir satt ut i livet og brukt i praksis etter at den er blitt vedtatt og akseptert av en organisasjon. I denne fasen vil tiltakene for å integrere innovasjonen utføres. Rogers legger vekt på betydningen av god implementering for å sikre at organisasjonen skal lykkes med innovasjonen. Implementering er derfor avgjørende for å sikre en jevn overgang fra aksept av innovasjonen til effektiv bruk i praksis (2003, s. 179–188).
I Forsvaret har cyberdomenet blitt innført først og deretter er FFOD revidert og konsepter utarbeidet. Aktørene har jobbet med fagområdet i lang tid før begreper og prosesser etableres, i den grad de er etablert. De mentale modellene blant aktørene skapes og bygges på deres egne tolkninger av situasjonen. De prosessene som skal samle aktørene og trekke de taktiske kommandoene i samme retning ledes av FOH og inngår i hovedkvarterets beslutningssløyfe.

Gjennom tabletop-øvelsene presenteres respondentene for en alvorlig hendelse med potensielt store operative konsekvenser i et scenario hvor Norge står i en i en større fellesoperasjon der både oppdragsløsning, Forsvarets omdømme og signalering er viktige faktorer. Gjennom diskusjonen blant respondentene kom det tydelig frem at det er varierende oppfatninger av hva CyWG er og hvilke forventninger de ulike aktørene har til arbeidsgruppen.
CyWG er den eneste arbeidsgruppen ved FOH som dekker cyberdomenet. Øvrige arbeidsgrupper og beslutningsmøter innbefatter kun cyberrelaterte problemstillinger dersom disse spesifikt løftes inn gjennom ulike arbeidsgrupper eller adresseres fra taktisk nivå inn i de respektive arbeidsgruppene. Respondenter fra både taktisk og operasjonelt nivå trakk frem CyWG som en utfordring. Ved begge gjennomføringene av tabletop-øvelser kom det tydelig frem at respondentene ikke hadde klart for seg hvilken rolle CyWG har eller er tiltenkt å ha. CyWG har en etablert Terms of Reference (ToR) som skal beskrive arbeidsgruppens hensikt, deltagere, input og output. Denne er etablert, men har vært oppe til diskusjon ved flere anledninger.

> «CyWG kan og bør være arenaen hvor informasjon tygges før den går videre inn i prosessene i hovedkvarteret» (R8).

Fra taktisk nivå uttrykkes det stor grad av frustrasjon over FOHs manglende vilje til å ta lederskapet over CyWG. Én respondent nevner at de faglige diskusjonene er gode, men det mangler en output fra

møtet. Den manglende outputen fra CyWG er en gjennomgående frustrasjon fra flere av respondentene. Det er også en klar forventning fra taktisk nivå at FOH ved J6 skal evne å lede DCO og at dette skal kunne koordineres tettere gjennom CyWG. Per i dag oppleves CyWG kun som et informasjonsdelingsfora, hvor ingen reell sakshåndtering foregår og ingen saker løftes videre inn i hovedkvarterets beslutningssløyfe.

Operasjonelt nivå på sin side uttrykker en klar formening om at pågående hendelser er ikke et tema for CyWG og at dette skal håndteres gjennom andre funksjoner ved hovedkvarteret. Eksempelvis nevnes det i T2 at operasjonssenteret ved FOH, Joint Operations Center (JOC), sitter med dette ansvaret og at disse har eget tiltakskort som skal følges ved cyberhendelser. Videre fremkommer det gjennom intervjuer med respondenter fra operasjonelt nivå at de har en klar formening om at det er den taktiske styrkesjef som eier problemet og som selv er ansvarlig for å løfte dette inn i hovedkvarterets øvrige prosesser.

Gjennom T1 var en av slutningene at hendelsen måtte løftes opp til FOH da omfanget gikk utover ansvarsområdet til den taktiske styrkesjefen. I tillegg ble hendelsen vurdert til å ha så store operative konsekvenser for fellesoperasjonen at det måtte gjøres en prioritering fra operasjonelt nivå. Respondentene konkluderte med at det burde igangsettes en DCO, men erkjente at de selv ikke hadde oversikt over hvordan prosess for å få til dette er. CyWG er de taktiske styrkesjefenes eneste faste innslagspunkt i FOH for å adressere cyberrelaterte saker. T1 diskuterte også hvorvidt en hendelse som den fra tabletop-øvelsen kunne utløst en Crisis Action Team (CAT)[16] ved FOH, men ble enige om at CyWG var deres naturlige innslagspunkt. I T2 kom det frem fra operasjonelt nivå at de ikke så på CyWG som en arena for pågående saker og at den type diskusjon hører hjemme i en CAT eller en ad-hoc plangruppe uten at det ble adressert hvordan prosessen er for å igangsette dette.

I gjennomføringen av T2 ble hendelsen presentert for CyWG med vurderinger og anbefalinger fra T1. Fremfor å ta tak i de operative konsekvensene og vurdere dilemmaet sett fra et taktisk og operasjonelt ståsted, dykket respondentene umiddelbart ned i tekniske detaljer og det tok tid før de kom så langt i diskusjonen at de kunne få et overblikk over det potensielle omfanget av situasjonen.

Flere av respondentene erkjente gjennom individuelle intervjuer at CyWG ofte er fokusert på et detaljnivå som er for teknisk i forhold til hva de har behov for på taktisk og operasjonelt nivå. Noe av denne utfordringen peker tilbake på funnene i drøfting av kompetanseaspektet. CDOC som utgjør

[16] En gruppe som samles når det oppstår en plutselig og uforutsett trussel eller hendelse som kan true hovedkvarterets operasjonsfokus og normalaktiviteter og må håndteres umiddelbart.

det taktiske nivået i Cyberforsvaret, skal i utgangspunktet være mellomleddet mellom subtaktisk/teknisk nivå som CSS utgjør, og operasjonelt nivå. Da CDOC av ulike årsaker ikke har fylt denne rollen har det blitt en aksept for at CSS rapporterer direkte til FOH. Dette medfører at tekniske data ikke filtreres bort og tillegges heller ikke de vurderinger fra taktisk nivå som vil gjøre informasjonen mer relevant for hovedkvarteret.

Fra operasjonelt nivå erkjennes det også at denne praksisen ikke er optimal. Respondenter fra operasjonelt nivå reflekterte også over at diskusjonen i T2 ble for teknisk og detaljfokusert. På den annen side legges det også opp til fra operasjonelt nivå at rapporteringen inn i CyWG og diskusjonene i arbeidsgruppen i stor grad handler om tekniske detaljer og informasjonsdeling.

Gjennom T1 kom det frem flere relevante spørsmål som respondentene opplever som uklare knyttet til ansvar og myndighet. Når en taktisk styrkesjef rapporterer en cyberrelatert hendelse til CyWG er det uklart hva som skjer videre med denne informasjonen. Det diskuteres ikke i CyWG om hvem som eier risikoen, om det er rammet taktisk sjef, eller Sjef FOH. Det fremkommer også stor usikkerhet knyttet til hvem som kan friskmelde systemer og sette enheter tilbake i drift, samt hvem som bærer denne risikoen. At det er CSS og teknisk personell som i stor grad støtter utførelse og gir anbefalinger er det enighet om, men det er uavklart hvem som vurderer og eier risikoen. Fra operasjonelt nivå uttrykkes det en forventning om at det er rammet styrkesjef som eier problemet og dermed også eier risikoen. Dette er også i tråd med den tidligere nevnte forventningen fra operasjonelt nivå om at taktiske styrkesjefer selv bringer cyberrelaterte hendelser inn i FOHs beslutningsprosess, og at det ikke gjøres av J6 som en output fra CyWG.

I håndteringen av en cyberrelatert hendelse er det mange aktører som involveres. Få av disse aktørene har tydelig avklarte roller. FOH sin rolle i den operative søylen bør være tydelig, men også her er det uklarheter som verken operativt planverk eller konsepter gir svar på. I tillegg er det også en rekke sivile aktører som har en rolle inn i håndtering av en slik hendelse som også må hensyntas i en DCO. Deres rolle er også lite oppgått og oppleves av respondentene som uklar. En av respondentene peker også på at i CyWG er det ulike aktører med ulike agendaer, for eksempel MilCERT[17]-funksjonen som CSS innehar bidrar til å vanskeliggjøre situasjonen. Innenfor CERT-miljøet er det et større fokus på deling av informasjon og lite fokus på vurdering av konsekvenser for militære operasjoner. At CSS gis en direkte kommunikasjonskanal inn mot operasjonelt nivå og tar

[17] MilCERT er forsvarssektorens responsmiljø for cyberrelaterte hendelser. Funksjonen innebærer ansvar for å overvåke, oppdage og svare på cybersikkerhetshendelser og trusler rettet mot Forsvarets nettverk, systemer og informasjon.

mye plass i CyWG, medfører at de mentale modellene som skapes på subtaktisk nivå også påvirker forholdet mellom taktisk og operasjonelt nivå.

> «Jeg er usikker på hvor man vil med CyWG, i prinsippet skal jo det som håndteres der håndteres av 3'er og 5'ere, men de er ikke til stede. Jo mer vi holder på med CyWG jo mindre sikker er jeg på hva vi egentlig holder på med» (R4).

Enkelte respondenter påpeker utfordringer knyttet til hvor ansvaret for DCO er plassert på operasjonelt nivå. J6 har opprettet en egen cybersikkehetsseksjon, og det er disse taktisk nivå møter på operasjonelt nivå i alle saker som angår cyberdomenet. Denne måten å håndtere domenet på avviker fra hvordan øvrige domener tilnærmes i hovedkvarteret, og det avviker fra hvordan mange andre operasjonelle hovedkvarter i blant annet NATO plasserer ansvaret. Dette fører igjen til at cyberdomenet håndteres på en annen måte og ikke integreres tilstrekkelig i operasjonsplanleggingen. En annen respondent har et litt annet perspektiv på dette og mener det er svært positivt at FOH har et 6'er-miljø som kan gå inn i plangrupper og bidra som fageksperter, men poengterer også at dersom dette skal fungere i praksis krever det mer skolering av J6-personellet. Respondenten tillegger at det finnes et stort mulighetsrom da FOH ikke avviser de innspillene som kommer fra taktisk nivå, men at taktisk nivå er mindre gode til å utnytte muligheten.

Implementering av en innovasjon er ofte mer utfordrende dersom aktøren som skal gjennomføre implementeringen er en organisasjon og ikke individer. De som skal stå for implementeringen er ikke de samme som har tatt beslutningen om at innovasjonen skal aksepteres (Rogers, 2003, s. 179). Denne utfordringen gjelder i stor grad for innføringen av cyberdomenet som et krigføringsdomene. Beslutningene tas på politisk og strategisk nivå, men det er personellet på operasjonelt og taktisk nivå som skal sette det ut i live. Med manglende tydelige føringer og ledelse som adressert i beslutningssteget, vil implementeringen bli utfordrende.

> «For å adressere cyber bedre fra et fellesoperativt nivå trenger vi en felles metodikk, felles mål og prosess. FOH vet ikke hva de skal bruke data de får til» (R2).

Det er bred enighet blant respondentene om at det mangler en felles forståelse av og tilnærming til planlegging av DCO. Siste versjon av *Comprehensive operations planning directive*[18] (NATO ACO, 2021) har tatt inn cyberdomenet, men i veldig liten grad. *Forsvarets stabshåndbok for Hæren* (Hæren, 2021) som danner grunnlaget for plan og beslutningsprosess (PBP) på fellesoperativt nivå, tar ikke inn cyberdomenet. NATOs cyberdoktrine skisserer løst hvilken rolle cyberoperasjoner har i en

[18] Comprehensive operations planning directive (COPD) er NATOs direktiv for operasjonsplanlegging

planlegging, men går ikke inn på hvordan dette skal gjennomføres i praksis (AJP-3.20, 2019, pargr. 3). Dette innebærer at det ikke finnes en etablert omforent metodikk for hvordan DCO skal planlegges og gjennomføres.

Flere respondenter belyser utfordringen med stammespråket som preger cyberfagfeltet og hvordan dette forsøkes tolket inn i en planprosess. Det gjøres forsøk på å omsette det tekniske stammespråket til ordbruk som er kjent fra militære landdoktriner, men det oppleves at dette ikke treffer godt nok. Én respondent stiller seg undrende til at valget har falt på å tilpasse «cybertaktikkene» til begrepsbruk fra landoperasjoner da disse to domene er langt fra hverandre. Respondenten mener det ville vært mer naturlig å se til for eksempel lufttaktikker da disse oppleves å være med i tråd med de utfordringer planleggingen og gjennomføringen av en DCO kan støte på.

Som tidligere nevn under første steg – Kunnskap-, så treffer opplæring innen cyberfaget hovedsakelig de som allerede har en grunnleggende forståelse basert på utdanning og erfaring, fremfor å treffe eksempelvis planpersonell på taktisk og operasjonelt nivå. Flere respondenter erkjenner at de selv har en viktig rolle i å sørge for at planpersonellet gis en grunnleggende forståelse for cyberdomenet slik at dette kan tas høyde for i planleggingen av operasjoner på taktisk nivå og i fellesoperasjoner. Én respondent vurderer at Forsvaret i dag ikke evner å se på cyberdomenet som et krigføringsdomene. Fokuset rettes mot administrative tiltak og cybersikkerhet. Konsekvensene av at FOH ikke har forstått hvordan de kan implementere cyberdomenet i eget planverk forplantes nedover i den hierarkiske militære organisasjonen.

Ett poeng som trekkes frem blant respondentene er at cyberdomenet bør inn og diskuteres på de samme arenaene som øvrige domener. Videre fremheves det at med en MDO tilnærming vil Forsvaret evne å se større på hvordan alle maktmidler kan samordnes og at alle beskyttelsestiltakene rettes mot ett sett med felles målsetting, ikke at de ulike taktiske kommandoene og FOH jobber mot hver sine mål.

Delkonklusjon

Gjennom interaksjonen mellom respondentene i T2 observeres det at forståelsen av utfordringene er svært ulike på taktisk og operasjonelt nivå. Fra taktisk nivå er det klare forventninger om at FOH skal lede CyWG og at dette er arenaen for å ta cyberdomenet inn i hovedkvarterets beslutningssløyfe. Fra operasjonelt nivå er derimot oppfatningen en helt annen, at de heller kan bistå den taktiske styrkesjef som løfter utfordringene med faglig støtte i FOHs beslutningssløyfe. Denne divergensen fremstår som en av årsakene til at respondentene opplever at CyWG ikke fungerer som det skal.

Roller bør klargjøres, ansvar fordeles og dokumenteres og aktørene bør opprette dialog. Kommunikasjon er nøkkelen for at denne arbeidsgruppen skal flyte bedre.

At kunnskap om militære cyberoperasjoner er lav i Forsvaret preger også samarbeidet mellom taktisk og operasjonelt nivå. Subtaktisk/teknisk nivå gis en unaturlig tilgang direkte til operasjonelt nivå, noe som også medfører at detaljgraden i det som håndteres ved J6 FOH er uhensiktsmessig høy. Rollene bør synliggjøres mellom alle tre nivåene, og CDOC bør på banen og ta sin rolle som taktisk kommando i dialogen fra Cyberforsvaret opp til FOH.

I omsetting av teknisk stammespråk gjøres det et forsøk å skape en felles forståelse gjennom begreper fra landoperasjoner, dette treffer målgruppen i liten grad, og resultatet er at begrepene vannes ut blant dem som faktisk forstår dem, samtidig som det ikke oppnås ønsket effekt hos eksempelvis planpersonell og beslutningstakere på operasjonelt nivå. For å lykkes med denne omsettingen bør begrepsbruken formaliseres gjennom doktrine. Det kan for eksempel ses til Forsvarets nye landdoktrine[19], hvor AJP 3.2[20] er operasjonalisert til norske forhold (Forsvarsstaben, 2024). Tilsvarende operasjonalisering bør også gjøres av AJP 3-20.

Implementeringen av cyberdomenet i Forsvaret og DCO som en del av fellesoperasjoner har gått sin gang over flere år, og fra taktisk og operasjonelt nivå kommer det frem flere faktorer som påvirker dette. Mentale modeller skapes på bakgrunn av deres egen kunnskap, erfaring og ståsted. I implementeringssteget kommer det frem tydelige forskjeller i aktørenes mentale modeller. Avviket fremstår som stort, men enkelt å redusere gjennom effektiv kommunikasjon.

5.5 Bekreftelse - Evaluering

«På bekreftelsesstadiet søker individet forsterkning for innovasjonsbeslutningen som allerede er tatt. På dette stadiet søker individet å unngå dissonans eller å redusere den hvis den oppstår» (Rogers, 2003, s. 189). Dette er det siste steget i Rogers innovasjons-beslutningsprosess. Dette steget kommer etter at beslutningen om å akseptere innovasjonen er tatt og implementering har funnet sted. Nå søker aktøren bekreftelse på sin beslutning gjennom erfaringer og tilbakemeldinger fra andre som har brukt innovasjonen (Rogers, 2003, s. 189–192).
I Forsvaret er det lange tradisjoner for å drive med erfaringshåndtering, og Forsvaret omtales ofte som en lærende organisasjon. I Forsvarssektorens verdigrunnlag fremheves også lederens ansvar for

[19] Forsvarets Doktrine for Landoperasjoner (FDLO) er i skrivende stund ikke effektuert, men er godkjent av doktrinerådet.
[20] Allied Joint Doctrine for Land Operations, NATO sin doktrine for landoperasjoner.

at læring finner sted «Ledere har et spesielt ansvar for å bygge en nysgjerrig og lærende organisasjon som er åpen for å utvikle seg, som gir rom for kreativitet og nytenkning, og det å gjøre feil» (Forsvarsdepartementet, 2021, s. 9). I FFOD tekkes det også frem erfaringshåndtering og doktrinerevisjon som et steg i fellesoperasjoner i det operasjonelle rammeverket (Forsvaret, 2019, s. 07012).

NATO benytter begrepet Lessons Learned (LL) for å beskrive aktiviteter knyttet til det å lære av erfaring i den hensikt å oppnå forbedring (AJP-3, 2019, s. E-1). LL betraktes som en viktig del for å være troverdig, kapabel og tilpasningsdyktig i krigføring og krigføringsutvikling gjennom å redusere operativ risiko, øke kostnadseffektiviteten og forbedre operativ effektivitet (JALLC, 2022, s. 9).

Erfaringshåndtering er dekket i liten grad av respondentene i denne oppgaven. Respondentene uttrykker en rekke meninger om forhold som kunne vært forbedret og flere har reflektert over at lite blir dokumentert. Som det ble fremhevet i implementeringssteget så mangler det felles prosesser og de prosessene som eksisterer er ofte lite utnyttet da cyberdomenet i mange tilfeller blir behandlet som «noe annet». Flere respondenter trekker frem nylige erfaringer fra øvelser som GRAM 23 og Cyber Coalition 23[21], men disse observasjonene fremstår som deres personlige synspunkter og ikke dokumentert og strukturert i en erfaringshåndteringsprosess. I CyWG er heller ikke erfaringshåndtering innen cyberdomenet et tema som diskuteres regelmessig.

> «Det er viktig å få tegnet ting ned. Personell rullerer og om vi ikke har noe dokumentert så virker det ikke» (R7).

En respondent peker på noe av kjernen som vist i sitatet. Erfaringer bør dokumenteres for å gi effekt. Dette suppleres også av en respondent som påpeker at kun dokumentering ikke er nok, men at erfaringer som er nedtegnet også bør følges opp. En annen respondent reflekterer også over hvordan planprosessen knyttet til utviklingen av Joint Coordination Order (JCO)[22] er en god eksersis, men at de læringsmomentene som trekkes ut av det arbeidet er noe de kun får kjørt gjennom en gang i året, noe som medfører at det går lang tid mellom hver gang.

> «Skal vi få FOH opp i ringene må de søke mot NATO-organisasjonene og omsette det de gjør til norske forhold» (R8).

[21] Cyber Coalition er NATOs største kollektive cyberforsvarsøvelse. Øvelsen planlegges og gjennomføres årlig av Allied Command transformation (ACT), under ledelse av Militærkomiteen (NATO, 2024).
[22] Koordineringsordre som utgis av FOH for å koordinere operasjoner og aktiviteter knyttet til det operative planverket Joint Guard.

Respondenten trekker frem at FOH bør skaffe seg overhøyde over de taktiske kommandoene, og mener at det kan best gjøres ved å se til andre større organisasjoner som har mer erfaring, eksempelvis NATO. Respondenten påpeker at FOH er opptatt av en flerårig utviklingsplan og det er naturlig at DCO inkluderes der. Skal dette oppnås bør de ha en formening om hva som ønskes oppnådd. Flere av respondentene fremhever at Cyberforsvarets våpenskole er et miljø som kan bidra til dette, men at den meste av læringen for operasjonelt nivå ikke bør skje fra taktisk.

Delkonklusjon

Under første verdenskrig ble stridsvogner introdusert som en innovasjon. Fra idé til produksjon tok det bare femten måneder. Utfordringen var ikke å bestemme seg for å produsere dem, men å evaluere den strategiske verdien sammenlignet med andre krigføringsmetoder. Et strategisk effektivitetsmål måtte etableres før læring fra erfaring fant sted. Deretter måtte hæren tilpasse seg for å bruke stridsvognene effektivt, en prosess som tok over førti måneder. Forsinkelsen i implementeringen skyldtes organisatorisk læringstreghet, knyttet til utfordringer med å definere effektivitetsmål, evaluere innovasjonen og mangelen på sentrale kontroller (Rosen, 1991, s. 127–128).

Å lære fra erfaring tar tid. Forsvaret har gode prosesser for erfaringshåndtering, men dette følges opp i liten grad innenfor cyberdomenet. Evaluering av hvor Forsvaret står i forhold til implementering av cyberdomenet på alle nivåer er fraværende, og lite strukturert læring skjer mellom taktisk og operasjonelt nivå. Aktørene gjør seg opp sine egne meninger og erfaringer fra ulike aktiviteter uten at dette adresseres i fellesskap. På denne måten kan aktørenes mentale modeller potensielt utvikle seg i ulike retninger og gapet mellom de mentale modellene vil øke.

Dersom en aktør får en positiv bekreftelse på at innovasjonen fungerer, vil dette styrke troen på innovasjonen, men om aktørene opplever negativ kommunikasjon vil det kunne føre til tvil og en svakere oppslutning om innovasjonen (Rogers, 2003, s. 189). Skal Forsvaret unngå dissonans i håndteringen av cyberdomenet og DCO er det hensiktsmessig at denne kommunikasjonen tas frem i lyset. Aktørene bør snakke sammen for å skape en felles forståelse og finne felles løsninger på utfordringene. At taktisk og operasjonelt nivå sitter på hver sine problemløsninger kan kanskje bidra til at gapet mellom de øker. Et større fokus på erfaringshåndtering som et verktøy vil potensielt kunne avdekke divergens mellom aktørenes forståelse og bidra til en forståelse av behovet for felles mentale modeller.

6 Mentale modeller og doktrine

Gjennom analyse og diskusjon av empiri er det avdekket flere områder hvor aktørenes mentale modeller kan påvirke taktisk og operasjonelt nivå i Forsvarets evne til militær innovasjon. Sammenhengen mellom mentale modeller og doktrineutvikling er sterk og i dette kapitlet vil det beskrives nærmere de funn som er utledet knyttet til mentale modeller og doktriners rolle.

6.1 Mentale modeller

For planlegging og gjennomføring av defensive cyberoperasjoner mellom ulike nivåer, er det en forutsetning at aktørene har en felles forståelse av cyberdomenet. Samvirket mellom taktisk og operasjonelt nivå forutsetter at felles mentale modeller er til stede. Felles mentale modeller bidrar til en samlet og helhetlig tilnærming til de utfordringer som aktørene møter.
I figur 6-1 er utfordringer i kommunikasjonen mellom taktisk og operasjonelt nivå illustrert. Taktisk og operasjonelt nivå samhandler i stor grad innenfor rammen av det operasjonelle planverket, Joint Guard. Som tidligere belyst har også dette planverket utfordringer i integreringen av cyberdomenet og defensive cyberoperasjoner. Dette preger kommunikasjonen mellom nivåene allerede før planer er effektuert.

Utenfor dette samarbeidet står en rekke eksterne aktører som også har en rolle i innføring og bruk av innovasjonen. Listen er ikke uttømmende, og kun eksempler på aktører for de ulike nivåene er illustrert.

NATO utgir doktriner for fellesoperasjoner og cyberoperasjoner[23], disse ratifiseres av Norge uten at de nødvendigvis er omsatt til norske forhold. Doktriner introduseres mot både taktisk og operasjonelt nivå uten at deres roller og ansvar i oppfølgingen av doktrinene er utledet og tydeliggjort. Politisk og strategisk nivå beslutter den overordnede retningen for cyberdomenet i Norge og Forsvaret. Fra respondentene fremkommer det at hva dette betyr for taktisk og operasjonelt nivå ikke er tydelig for aktørene.

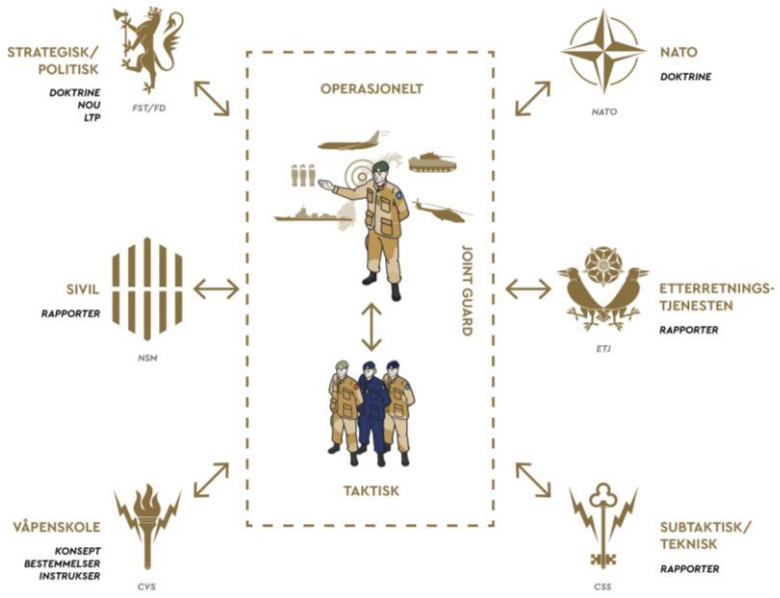
Etterretningstjenesten har rollen som Cyber commander og er gitt fagmyndighet for cyberoperasjoner. Deres rolle er svært utydelig og det skilles i liten grad på deres forhold til taktisk og til operasjonelt nivå, den samme informasjonen kommer til begge nivåer. Det samme gjelder for rapportering fra subtaktisk og teknisk nivå, i denne figuren illustrert ved Cyberforsvarets Cybersikkerhetssenter. Disse rapporterer hendelser og trusler i cyberdomenet, og samme

[23] AJP 3 Allied Joint Doctrine for the conduct of operations og AJP 3.20 Allied Joint Doctrine for cyberspace operations

rapportering går i stor grad direkte til både taktisk og operasjonelt nivå. Når roller og ansvar ikke er tydelig kjent for aktørene er det uklart hvem som gjør hva med denne informasjonen. Mentale modeller formes hos den enkelte aktør uten fokus på behovet for en felles mental modell.

Våpenskoler, her eksemplifisert med Cyberforsvarets våpenskole utgir konsepter, bestemmelser og instrukser som skal bidra til avklaringer og felles forståelse for cyberdomenet. At slike dokumenter effektueres med mindre involvering fra taktisk og operasjonelt nivå kan bidra til økt usikkerhet knyttet til aktørenes roller. Dokumentene kan bidra til at divergens mellom aktørenes mentale modeller reduseres, men dette krever at aktørene samles om produktene og at disse utarbeides i tråd med andre ledelsesprodukter.

Til slutt er også sivile aktører inkludert i figuren, dette forholdet er ikke dekket i oppgaven da fokuset er på forholdet mellom taktisk og operasjonelt nivå i den militære hierarkiske strukturen, men det er vanskelig å komme utenom at forholdet til sivile aktører også preger de mentale modellene til taktisk og operasjonelt nivå. I figuren er sivilt nivå illustrert med Nasjonal Sikkerhetsmyndighet som den største aktøren, men her skjuler det seg et stort antall aktører fra ulike sektorer.



Figur 6-1 Aktører som påvirker forholdet mellom taktisk og operasjonelt nivå i Forsvaret

All kommunikasjon inn til taktisk og operasjonelt nivå, sendes i ulike kanaler direkte til begge nivåer. Igjen fremkommer det ikke hvem som skal gjøre hva med informasjonen som mottas. Informasjonen behandles ikke nødvendigvis på rett nivå og rådata kommer rett inn til flere aktører. FFOD

understøtter også at dette medfører kommandomessige utfordringer da det fastslås at «informasjon må behandles før den kan brukes» (Forsvaret, 2019, pargr. 06032).

Oppsummert er det flere områder hvor respondentene indikerer motstridende oppfatninger som understøtter at taktisk og operasjonelt nivå har divergerende mentale modeller. Enkelte faktorer er dog sammenfallende og kan indikere felles mentale modeller. Det vil være en mengde faktorer som påvirker aktørenes mentale modeller, de som er identifiser i denne oppgaven er oppsummert i figur 6-2.

Taktisk nivå	Operasjonelt nivå
- FOH skal lede og gi føringer - FOH skal bringe output fra CyWG inn i øvrige prosesser - Usikkerhet på hva som er CDOC sin rolle - Hvordan begreper tolkes	- De taktiske skal ta mer ansvar - Taktiske styrkesjefer selv bringer saker inn i øvrige prosesser - Forventninger om at CDOC skal ta en større rolle - Hvordan begreper tolkes
Felles	
Forholdet til Cyber commander	
Usikkerhet roller, ansvar og myndighet	
Kunnskap og kompetanse	

Figur 6-2 Divergerende og sammenfallende faktorer i de mentale modellene på taktisk og operasjonelt nivå

Med divergerende mentale modeller vil aktørene ha ulike forståelse av hvordan de ulike produktene skal håndteres og det legges opp til at det er den enkeltes tolkning som blir styrende. Dersom aktørene ikke samles og setter fokus på etablering av felles mentale modeller vil de potensielt fortsette å snakke forbi hverandre og samarbeidet mellom de to nivåene vil være dysfunksjonelt.

6.2 Doktrine

Et av de typiske problemene i spredningen av innovasjon er at aktørene ofte er en blandet gruppe bestående av ulike individer. Denne forskjellen fører ofte til ineffektiv kommunikasjon da aktørene ikke snakker samme språk. Det ligger til spredningsteoriens natur at den preges av ulike aktører, mens det ideelt sett for effektiv kommunikasjon er en viss grad av likhet i andre variabler som påvirker aktørenes mentale modeller, selv om de divergerer i synet på innovasjonen (Rogers, 2003, s. 18–19).

En kommunikasjonskanal er måten en melding bringes fra en aktør til en annen. Informasjonsutvekslingen mellom aktører påvirkes av det eksiterende forholdet som råder mellom

dem. Dette påvirker i stor grad hvordan informasjon om innovasjonen blir delt, og hvordan den blir mottatt og integrert av mottakeren (Rogers, 2003, s. 18).

Doktrine som et verktøy for standardisering vil kunne bidra som en kommunikasjonskanal mellom aktørene og skape felles mentale modeller. Operasjonalisering av doktrine vil påvirke hvordan budskapet kommuniseres og mottas samt hvordan de mentale modellene bygges. Samtidig som de mentale modellene igjen vil påvirke hvordan doktrinen formes og utvikles videre. Mentale modeller gir grunnlaget for hvordan militære ledere og operasjonsplanleggere forstår og tolker situasjoner og utfordringer. Doktriner er utformet basert på et sett av mentale modeller om hvordan militære operasjoner skal gjennomføres mest effektivt. Samlet sett spiller mentale modeller en sentral rolle i utforming, implementering og utvikling av militære doktriner.

Som Høiback argumenterer for, er doktriner et ledelsesverktøy, endringsverktøy og læringsverktøy (Høiback, 2011, 2013, s. 888–889). I alle disse formene, men spesielt som læringsverktøy vil doktriner i stor grad bidra til å forme felles mentale modeller.

7 Konklusjon

Hensikten med denne oppgaven har vært å undersøke hvorfor forholdet mellom taktisk og operasjonelt nivå oppleves som uavklart i planlegging og gjennomføring av defensive cyberoperasjoner som en del av fellesoperasjoner. Dette har blitt utforsket gjennom to forskningsspørsmål som benytter teori om militær innovasjon, spredningsteori og mentale modeller som rammeverk.
Hvordan påvirker aktørenes mentale modeller og evne til militær innovasjon forholdet mellom taktisk og operasjonelt nivå innen defensive cyberoperasjoner?

Funn i oppgaven indikerer at mentale modeller kan ha en avgjørende betydning for at Forsvaret skal lykkes med en effektiv militær innovasjon. Fokuset på hvor mentale modeller sammenfaller og divergerer kan bidra til en mer helhetlig tilnærming til defensive cyberoperasjoner. De operasjonelle dilemmaene vil i bedre forstås i fellesskap, og oppgaver fordeles hensiktsmessig mellom aktørene dersom kommunikasjonen er mer åpen.

Funnene i oppgaven sett i lys av Everett M. Rogers sine fem karakteristikker for en innovasjon indikerer at det finnes naturlige forklaringer på hvorfor forholdet mellom taktisk og operasjonelt nivå oppleves som utfordrende.

Å spre kunnskap ut i Forsvaret, ut over personell med defensive cyberoperasjoner som primæroppgave, vil bidra til at de mentale modellene som formes om cyberdomenet vil være mindre divergerende. Dersom det oppnås en forståelse av innovasjonens relative fordel, vil spredningen også gå raskere og med mindre motstand.

Gjennom at cyberdomenet fremstilles som noe helt spesielt som krever en annen tilnærming enn øvrige domener øker avstanden mellom de mentale modeller som formes hos beslutningstakere og personell på taktisk og operasjonelt nivå. Cyberdomenet fremstilles som mer komplekst og mindre kompatibelt med eksisterende verdier, erfaringer og behov. Dette medfører en langsommere spredning av innovasjonen.

Det som ikke kan observeres er også vanskelig å teste ut og forstå. Cyberdomenets abstrakte natur bidrar til at aktørene former egne mentale modeller dersom doktriner og konsepter ikke peker i samme retning. Lav grad av etterprøvbarhet og observerbarhet bidrar til en lavere hastighet på integrering av defensive cyberoperasjoner i fellesoperasjoner. At cyberdomenet er innført som en forebyggende innovasjon understøtter ytterligere at det vil være en lavere spredningshastighet enn andre innovasjoner.

Disse faktorene påvirker i stor grad forholdet mellom taktisk og operasjonelt nivå. Usikkerhet knyttet til roller, ansvar og myndighet innenfor cyberdomenet kombinert med lav bevissthet knyttet til divergerende mentale modeller gjør forholdet dysfunksjonelt. Aktørene jobber ikke nødvendigvis mot ulike mål, men forståelsen av målet og veien dit ser ulik ut.

Ut fra disse faktorene vil det være krevende å drive militær innovasjon i form av innføring av cyberdomenet som et krigføringsdomene og integrering av defensive cyberoperasjoner i fellesoperasjoner. Spredningsteorien bidrar med en årsaksforklaring til hvorfor det oppleves liten reell fremgang til tross for god kompetanse blant mye av personellet og høy satsning på cyberfagfeltet. Innovasjonen er ikke spredt godt nok ut i Forsvaret til at vi får med oss den sene majoriteten og etternølerne.

Hvordan kan doktrine bidra til en felles tilnærming til defensive cyberoperasjoner som en del av fellesoperasjoner?

Skal Forsvaret lykkes med en reell integrasjon av nye domenet og nye måter å operere på, bør tilnærmingen til fellesoperasjoner endres. Å fortsette å operere som før og bare legge til nye

domener som cyberdomenet og romdomenet gir ingen reell integrasjon. Den relative fordelen for militære operasjoner bør kommuniseres tydelig og forstås på alle nivåer i Forsvaret.

I byggingen av felles mentale modeller har doktriner en vital rolle. Doktrine kan bidra med de overordnede prinsippene, avklare begreper og peke ut retningen, men innholdet må forstås av aktørene og det må forstås i konteksten av deres egne roller.

Operasjonalisering av NATO sin cyberdoktrine, *AJP 3.20 ALLIED Joint Doctrine for cyberspace operations* og *Forsvarets fellesoperative doktrine* er nødvendig for å skape felles forståelse i Forsvaret, og for at taktisk og operasjonelt nivå skal kunne fordele sine roller hensiktsmessig.

All informasjon som tilkommer aktørene (ref. figur 6-1) utenfra, bør håndteres på en enhetlig måte. Det bør være en tydelighet i hvem som håndterer hva og hva aktørene kan forvente fra hverandre. De mentale modellene bør bygges i fellesskap med utgangspunkt i en felles forståelse av doktrine, planverk og andre styrende dokumenter.

Avslutningsvis kan det gjennom analyse av funn i denne oppgaven tydelig pekes på at forholdet mellom taktisk og operasjonelt nivå ikke fungerer optimalt. Det er flere faktorer som påvirker dette forholdet, men analysen her har vært rettet mot defensive cyberoperasjoner. En operasjonalisering av doktriner, felles tilnærming til operasjonsplanlegging for alle domener basert på felles mentale modeller og tydelige rollefordelinger vil redusere mye av frustrasjonen og friksjonen som oppleves mellom nivåene.

Funnene i oppgaven i stor grad sammenfallende med Modig og Anderssons konklusjoner om mentale modellers innvirkning på militær innovasjon (2022, s. 59). Selv om oppgaven har hatt et noe annet fokus, kan det gjennom funnene bekreftes at Forsvaret sannsynlig er tjent med å sette et fokus på mentale modeller i en kapabilitetsutvikling.

Videre understøtter funnene Stephen Rosen sin argumentasjon for at militære organisasjoner er bygget konservativt og at militære byråkratier motstår endring i stor grad (1991, s. 2). En bevissthet og åpen kommunikasjon rundt de faktorene som fører til denne motstanden er derfor en nødvendighet for å lykkes med endring.

7.1 Videre forskning

Cyberdomenet er fortsatt ungt og umodent, selv om det er mye forskning som gjennomføres på området er det fortsatt mye å ta tak i. I arbeidet med denne oppgaven er det flere områder som har åpenbart seg som interessante å studere videre.
I fortsettelsen er det mange aspekter knyttet til mentale modeller som kan utforskes. Blant annet hvordan mentale modeller påvirker forholdet mellom sivile og militære aktører, og hvordan disse påvirker det sivil-militære samarbeidet.

Forholdet til Cyber commander har vært et gjennomgående tema i datainnsamlingen, og det er tydelig at det hersker mye usikkerhet knyttet til hva denne rollen innebærer. Uavklarte rollefordelinger skaper usikkerhet og friksjon. Dette forholdet vil være relevant inn mot en fremtidig problemstilling.

Hvordan Forsvaret planlegger og gjennomfører defensive cyberoperasjoner er en prosess som har tatt form over de siste 10-15 årene. *Konseptet for defensive cyberoperasjoner* ble først etablert i 2022. Det er ikke gjennomført noen større evaluering av verken konseptet eller hvordan prosessen gjennomføres på taktisk og operasjonelt nivå. En studie hvor det gjennomføres en fokusert evaluering, eller en sammenligning av andre nasjoner hvordan de planlegger og gjennomfører defensive cyberoperasjoner, ville gitt en bedre forståelse av aktørenes roller.

Til sist er forholdet mellom doktrine og mentale modeller et tema som i større grad kan belyses i den videre utviklingen og operasjonaliseringen av Forsvarets doktriner. Ytterligere forskning på dette området ville potensielt forsterket og videreutviklet funnene i denne oppgaven.

8 Litteraturliste

AJP-01. (2017). *Allied Joint Doctrine*. NATO. https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDE_V1_E_2437.pdf

AJP-3. (2019). *Allied Joint Doctrine for the conduct of operations*. NATO. https://www.coemed.org/files/stanags/01_AJP/AJP-3_EDC_V1_E_2490.pdf

AJP-3.20. (2019). *Allied Joint Doctrine for Cyberspace Operations*. NATO. https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

Andersen, M., & Ødegaard, G. (2016). *Militære fellesoperasjoner—En innføring*. Abstrakt. https://urn.nb.no/URN:NBN:no-nb_digibok_2021072248647

Brantly, A. F. (2016). *The Decision to Attack: Military and Intelligence Cyber Decision-Making*. University of Georgia Press.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*. https://doi.org/10.1191/1478088706qp063oa

Brunstad, K.-R. (2018). *Småstaten Norge – en cyberstormakt?* [Masteroppgave, Forsvarets høgskole]. http://hdl.handle.net/11250/2505617

Cannon-Bowers, J., Salas, E., & Converse, S. (1993). Shared mental models in expert team decision making. I *Individual and Group Decision Making: Current Issues*. L. Erlbaum Associates.

CCDCOE. (2020). *Cyber Commanders' Handbook*. CCDCOE.

CCDCOE. (2023). https://ccdcoe.org/about-us/

Craik, K. J. W. (1967). *The Nature of Explanation*. Cambridge University Press.

Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches* (sixth edition). SAGE Publications.

Cyberforsvaret. (2022). *Konsept for defensive cyberoperasjoner*. Cyberforsvaret.

Duguin, S., & Pavlova, P. (2023). *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*.

Economic security council of Ukraine. (2022). *Cyber, Artillery, Propaganda: Comprehensive Analysis of Russian Warfare Dimensions*. State Service of Special Communication and Information Protection of Ukraine. https://nsarchive.gwu.edu/document/30063-18-cyber-artillery-propaganda-comprehensive-analysis-russian-warfare-dimensions

Fornyings-, administrasjons- og kirkedepartementet. (2012). *Nasjonal strategi for informasjonssikkerhet*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-informasjonssikker/id710469/

Forsvaret. (2019). *Forsvarets fellesoperative doktrine*. Forsvarsstaben. https://regelverk.forsvaret.no/fileresult?attachmentId=18333277

Forsvaret. (2020). *(B) Konsept for nasjonale militære cyberoperasjoner*. Forsvaret. (Interndokument Forsvaret)

Forsvaret. (2023). *Trygghet i usikre tider Forsvarssjefens fagmilitære råd 2023*. Forsvaret. https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fagmilitaert-rad

Forsvarets stabsskole. (2010). *Stabshåndbok for Forsvaret*. Forsvarets høgskole. https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2405039/Stabsh%C3%A5ndbok%20for%20Forsvaret.pdf

Forsvarsdepartementet. (2014). *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren*. Forsvarsdepartementet. https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf

Forsvarsdepartementet. (2021). *Forsvarssektorens verdigrunnlag (2021)*. Forsvarsdepartementet. https://www.regjeringen.no/no/dokumenter/forsvarssektorens-verdigrunnlag/id2886672/

Forsvarsstaben. (2020). *Forsvarets grunnsyn på ledelse*. Forsvarsstaben. https://regelverk.forsvaret.no/fileresult?attachmentId=19703941

Forsvarsstaben. (2024). *Forsvarets doktrine for landoperasjoner (under utarbeidelse)*. Forsvarsstaben.

Gibson, W. (1982). *Burning Chrome*. Ace Books.

Gibson, W. (1984). *Neuromancer*. Ace Books.

Granlund, L., & Andersen, G. (2010). *Samfunnsvitenskapelig tenkemåter. Et hjelpehefte*. Universitetsforlaget.

Greenwood, D. J., & Levin, M. (2006). *Introduction to Action Research: Social Research for Social Change* (2nd edition). SAGE Publications.

Grissom, A. (2006). The future of military innovation studies. *Journal of Strategic Studies*, *29*(5), 905–934. https://doi.org/10.1080/01402390600901067

Handelsdepartementet, N. (2003). *Nasjonal strategi for informasjonssikkerhet*. regjeringen.no. https://www.regjeringen.no/no/dokumentarkiv/Regjeringen-Bondevik-II/nhd/Nyheter-og-pressemeldinger/2003/nasjonal_strategi_for_informasjonssikker/id249670/

Hæren. (2021). *Stabshåndbok for Hæren*. Forsvaret.

Høiback, H. (2011). What is Doctrine? *The Journal of Strategic Studies*, *34*(6), 879–900.

Høiback, H. (2013). *Understanding Military Doctrine: A Multidisciplinary Approach*. Routledge. https://doi.org/10.4324/9780203559345

Høiback, H. (2016). The Anatomy of Doctrine and Ways to Keep It Fit. *The Journal of Strategic Studies*, *39*(2), 185–197. https://doi.org/10.1080/01402390.2015.1115037

Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser? Innføring i Samfunnsvitenskapelig metode* (3. utg.). Cappelen Damm Akademisk.

JALLC. (2022). *Lessons Learned Handbook*. NATO. https://www.jallc.nato.int/application/files/4416/5781/2017/JALLC_LL_Handbook_Update_-_4th_Edition_FINAL_14072022.pdf

Johnson-Laird, P. N. (1983). *Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness*. Harvard University Press.

Justis- og beredskapsdepartementet. (2019, januar 30). *Nasjonal strategi for digital sikkerhetskompetanse*. https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhetskompetanse/id2627189/

Justis- og beredskapsdepartementet, & Forsvarsdepartementet. (2019a). *Nasjonal strategi for digital sikkerhet*. https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/

Justis- og beredskapsdepartementet, & Forsvarsdepartementet. (2019b). *Tiltaksoversikt til nasjonal strategi for digital sikkerhet*. https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhetskompetanse/id2627189/

Justis- og politidepartementet, Forsvarsdepartementet, Samferdselsdepartementet, & Fornyings- og administrasjonsdepartement. (2007). *Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010*. https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/fad-lav.pdf

Kramer, F., Starr, S. H., & Wentz, L. (2009). *Cyberpower and National Security* (1st ed.). Potomac Books.

Levin, M. (2017). Aksjonsforskning som forskning – epistemologiske og metodiske utfordringer. I *Aksjonsforskning i Norge: Teoretisk og empirisk mangfold*. Cappelen Damm Akademisk.

Martinsen, G. T. (2021). *Det fellesoperative problemet* [Masteroppgave, Forsvarets høgskole]. https://hdl.handle.net/11250/2832296

Masters, J. (1995). *The History of Action Research*.

Meld. St. 30 & (2019–2020). (2020). *En innovativ offentlig sektor Kultur, ledelse og kompetanse*. Kommunal- og moderniseringsdepartementet. https://www.regjeringen.no/contentassets/14fce122212d46668253087e6301cec9/no/pdfs/stm201920200030000dddpdfs.pdf

Meld. St. 38 (2016–2017). (2017). *IKT-sikkerhet—Et felles ansvar*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/

Microsoft. (2022). *Defending Ukraine: Early Lessons from the Cyber War*.

Mitchell, J. (1838). *Thoughts on Tactics and Military Organization: Together with an Enquiry Into the Power and Position of Russia*. Longman, Orme, Brown, Green and Longmans.

Modig, O. (2020). *Militär innovation som resultat av aktörers mentala modeller av ny teknologi* [Masteroppgave, Försvarshögskolan]. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1446128&dswid=7433

Modig, O., & Andersson, K. (2022). Military Innovation as the Result of Mental Models of Technology. *Scandinavian Journal of Military Studies*, *5*(1), 45–62. https://doi.org/10.31374/sjms.117

NATO. (2002, november 21). *Prague Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Cou...* NATO. https://www.nato.int/cps/en/natohq/official_texts_19552.htm

NATO. (2006). *Riga Summit Declaration issued by NATO Heads of State and Government (2006)*. NATO. https://www.nato.int/cps/en/natohq/official_texts_37920.htm

NATO. (2007). *Final Communiqué—Meeting of the North Atlantic Council in Defence Ministers Session*. NATO. http://www.nato.int/cps/en/natohq/news_47011.htm

NATO. (2012). *Chicago Summit Declaration issued by NATO Heads of State and Government (2012)*. NATO. https://www.nato.int/cps/en/natohq/official_texts_87593.htm

NATO. (2014). *Wales Summit Declaration Issued by the Heads of State and Government (2014)*. NATO. https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO. (2016, juli 9). *Warsaw Summit Communiqué issued by NATO Heads of State and Government (2016)*. NATO. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO. (2018). *Brussels Summit Declaration issued by NATO Heads of State and Government (2018)*. NATO. https://www.nato.int/cps/en/natohq/official_texts_156624.htm

NATO. (2019). *AJP-3 Allied Joint Doctrine for the Conduct of Operations*. NATO standardization office.

NATO. (2021a). *Brussels Summit Communiqué issued by NATO Heads of State and Government (2021)*. NATO. https://www.nato.int/cps/en/natohq/news_185000.htm

NATO. (2021b). *AAP-06 NATO Glossary of terms and definitions*. NSO.

NATO. (2023a, juli 11). *Vilnius Summit Communiqué issued by NATO Heads of State and Government (2023)*. NATO. https://www.nato.int/cps/en/natohq/official_texts_217320.htm

NATO. (2023b, oktober 5). *Multi-Domain Operations in NATO - Explained*. NATO ACT. https://www.act.nato.int/article/mdo-in-nato-explained/

NATO. (2024). *Cyber Coalition*. NATO ACT. https://www.act.nato.int/activities/cyber-coalition/

NATO ACO. (2021). *Comprehensive Operations Planning directive: Bd. 3.0*.

NOU 2015:13. (2015). *Digital sårbarhet – sikkert samfunn—Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

OECD & Eurostat. (2018). *Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation, 4th Edition*. OECD. https://doi.org/10.1787/9789264304604-en

Peirce, C. S. (1960). *Collected Papers of Charles Sanders Peirce* (Bd. 1). Harvard University Press.

Pinker, S. (2018). *Enlightenment Now: The Case for Reason, Science, Humanism, and Progress*. Penguin UK.

Prestmo, N. G. (2015). *Cybersikkerhet i væpnet konflikt* [Masteroppgave, Forsvarets høgskole]. Forsvarets høgskole. http://hdl.handle.net/11250/297650

Prop. 73 S (2011-2012). (2012). *Et forsvar for vår tid*. Forsvarsdepartementet. https://www.regjeringen.no/no/dokumenter/prop-73-s-20112012/id676029/?ch=1

Prop. 87 S (2023–2024). (2024). *Forsvarsløftet – for Norges trygghet—Langtidsplan for forsvarssektoren 2025–2036*. Forsvarsdepartementet. https://www.regjeringen.no/no/dokumenter/prop.-87-s-20232024/id3032217/

Prop. 151 S (2015–2016). (2016). *Kampkraft og bærekraft—Langtidsplan for Forsvaret*. Forsvarsdepartementet. https://www.regjeringen.no/no/dokumenter/prop.-151-s-20152016/id2504884/

Rogers, E. M. (2003). *Diffusion of innovations* (Fifth edition). Free Press.

Rosen, S. P. (1991). *Winning the Next War: Innovation and the Modern Military*. Cornell University Press.

Rummelhoff, S. M. (2021). *Militære operasjoner i cyberdomenet* [Masteroppgave, Forsvarets høgskole]. Forsvarets høgskole. https://hdl.handle.net/11250/2834228

Russel, A. L. (2014). *Cyber Blockades* (1st ed.). Georgetown University Press.

Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Bd. 1). Cambridge University Press.

Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Bd. 2.0*. Cambridge University Press.

Senge, P. M. (1991). Den femte disiplin: Kunsten å utvikle den lærende organisasjon. I A. Lillebø (Overs.), *Norbok*. Hjemmets bokforlag. https://urn.nb.no/URN:NBN:no-nb_digibok_2014070206047

SHAPE. (2021). *Comprehensive operations planning directive v 3.0*. ACO.

Smeets, M. (2022). *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*. Oxford University Press.

Utenriksdepartementet. (2017). *Internasjonal cyberstrategi for Norge*. https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategi_web.pdf

Vego, M. (2015). On Operational Leadership. *Joint Force Quarterly, 77*, 60–69.

Wiener, N. (1948). *Cybernetics or Control and Communication in the Animal and the Machine*. The MIT Press. https://doi.org/10.7551/mitpress/11810.001.0001

Willett, M. (2022). The Cyber Dimension of the Russia–Ukraine War. *Survival*, *64*(5), 7–26. https://doi.org/10.1080/00396338.2022.2126193

Zuber-Skenitt, O. (1993). Improving Learning and Teaching Through Action Learning and Action Research. *Higher Education Research and Development*, *12*(1), 45–58. https://doi.org/10.1080/0729436930120105

9 Vedlegg

Vedlegg A – Vurdering av behandling av personopplysninger

Sikt

Vurdering av behandling av personopplysninger

Referansenummer
291707

Vurderingstype
Automatisk

Dato
13.10.2023

Tittel
"Integrering av defensive cyberoperasjoner i fellesoperasjoner"

Behandlingsansvarlig institusjon
Forsvarets Høgskole / Forsvarets stabsskole

Prosjektansvarlig
Stig Tore Aannø

Student
Gry-Mona Nordli

Prosjektperiode
01.08.2023 - 31.05.2024

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 31.05.2024.

Meldeskjema

Grunnlag for automatisk vurdering
Meldeskjemaet har fått en automatisk vurdering. Det vil si at vurderingen er foretatt maskinelt, basert på informasjonen som er fylt inn i meldeskjemaet. Kun behandling av personopplysninger med lav personvernulempe og risiko får automatisk vurdering. Sentrale kriterier er:

- De registrerte er over 15 år
- Behandlingen omfatter ikke særlige kategorier personopplysninger;
  - Rasemessig eller etnisk opprinnelse
  - Politisk, religiøs eller filosofisk overbevisning
  - Fagforeningsmedlemskap
  - Genetiske data
  - Biometriske data for å entydig identifisere et individ
  - Helseopplysninger
  - Seksuelle forhold eller seksuell orientering
- Behandlingen omfatter ikke opplysninger om straffedommer og lovovertredelser
- Personopplysningene skal ikke behandles utenfor EU/EØS-området, og ingen som befinner seg utenfor EU/EØS skal ha tilgang til personopplysningene
- De registrerte mottar informasjon på forhånd om behandlingen av personopplysningene.

Informasjon til de registrerte (utvalgene) om behandlingen må inneholde

- Den behandlingsansvarliges identitet og kontaktopplysninger
- Kontaktopplysninger til personvernombudet (hvis relevant)
- Formålet med behandlingen av personopplysningene
- Det vitenskapelige formålet (formålet med studien)
- Det lovlige grunnlaget for behandlingen av personopplysningene
- Hvilke personopplysninger som vil bli behandlet, og hvordan de samles inn, eller hvor de hentes fra
- Hvem som vil få tilgang til personopplysningene (kategorier mottakere)
- Hvor lenge personopplysningene vil bli behandlet
- Retten til å trekke samtykket tilbake og øvrige rettigheter

Vi anbefaler å bruke vår mal til informasjonsskriv.

Informasjonssikkerhet
Du må behandle personopplysningene i tråd med retningslinjene for informasjonssikkerhet og lagringsguider ved behandlingsansvarlig institusjon. Institusjonen er ansvarlig for at vilkårene for personvernforordningen artikkel 5.1. d) riktighet, 5. 1. f) integritet og konfidensialitet, og 32 sikkerhet er oppfylt.

Vedlegg B – Samtykkeerklæring for respondenter

Forespørsel om deltagelse i datainnsamling til: ”Integrering av defensive cyberoperasjoner i fellesoperasjoner”

Dette er en forespørsel til deg om å delta som respondent i min masteroppgave. I dette skrivet gis du informasjon om masteroppgaven og hva deltakelse vil innebære for deg.

Bakgrunn og formål
Selv siden før Cyberdomenet ble anerkjent av NATO som et eget krigføringsdomene har Forsvaret forsøkt å integrere cyberforsvar og cyberoperasjoner på både operasjonelt og taktisk nivå. Til sammenligning med de tradisjonelle krigføringsdomenene land, sjø og luft har cyber og romdomenet fortsatt en lang vei å gå, og det er trygt å anta at det fortsatt er et stort forbedringspotensial i integreringen av cyberdomenet.
I min masteroppgave i militære studier ved Forsvarets høgskole ønsker jeg å se nærmere på i hvilken grad Forsvaret lykkes med dette, og mer spesifikt hvordan taktiske kommandoer bedre kan understøtte integrering av defensive cyberoperasjoner i fellesoperasjoner.

Den valgte problemstillingen er:
«Hvordan kan Forsvaret bedre sin evne til integrering av defensive cyberoperasjoner i fellesoperasjoner?»

For å komme frem til svar på denne problemstillingen vil jeg også søke å finne svar på hvordan Forsvarets taktiske kommandoer kan legge til rette for effektive defensive cyberoperasjoner samt integrering i fellesoperasjoner.

Informasjonen som innhentes for denne oppgaven vil kun benyttes til dette formålet.

Hvorfor du får spørsmål om å delta
Erfaringer fra din, og flere avdelinger i Forsvaret, rundt håndtering av spesifikke hendelser vil være relevant for å belyse hvordan personell på taktisk og operasjonelt nivå opplever og vurderer hvor Forsvaret står i dag. Ditt bidrag til denne oppgaven er ønsket på grunn av din kjennskap til egen organisasjon samt din rolle i planlegging og utøvelse av operasjoner i din organisasjon. Forkunnskap om defensive cyberoperasjoner er ingen forutsetning for å delta.

Hva det innebærer for deg å delta
Dersom du ønsker å delta i denne studien vil dette innebære deltagelse i en Tabletop øvelse hvor du sammen med flere kollegaer vil diskutere dere gjennom et scenario med ulike cyberoperasjoner som rammer deres organisasjon. I tillegg vil utvalgte deltagere gjennomføre et dybdeintervju påfølgende øvelsen for å fange opp refleksjoner og betraktninger rundt prosessen.

Øvelsen er estimert til å vare ca 90 minutter, avhengig av diskusjonene som oppstår rundt bordet. Påfølgende intervju vil ta inntil 60 minutter. Dersom graderingsnivå tillater, vil det tas opptak av både øvelsen og intervjuet og jeg vil supplere med egne notater.

Det er frivillig å delta
Det er frivillig å delta i studien. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Behandling av dine personopplysninger
Jeg vil kun bruke personlige opplysninger for å komme i kontakt med deg. All identifiserbar informasjon, både navn og stilling vil være anonymisert når oppgaven publiseres. All informasjon om deg vil behandles konfidensielt og i samsvar med personvernregelverket. Ditt navn og kontaktopplysninger vil under databehandlingen erstattes med en kode som lagres på egen navneliste adskilt fra øvrige data lokalt på min FO365 klient og vil kun være tilgjengelig for meg. I oppgaven vil det kunne publiseres hvilke avdelinger som har deltatt, men det vil ikke kobles observasjoner, uttalelser direkte til en avdeling med mindre dette er avklart på forhånd.

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

- innsyn i hvilke opplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Jeg behandler opplysninger om deg basert på ditt samtykke. Studien er også meldt inn til Norsk senter for forskningsdata (NSD). Dette innebærer at jeg har forpliktet meg til å oppbevare data knyttet til studien på en forsvarlig måte, samt å slette alle personidentifiserende opplysninger når oppgaven er avsluttet. Oppgaven skrives i perioden 01.08.2023 – 31.05.2024, alle opptak og notater som inneholder personidentifiserende opplysninger vil slettes etter denne perioden.

Hvis du har spørsmål til studien, eller forhold du ønsker å ta opp, ta kontakt per mail eller telefon.

Kontaktinformasjon masterstudent:
Epost: gnordli@mil.no

Kontaktinformasjon veileder ved FHS:
Epost: saanno@mil.no

Kontaktinformasjon Forsvarets personvernombud:
Epost: forsvarets.personvernombud@mil.no Telefon 915 03 003

Med vennlig hilsen

Gry-Mona Nordli, Mastergradsstudent, Forsvarets Høgskole

Samtykkeerklæring

Jeg samtykker til å delta i studien og at mine opplysninger behandles frem til oppgaven er avsluttet

---

(Signert av respondent, dato)

Vedlegg C - Intervjuguide

Bakgrunn

Som en del at min masterstudie ved Forsvarets høgskole vil jeg skrive en masteroppgave hvor jeg ønsker å se på Forsvarets evne til å håndtere Cyberoperasjoner som rammer Forsvarets systemer og operasjoner. Gjennom å søke etter svar på problemstillingen «Hvordan kan Forsvaret bedre sin evne til integrering av defensive cyberoperasjoner i fellesoperasjoner» vil jeg forsøke å komme frem til konkrete tiltak som kan bedre Forsvarets evne til å motstå fiendtlige cyberoperasjoner.

Hypotese 1: Forsvarets fellesoperative nivå er ikke i mål med integrering av cyberdomenet i sine fellesoperasjoner (utkast)
Hypotese 2: Taktiske kommandoer har et potensiale i å understøtte defensive cyberoperasjoner i fellesoperasjoner (utkast)

Informasjon

Del 1 - Rammer for intervjuet og bakgrunn for problemstillingen

- Presentasjon
- Intervjuformen er semi-strukturert, hvor det er ønskelig at informanten snakker og reflekterer mest mulig på egenhånd. Tilleggsspørsmål vil benyttes for oppklaring, utdyping eller for å holde intervjuet på rett spor.
- Bakgrunn for masteroppgaven
- Samtykke – eget skjema
- Gradering
- Eventuelle spørsmål fra informanten

Del 2 – Refleksjoner rundt tabletop/øvelser

1. Betraktninger/refleksjoner rundt caseoppgaven?
2. Var diskusjonen/øvelsen konstruktiv? Realistisk?
3. Ser du faktorer fra denne øvelsen som kan være nyttig inn mot andre prosesser ved hovedkvarteret? Evt hvilke?
4. Hvilken informasjon ser du fra denne øvelse som kunne vært verdifull inn mot andre prosesser i din avdeling?
5. Hva forventer du bør håndteres av
    a. Egen avd
    b. FOH
    c. Andre taktiske/hvilke
    d. Andre (Hvem)

Del 3 – Tanker rundt integrasjon av cyber i Forsvaret

6. Hva kunne vært gjort for at dere fikk bedre forståelse for egne avhengigheter av cyberdomenet?
    a. Evt hvordan kunne cyber vært adressert bedre fra fellesoperativt nivå
7. Hvordan vil du vurdere modenheten innen cyber?

    a. egen avd
    b. FOH
    c. Forsvaret
8. I hvilken grad vil du si cyberdomenet er integrert i Forsvaret?
    a. Hva ser du på som hovedutfordringen?
    b. Hva kunne vært gjort bedre?
    c. Hva forventer du andre bør bidra med?
9. Hvilke tiltak kan din organisasjon gjøre for bedre integrasjon av cyber?
    a. Hvilke tiltak kan andre (evt hvem) gjøre for å bedre integrasjon av cyber?
10. Er FOH i stand til å lede defensive cyberoperasjoner fra fellesoperativt nivå?
    a. Er de taktiske kommandoene i stand til å lede defensive cyberoperasjoner på taktisk nivå?
    b. Understøtte cyberoperasjoner på fellesoperativt nivå?

Avslutning

11. Avsluttende betraktninger eller refleksjoner

Takk for deltagelsen!