FORSVARET
Forsvarets høgskole

Samhandling i Cyberforsvaret

Har Cyberforsvarets avdelinger felles forståelse for organisasjonens oppgaver?

Silje Nythun

Masteroppgave
Forsvarets høgskole
2016

Forord

Denne studien er den avsluttende delen av masterstudiet ved Forsvarets høgskole. Forberedelsene startet høsten 2015 mens selve undersøkelsen ble gjennomført våren 2016. Det har vært et utfordrende halvår, samtidig har det vært en svært lærerik prosess.

Jeg vil rette den største takken til min veileder Hanne Eggen Røislien som villig har gitt meg råd, veiledning og tilbakemeldinger underveis. Jeg er ydmyk og takknemlig for at jeg har fått støtte av et så kunnskapsrikt menneske. Tusen takk til bibliotekarene ved Forsvarets høgskole for god service. Jeg vil takke respondentene for at dere tok dere tid og for det dere delte meg under intervjuene. Jeg vil også takke medstudenter for gode samtaler og motiverende utveksling av erfaringer i skriveprosessen. Til slutt vil jeg takke min familie for støtte og forståelse for at jeg har vært delvis fraværende det siste halve året. Nå skal jeg fokusere på noe annet enn meg selv!

Lillehammer 18. Mai 2016

Silje Nythun

Sammendrag

Cyberforsvaret er en videreføring av Forsvarets informasjonsinfrastruktur. Navneendringen og etableringen ble besluttet av Stortinget i 2012. Cyberforsvaret har en kompleks oppdragsportefølje, oppgavene spenner vidt og organisasjonen er preget av arv fra gammel organisasjonsstruktur.

Dette er en kvalitativ empirisk undersøkelse av samhandling i Cyberforsvaret. Studien vil besvare følgende spørsmål: *Har Cyberforsvarets avdelinger felles forståelse for organisasjonens oppgaver?* For å belyse problemstillingen i bredde og dybde er analysen basert på intervjuer i kombinasjon med en studie av faglitteratur og dokumenter. Utvalget består av offiserer med flere års erfaring fra Cyberforsvaret. Flertallet av respondentene har også noe av sin utdanning og bakgrunn fra Forsvarets informasjonsinfrastruktur. Dette innebærer at de besitter kunnskap og har innsikt i de endringer etableringen av Cyberforsvaret har medført.

Hovedfunnet er at Cyberforsvarets avdelinger ikke har felles forståelse for organisasjonens oppgaver. Gitt metoden og det begrensede antall respondenter kan ikke funnene generaliseres, men enkelte årsakssammenhenger er identifisert. Funnene indikerer at samhandling i Cyberforsvaret kun foregår mellom avdelinger og aktører som er gjensidig avhengig av hverandre. Dette kan årsaksforklares med det brede spekteret av oppgaver og svært ulike fagmiljøer. Organisasjonsstrukturen omtales som dysfunksjonell, kommandolinjene er ikke klare og utfordringer på nivåene over de undersøkte avdelingene preger organisasjonen. Som en konsekvens av dette er det manglende tillit til avdelingen de er underlagt. De avdelingsvise prestasjonene er en medvirkende årsak til at Cyberforsvaret i helhet løser sine oppgaver. De avdelingsvise prestasjonene er imidlertid et resultat av selvstendig oppdragsløsning, kun avhengige av enkelte andre aktører. Ansvar og myndighet er ikke tydelig avklart. Dette kan skyldes at organisasjonen fremdeles er ung og i sine formative år.

Summary

The Norwegian Armed Forces Cyber Defence is a continuation of the Armed Forces Information Infrastructure. The change of name and the establishment was decided by the Parliament in 2012. The Cyber Defence has a complex mission portfolio, their task has a wide range and the organization is characterized by heritage from an old structure.

This is a qualitative empirically investigation of interaction in the Cyber Defence. The study will answer following question: *"Have the departments in the Cyber Defence common understanding of the organizations tasks?"* To enlighten the issue broadly, the analysis is based on interviews in combination with a study of literature and documents. The selection consists of officers with several years of experience from the Cyber Defence. The majority of the respondents also have some of their education and background from the Armed Forces Information Infrastructure. This means they possess knowledge and have insight in those changes the establishment of the Cyber Defence have caused.

The main finding is that departments within the Cyber Defence not have a common understanding of the organizations tasks. Given the method and the limited number of respondents, the findings cannot be generalized, but certain causes of action are identified. The findings indicate that interaction in the Cyber Defence only takes place between departments who are equally dependent on each other. The wide range of tasks and very different academic environment can explain this. The organization structure is reviewed as dysfunctional, the lines of command are not straight and the challenges on the level above the examined departments characterize the organization. As a consequence of this, there is a lack of confidence between the levels in the organization.

Innholdsfortegnelse

1 Innledning 1
1.1 Bakgrunn for studien 1
1.2 Cyberforsvarets organisasjon og oppgaver 3
1.2.1 Cyberforsvarets kompetanse- og transformasjonsavdelig 5
1.2.2 Cyberforsvarets avdeling for cybertjenester og -operasjoner 6
1.3 Problemstilling 8
1.4 Avgrensning 9
1.5 Relevans 10
1.6 Empiri 11
1.7 Struktur 12
2 Teoretisk tilnærming og utvalg av forskningslitteratur 13
2.1 Litteraturoversikt 13
2.2 Organisasjonsteori 14
2.3 Instrumentelt perspektiv 15
2.3.1 Hierarkisk variant 18
2.3.2 Forhandlingsvariant 19
2.3.3 Samhandling 20
2.4 Faktorer 21
2.4.1 Tilhørighet 21
2.4.2 Prestasjon 22
2.4.3 Ansvar 22
3 Metode 24
3.1 Utvikling av problemstilling og valg av metode 24
3.2 Valg av undersøkelsesdesign 26
3.3 Datainnsamling og utvalgets sammensetning 30
3.4 Bearbeidelse og analyse av data 31
3.5 Validitet og reliabilitet 32
4 Presentasjon og drøfting av funn 34
4.1 Samhandling 34
4.1.2 Delkonklusjon 42
4.2 Tilhørighet 43
4.2.2 Delkonklusjon 50
4.3 Prestasjon 50
4.3.2 Delkonklusjon 56
4.4 Ansvar 57
4.4.2 Delkonklusjon 63
5 Konklusjon 65
5.1 En endelig konklusjon 65
5.2 Styrker og begrensninger ved forskningen 68
5.3 Mulige utviklingstrekk og videre forskning 69
6 Litteraturliste 70
Vedlegg A: Forkortelser 1
Vedlegg B: Informasjon om forskningsprosjekt 2
Vedlegg C: Intervjuguide 3
Vedlegg D: Samtykkeerklæring 8
Vedlegg E: Godkjenning fra NSD 9

1 Innledning

Det er skrevet mange bøker og artikler om organisasjoner, opprettelse av organisasjoner, omorganisering av organisasjoner, organisasjoners eksistensgrunnlag, offentlige og private organisasjoner, og så videre. Det er imidlertid skrevet lite om samhandling og intern enhetlig forståelse i en organisasjon, for organisasjonens oppgaver. Det er derfor relevant å se nærmere på samhandling i Cyberforsvaret da det enorme omfanget av tidligere studier, forskning og litteratur innen organisasjonsteorien ikke kan sies å ha tilstrekkelig overførbarhet.

Jeg vil i denne studien vise at samhandling forekommer mellom aktører og nivåer i Cyberforsvaret der hvor man er gjensidig avhengig av hverandre for å utføre konkrete oppgaver. Funnene i studien indikerer at forståelse for organisasjonens oppgaver i begrenset grad er felles. Dette skal jeg vise ved å analysere og drøfte empiri innsamlet i intervjuer, og se funnene i lys av organisasjonsteori.

Dette kapittelet presenterer bakgrunnen for studiens tema, og hvilken problemstilling studiet søker å besvare. Kapittelet gir et overordnet innsyn i studiens hensikt, formål, dens relevans for samtiden og den faglige og teoretiske tilnærmingen. Kapittelet vil avslutningsvis beskrive studiens struktur.

1.1 Bakgrunn for studien

Overgangen fra et tradisjonelt invasjonsforsvar til et høyteknologisk, nettverksbasert innsatsforsvar har medført en rekke endringer og omstillinger i Forsvarets innretning, organisering og oppgaver. Norges sikkerhets- og forsvarspolitikk har fått nye og mer krevende oppgaver og Forsvaret er i rask endring (Meld. St. 14, 2012-2013, s. 7). Informasjons- og kommunikasjonsteknologien (IKT) har i løpet av de siste 20 år endret samfunnet. På den ene siden bidrar IKT til økonomisk vekst, økt velferd og effektivisering av offentlig sektor. På den andre siden oppstår nye utfordringer i form av cyberkriminalitet, trusler mot personvernet og ivaretagelse av individuelle rettigheter (R. Johnsen, 2013, s. 242). For å utnytte de muligheter som ligger i den nye teknologien og for å beskytte Forsvaret, og samfunnet, mot de trusler og sårbarheter den nye teknologien innebærer besluttet Stortinget i 2012 å etablere Cyberforsvaret.

Under den offisielle etableringen av Cyberforsvaret 18.september 2012 uttalte daværende Forsvarsminister Espen Barth Eide:

> *"Cyber må betraktes som et operasjons- og trusselområde på samme måte som de tradisjonelle domene land, sjø og luft … Cyberdomenet gir Forsvaret store muligheter til å samhandle og dele informasjon i sanntid på tvers av våpengrener på måter som man bare kunne drømme om for få år siden. Dette styrker vår operative evne, men gjør oss også mer sårbare. Derfor er et godt cyberforsvar helt nødvendig for å sikre et effektivt forsvar" (Forsvarsdepartementet, 2012).*

Vi ser en dreining mot et nettverksbasert Forsvar og jeg vil i denne sammenheng fremheve Espen Bart Eides uttalelse: "…*cyberdomenet gir Forsvaret store muligheter til å samhandle og dele informasjon i sanntid"*. Jeg vil anta at for å få dette til i Forsvaret vil en forutsetning være at dette fungerer internt i Cyberforsvaret.

Forsvarets informasjonsinfrastrukturs videreføring og navneendring til Cyberforsvaret i 2012 tilsa en styrket oppmerksomhet på Forsvarets evner innen cyberområdet (Prop. 73 S, 2011-2012, s. 17). For å møte Forsvarets og samfunnets forventninger må Cyberforsvaret være organisert på en hensiktsmessig måte og strukturen må utnyttes på en god måte. I den sammenheng er det relevant å se på den interne forståelse for de oppgaver Cyberforsvaret skal løse, og om den bidrar til et godt cyberforsvar, som Espen Barth Eide sa er helt nødvendig for å sikre et effektivt forsvar. Forutsetninger for løse pålagte oppgaver kan sies å være tilstede da organisasjonen er godt utstyrt, med moderne materiell, og består av personell med bred erfaring og høy fagkompetanse. Dette vil kunne muliggjøre å nå visjonen *økt operativ evne gjennom samhandling i nettverk (Forsvarsstaben, 2016, s. 32).* Det er imidlertid ikke nødvendigvis en direkte sammenheng mellom gode forutsetninger og gode resultater. Proposisjon 73 S beskriver en relativt klar, men ikke detaljert, arbeidsfordeling mellom avdelingene i Cyberforsvaret (Prop. 73 S, 2011-2012, s. 103). Tilgjengelig ugradert kilder som Forsvarets intranett spesifiserer oppgavene noe mer. Graderte og ugraderte dokumenter synliggjør imidlertid ikke hvordan avdelingene skal samhandle for å løse pålagte oppgaver.

På bakgrunn av forhold som påpekes i McKinsey-rapporten fra 2015 er det grunn til å reise en viss tvil om Cyberforsvaret er ideelt organisert og om organisasjonsstrukturen fungerer i praksis. Rapporten ble skrevet med den hensikt å identifisere, kvantifisere og beskrive potensialet for

ytterligere modernisering og effektivisering av utvalgte forvaltningsområder og funksjoner i forsvarssektoren (McKinsey & Company, 2015, s. 7). Rapporten slår fast:

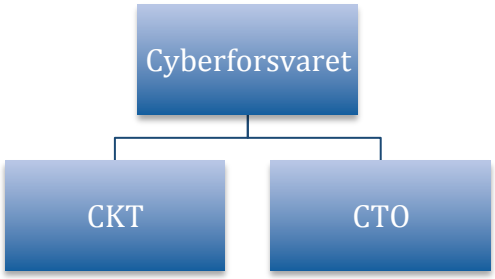
> *"IKT-virksomheten i Forsvaret leverer ikke tilfredsstillende resultater (...) Videre eksisterer det ingen omforent oversikt over alle systemene i sektoren og hvem som har ansvaret for disse. Problemene skyldes frem årsaker. For det første har sektoren valgt en uegnet organisering av IKT. Modellen bidrar til ansvarspulverisering og uløste oppgaver. Det er videre store uklarheter i ansvarsforhold og ingen unison begrepsbruk mellom funksjoner. Dette driver både duplisering av funksjoner, eksempelvis i skillet mellom forvaltning og drift, og uløste oppgaver, eksempelvis rundt brukerstyring av systemer. Det er store variasjoner i prosjektgjennomføring og viktige kompetansegap til mønsterpraksis, som blant annet driver unødvendig lang leveransetid. Investeringsprosessen er ikke operasjonalisert på en fornuftig måte, og bruken av denne er derfor for omfattende og unødvendig komplisert. Sektoren benytter en for stor grad av prosjektfinansiering, som bidrar til økt leveringstid for prosjekter" (McKinsey & Company, 2015, s. 51)*.

Dette gjelder riktignok for hele forsvarssektorens IKT-enheter, Cyberforsvaret er primært ansvarlig for etterspørselsstyring og drift. Det kan imidlertid være relevant å bruke det som fastslås i rapporten som et bakteppe for å se nærmere på hvordan Cyberforsvaret, som en av forsvarssektorens IKT-enheter, er organisert og at den totale leveransen ikke leverer tilfredsstillende resultater.

1.2 Cyberforsvarets organisasjon og oppgaver

Frem til 2012 var Forsvarets kompetansesenter for kommando og kontroll-informasjonssystemer (FK KKIS) ansvarlig for styrke- og kompetanseproduksjon, samt at de hadde ansvar for deployerbare kapasiteter. Den daglige driften av informasjonsinfrastrukturen ble ivaretatt av INI operasjoner (INI OPS). Cyberforsvaret er en videreføring av Forsvarets informasjonsinfrastruktur med stab på Jørstadmoen (Prop. 73 S, 2011-2012, s. 17). Siden opprettelsen av Cyberforsvaret har vi sett en intern omorganisering med opprettelsen av Cyberforsvarets avdeling for cybertjenester og -operasjoner (CTO), tidligere INI OPS, og Cyberforsvarets kompetanse- og transformasjonsavdelig (CKT), tidligere FK KKIS. Organisasjonen er for øvrig desentralisert og lokalisert over hele landet.

Cyberforsvaret er organisert på nivå 2 i Forsvarets militære organisasjon, på lik linje med Hæren, Luftforsvaret og Sjøforsvaret. Cyberforsvarets organisasjonsstruktur har to nivå 3 avdelinger, dette er CTO og CKT. Organisatorisk ser Cyberforsvarets slik ut på nivå 2 og 3:



Figur 1 Cyberforsvarets organisasjonsstruktur

Forsvarssjefen stiller krav til sine undergitte sjefer gjennom målbilde og oppdrag i virksomhetsplanen, resultatene følges opp helhetlig i Forsvarssjefens ledergruppe. Forsvarssjefens målbilde suppleres med målbilder ved driftsenheten på nivå 2 i Forsvaret (Forsvaret, 2015, s. 40). Målbildene skal, i tillegg til å vise egne mål, understøtte overordnet målbilde. Dette er grunnlaget for å etablere et styringshierarki i Forsvaret (Forsvarsstaben, 2010, s. 18). Cyberforsvaret har eget målbilde, dette er imidlertid kun tilgjengelig i graderte dokumenter og kan derfor ikke gjengis her.

Militære operasjoner i det digitale rom har både beskyttende, etterretningsmessige og offensive siktemål. Dette har blitt en tilleggsdimensjon ved militære operasjoner og dermed et nytt krigføringsområde hvor både evnen til defensive og offensive operasjoner vil kunne være avgjørende i fremtidige konflikter (Prop. 73 S, 2011-2012, s. 102). I Norge er ansvaret for Forsvarets cyberoperasjoner delt mellom Etterretningstjenesten og Cyberforsvaret. Defensive cyberoperasjoner i Forsvarets informasjonsinfrastruktur er underlagt sjef Cyberforsvarets myndighet. Ansvaret for alle offensive cyberoperasjoner er tillagt sjef Etterretningstjenesten. Nasjonal sikkerhetsmyndighet (NSM) har et nasjonalt koordineringsansvar for beskyttelse av informasjon og infrastruktur av betydning for samfunnskritiske og andre viktige samfunnsfunksjoner. I tillegg har NSM et nasjonalt tverrsektorielt ansvar for å identifisere, varsle og koordinere håndteringen av alvorlige cyberhendelser (Forsvarsstaben, 2014, s. 124).

Sjef Cyberforsvaret skal gi operasjonsstøtte til Forsvarets planlagte og pågående operasjoner, dette innebærer å gjennomføre defensive cyberoperasjoner. Hovedoppgaven til Cyberforsvaret er å drifte og utvikle Forsvarets samband og understøtte Forsvarets operasjoner både hjemme og ute. Organisasjonen skal understøtte nettverksbaserte operasjonsformer og bidra til vesentlig forbedringer innenfor operabilitet, fleksibilitet, reaksjonsevne, mobilitet og deployerbarhet

(Prop. 73 S, 2011-2012, s. 102). Dette innebærer å støtte den teknologiske utviklingen av Forsvaret, og implementere ny teknologi og nye konsepter innenfor sikre operative rammer. Organisasjonen skal lede utviklingen av et nettverksbasert forsvar (NbF) og konseptutviklings- og eksperimenteringsaktivitet i Forsvaret. Cyberforsvaret er leverandør av tjenester, IKT, kommando- og kontrollsystemer og kommunikasjonssystemer til Forsvarets avdelinger i inn- og utland (Forsvaret, 2016). Cyberforsvaret har ansvar for etablering, drift og beskyttelse av Forsvarets informasjonsinfrastruktur for å understøtte Forsvarets evne til å gjennomføre operasjoner (Forsvarsstaben, 2014, s. 125). Innenfor gjeldende budsjettramme skal Cyberforsvaret tilpasse organisasjonen og oppgavene i samsvar med de strukturendringer som gjøres i andre deler av Forsvaret (Prop. 73 S, 2011-2012, s. 102).

1.2.1 Cyberforsvarets kompetanse- og transformasjonsavdelig

CYFOR CKT utvikler og etablerer kommunikasjonssystemene Forsvaret trenger for å kommunisere og ha kontroll med sine styrker i et operasjonsområde. Forsvarets forsterkede innretning mot operasjoner innenfor en fellesoperativ ramme, og behov for kommando- og kontrollsystemer som virker på tvers av forsvarsgrenene er sentrale fokusområder for avdelingen (Forsvaret, 2016).

CYFOR CKT styrkestruktur og operative evne har følgende kapasiteter (Prop. 73 S, 2011-2012, s. 103):

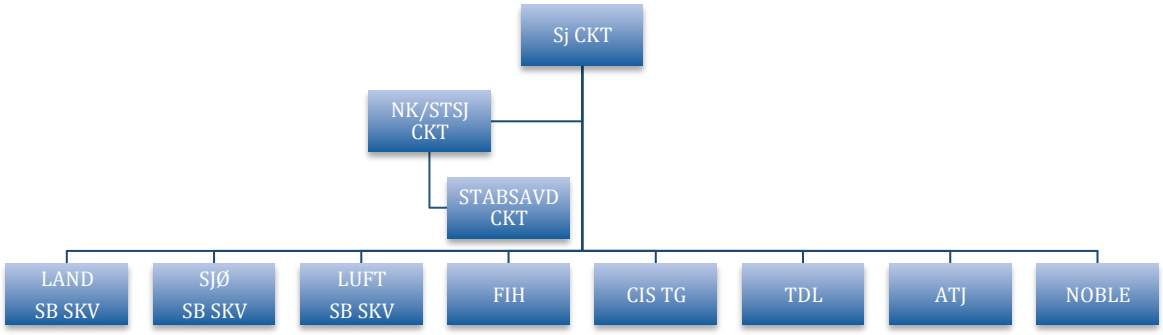
Communication Information Systems Task Group (CIS TG) er en nivå 4 avdeling i Cyberforsvaret. Avdelingen støtter norsk deltagelse i hele bredden av militære operasjoner med CIS-kapasiteter. På Forsvarets intranett beskrives CIS TGs oppgaver på en mer utfyllende måte, respondentene har også forklart hvilke oppgaver avdelingen utfører og hva dette innebærer;

CIS TG er en operativ enhet i CKT. Avdelingen støtter deployering av norske styrker nasjonalt og internasjonalt. CIS TG er Cyberforsvarets innsatsstyrke og avdelingen har kapasitet til å etablere, bemanne og drifte transportable IKT-moduler og kommandoplasser på kort varsel. Personellet utdannes og trenes daglig for å kunne være klare for oppdrag i henhold til et beredskapskrav på 30 dager. Avdelingen er en fellesstyrke med personell og kompetanse til å støtte alle forsvarsgrener. En av CIS TGs viktigste oppgaver er å gi norske soldater en ”link hjem” når de deltar i internasjonale operasjoner. Dette innebærer alt fra satellittkommunikasjon, nasjonalt strategisk samband til Forsvarets operative hovedkvarter til velferdssamband i form av

telefon og internett. Siden etableringen av CIS TG i 2005 har avdelingen blant annet løst oppdrag i Afghanistan, Afrika/Tsjad, Sverige, Kypros, Seychellene, Sicilia og Kreta.

Taktisk datalink-skvadron (TDL) er en annen nivå 4 avdeling i CKT. Avdelingen utøver kontinuerlig planlegging gjennom Joint Datalink Operation Centre ved Forsvarets operative hovedkvarter, ledelse og overvåking av Forsvarets datalink operasjoner. TDL har deployerbare elementer og yter taktisk datalink-tjenester i samsvar med hovedkvarterets behov.

CYFOR CKT består i tillegg av flere underenheter lokalisert flere steder i landet, avdelingen ser organisatorisk slik ut:



Figur 2 CKT organisasjonskart (Hentet fra Forsvarets intranett)

1.2.2 Cyberforsvarets avdeling for cybertjenester og -operasjoner

CYFOR CTOs fremste oppgaver er tjenesteleveranser, drift og forsvar av Forsvarets IKT-systemer, samt å levere sensor- og radardata til operative miljøer. Avdelingen er også ansvarlig for teknisk drift og videreutvikling av Forsvarets integrerte forvaltningssystem (FIF). Avdelingen bidrar til samfunnssikkerhet gjennom overvåking og informasjonsinnhenting, og ved å levere infrastruktur og virksomhetskritiske tjenester til sentrale deler av statsforvaltningen (Forsvaret, 2016).

CYFOR CTO styrkestruktur og operativ evne har følgende kapasiteter (Prop. 73 S, 2011-2012, s. 103):

Avdeling for beskyttelse av kritisk infrastruktur (BKI) er en nivå 4 avdeling i CTO. Avdelingen bidrar til å beskytte Forsvarets infrastruktur gjennom støtte til analyse av sårbarheter, ondsinnet kode og angrep mot Forsvarets systemer. Avdelingen har deployerbare elementer og mulighet til

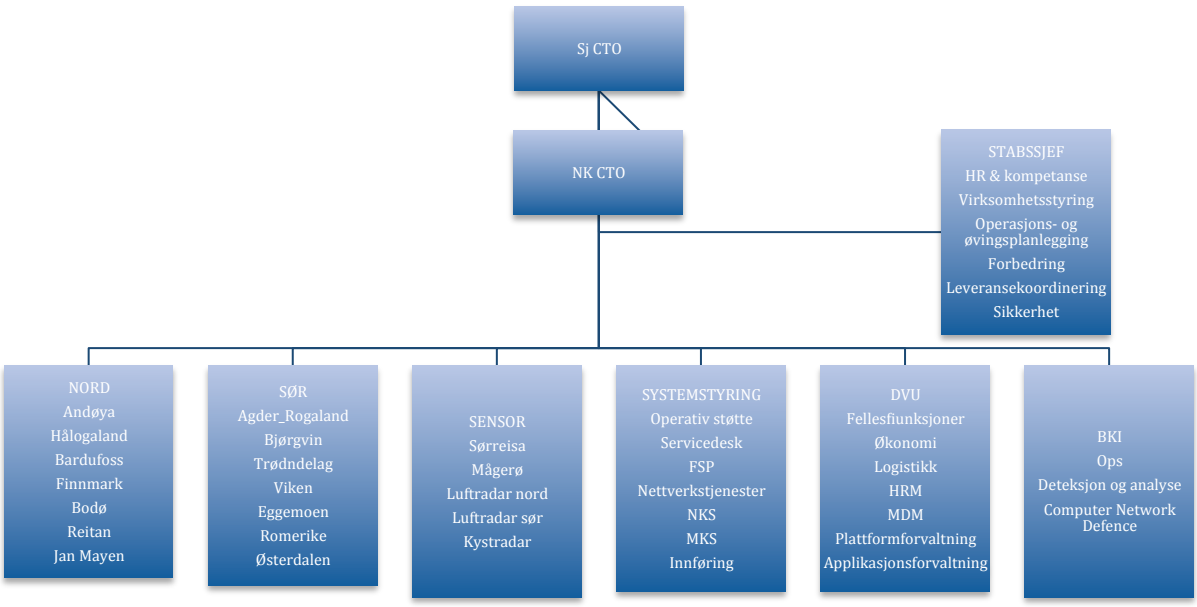
å bistå med rådgivning og liasonering ved håndtering av trusler og angrep mot norsk infrastruktur ute og hjemme. Respondentene og Forsvarets intranett beskriver avdelingens oppgaver slik; BKI er Forsvarets primære kapasitet innen overvåking av datatrafikk i Forsvarets informasjonssystemer. Avdelingen er i tillegg ansvarlig for å utøve Computer Network Defence (CND) for Forsvaret, de skal støtte Forsvarets avdelinger med operasjonssikkerhetsvurderinger for deres kommandoplasser og informasjonssystemer (OPSEC) og de skal operere Forsvarets alarmsentral (FAS)

Forsvarets satellittkapasiteter – Forsvarets satellittstasjon Eggemoen etablerer informasjonsbærere i hele bredden av nasjonale og utenlandske militære operasjoner tilpasset operative behov og krav. Stasjonær kommunikasjonsinfrastruktur leverer et bredt spekter av tjenester til alle Forsvarets avdelinger, i tillegg til vitale brukere i samfunnet for øvrig.

Avdeling for sensor – samler inn data til bruk for beslutningstakere på alle nivåer i Forsvaret, for sivile myndigheter og NATO.

Kontrollsentre – Forsvarets nettkontrollsenter og Forsvarets meldingskontrollsenter – er ansvarlig for overvåking og kontroll av henholdsvis Forsvarets kommunikasjonsinfrastruktur og Forsvarets meldingssystemer på døgnkontinuerlig basis.

CYFOR CTO består i tillegg av flere underavdelinger lokalisert flere steder i landet, organisatorisk ser avdelingen slik ut;



Figur 3 CTO organisasjonskart (hentet fra Forsvarets intranett)

1.3 Problemstilling

Innenfor en organisasjon vil det over tid feste seg bestemte tenkemåter, verdier, oppfatninger og holdninger. Dette innebærer hvordan ulike ting gjøres og også måter å snakke og kommunisere på. I en sterk organisasjonskultur vil slike kulturelle uttrykk prege adferden og være tydelige for de ansatte. I dette kan det ligge en betydelig styrke, det vil gjøre det lettere å kommunisere og samarbeide. En sterk organisasjonskultur kan også gjøre det vanskeligere å få til forandring, med mindre evnen til forandring blir en del av kulturen (Knudsen & Flåten, 2015, s. 71).

Flere kryssende interesser møtes når gammel organisasjonsstruktur skal gå sammen om å bli noe nytt. Felles for interessene bør imidlertid samhandling stå sentralt for at organisasjonen skal løse oppgavene med et så godt resultat som mulig.

På tidspunktet for Espen Barth Eides uttalelser i 2012 var Cyberforsvaret en ny organisasjon med oppgaver i et forholdsvis nytt domene (Prop. 73 S, 2011-2012, s. 11, 146). Til tross for etableringen av en ny organisasjon, var den tuftet på arv fra gammel organisasjonsstruktur. En av intensjonene med etableringen av Cyberforsvaret var å styrke Forsvarets operative evne. Cyberforsvaret ble ansett som nødvendig for å sikre et effektivt forsvar. Utviklingen innen cyberområdet ble sett på som en tilleggsdimensjon ved militære operasjoner. Navneendringen skulle reflektere Forsvarets styrkede evne til å ivareta dette området (Prop. 73 S, 2011-2012, s. 102). På tidspunktet for utgivelsen av McKinsey-rapporten hadde organisasjonen eksistert i nesten tre år. Rapporten kan sies å indikere at Cyberforsvaret som en av Forsvarets fire rendyrkede IKT-enheter, ikke leverer tilfredsstillende resultater da *"IKT-virksomheten i Forsvaret leverer ikke tilfredsstillende resultater…"* (McKinsey & Company, 2015, s. 51-52). Innebærer dette at Cyberforsvaret fortsatt holder fast ved oppgavene de utførte før organisasjonen ble etablert? Eller har Cyberforsvaret evnet å tilpasse seg det nye domenet og slik sett styrket Forsvarets operative evne og sikret et mer effektivt forsvar? Svarene på disse spørsmålene kan ha betydning for Cyberforsvarets utførelse av oppgaver og hvordan organisasjonen løser oppgavene i det nye operasjons- og trusselområde (Prop. 73 S, 2011-2012, s. 102-103).

Basert på bakgrunnen for studien formuleres problemstillingen på følgende måte:

Har Cyberforsvarets avdelinger felles forståelse for organisasjonens oppgaver?

For å besvare problemstillingen er det nødvendig å tilnærme seg den fra et teoretisk og praktisk utgangspunkt. Jeg vil ta utgangspunkt i deler av organisasjonsteorien for å sette Cyberforsvarets organisasjonsstruktur og oppgaver i vitenskapelig kontekst. Valgt teoretisk retning anvendes for å kunne analysere empirien i lys av samfunnsvitenskapelig forskning. Ingen teori innen offentlig organisasjonsteori kan sies å være universell eller så representativ at det hersker bred enighet om at den er gjeldende på alle områder. Som teori for den empiriske analysen har jeg valgt det instrumentelle perspektivet i organisasjonsteorien. I lys av teorien og samhandlings-begrepet vil problemstillingen kunne betraktes, og anvendes som et redskap for å avgrense hva som er relevant for å kunne besvare problemstillingen. To av Cyberforsvarets avdelinger benyttes som en casestudie i denne studien. Avdelingene er valgt av flere grunner. For det første kan de sies å representere bredde i Cyberforsvarets oppdragsportefølje da de kan ses på som ytterpunkter med tanke på fagområder. For det andre representerer de spisskompetanse og leverer nisjeprodukter. For det tredje tilhører de hver sin nivå 3 avdeling.

Det vil være av stor betydning å avdekke respondentenes oppfattelse og synspunkter innen studiens faktorer for å besvare problemstillingen. Dette vil det kunne være vanskelig å få frem gjennom bruk av andre metoder enn intervju. Metoden jeg har valgt for å undersøke dette er en kvalitativ tilnærming. Metoden er hensiktsmessig fordi det tidligere ikke er forsket på dette i Cyberforsvaret. Kvalitativ tilnærming har som utgangspunkt at virkeligheten er for kompleks til å reduseres til tall, og at man derfor må samle inn informasjon i form av ord som åpner for mer nyanserikdom (Jacobsen, 2015, s. 24). Den valgte metoden har også svakheter; de svar jeg får under intervjuene vil kunne være påvirket av sted, tid og rom – de kan sies å være kontekstuelt tidsavhengig. Jeg vil trolig ikke kunne tegne et bilde, men forhåpentligvis vil jeg kunne identifisere årsakssammenhenger.

1.4 Avgrensning

Espen Barth Eides sa under den offisielle etableringen av Cyberforsvaret at et godt cyberforsvar er helt avgjørende for å sikre et effektivt forsvar. Denne studien vil ikke fokusere på hvorvidt opprettelsen av Cyberforsvaret har bidratt til å sikre et mer effektivt forsvar. Uttalelsen har uansett relevans for studien da den er med på å sette opprettelsen av organisasjonen i en større kontekst.

Cyberforsvaret har ulike komplekse oppgaver og samarbeider med aktører internt i Forsvaret og eksternt. Det være seg eksempelvis Etterretningstjenesten og Nasjonal Sikkerhetsmyndighet. Denne oppgaven har ikke til hensikt å se på om de ulike interne og eksterne aktørene har felles forståelse for de oppgaver som skal løses i fellesskap og hvor aktørene er gjensidig avhengige av hverandre. Studien avgrenses til å kun se på interne forhold i Cyberforsvarets. Selv om studien avgrenses til Cyberforsvaret er det ikke mulig å vurdere alle forhold ved samhandling innenfor rammene til studien. For å innhente empiri avgrenses undersøkelsen til å se på to nivå 4 avdelinger, dette er CIST TG og BKI. Denne avgrensningen er gjort med bakgrunn i de to underavdelingenes oppgaver og tilhørighet i organisasjonen. CIS TG og BKI er operative avdelinger som hver for seg leverer nisjeprodukter i form av oppgaver som beskrevet i kapittel 1.2. Avdelingens ulike fagområder kan dermed sies å representere bredde i form av ytterpunkter i Cyberforsvarets komplekse oppdragsportefølje. Hensikten med denne avgrensningen er å innhente empiri som kan analyseres for å besvare problemstillingen.

Oppgavens tittel og problemstilling kan klart sees i lys av ulike teoretiske retninger. Jeg har valgt å ta utgangspunkt i organisasjonsteori. Innen organisasjonsteori vil flere retninger kunne anvendes. Jeg velger å avgrense til å se problemstillingen i lys av et instrumentelt perspektiv da Cyberforsvaret har en hierarkisk organisasjonsstruktur. Et element i denne studien vil være organisasjonskulturen i Cyberforsvaret. Kulturbegrepet er imidlertid så komplekst at jeg velger å ikke la det få en stor plass det i teoridelen, ei heller som et stort fokusområde i empirien. Dette begrunnes med en antagelse om begrenset kjennskap til kultur som fenomen, utover forventet allmennkunnskap om begrepet blant personellet som skal intervjues. Det vil være opp til respondentene hva de legger i forståelsen av kultur. Den individuelle tolkningen og forståelsen av kulturbegrepet vil likefremt berøres i analysedelen.

1.5 Relevans

Utredningens relevans for samtiden har flere sider. Jeg vil hevde at å undersøke om Cyberforsvaret, som er en forholdvis ny organisasjon tuftet på arv fra gammel organisasjonsstruktur har bidratt til et godt Cyberforsvar, eller ikke, kan ha overføringsverdi med tanke på ekstern gyldighet. Funnene kan også være relevante for andre virksomheter. Videre vil jeg hevde at å undersøke om Cyberforsvarets avdelinger har felles forståelse for organisasjonens oppgaver implisitt vil kunne belyse om Cyberforsvaret bidrar til å sikre et mer effektivt forsvar.

Det er som tidligere nevnt ikke et mål for denne studien å finne ut av dette, men funnene i studien vil kunne ha en form for ekstern gyldighet for Forsvaret.

Sist, men ikke minst er det en intensjon at studien bidrar til å øke kunnskap og bevissthet internt i Cyberforsvaret om organisasjonsstruktur og betydningen av felles forståelse for oppgaver.

Cyberforsvarets eksistensgrunnlag er nedfelt i Stortingsproposisjon 73 S hvor det fastslås å videreføre Forsvarets informasjonsinfrastruktur med navneendring til Cyberforsvaret (Prop. 73 S, 2011-2012, s. 17). Videre beskrives angrep i det digitale rom som en av dagens raskest voksende trusler. Forsvarssektoren skal derfor utvikle sin evne til å møte disse truslene (Prop. 73 S, 2011-2012, s. 11-12). Et konkret resultat av å ha identifisert truslene og håndtere de kan være etableringen av Cyberforsvaret. Dermed kan jeg hevde at problemstillingen har vitenskapelig og praktisk relevans. Vitenskapelig på den måten at studien vil kunne bidra til å belyse hvorvidt det er samhandling i Cyberforsvaret og om avdelingene har felles forståelse for organisasjonens oppgaver. Og praktisk fordi den vil kunne øke intern bevissthet omkring hvorvidt organisasjonen arbeider mot felles mål.

1.6 Empiri

Utredningen baserer seg på et casestudie av Cyberforsvaret. Det er hovedsakelig nyttet to former for kvalitativ metode. Det er dokumentstudier og semi-strukturerte intervjuer. De kvalitative intervjuene ble gjennomført i CIS TG og BKI. De gjennomførte intervjuene ble foretatt på ledelsesnivå i avdelingene og respondentene representerer intern avdelingsvis forståelse. Respondentene hadde alle flere års erfaringer fra stillinger i Cyberforsvaret og flertallet også fra tidligere avdelinger som nå er en del av Cyberforsvaret. Bakgrunnen for å velge respondenter på ledelsesnivå i de to avdelingene var å få et så dypt og kvalifisert grunnlag i analysegrunnlaget som mulig. Dette alene vil kunne medføre mindre grad av bredde i analysegrunnlaget. For å kunne styrke studiens validitet er valgte avdelinger og respondenter gjort med bakgrunn i avdelingenes oppgaver. CIST TG og BKI representerer avdelinger som begge har operative oppgaver og i så måte vil respondentene kunne uttale seg relevant med tanke på oppgavens problemstilling og forskningsspørsmål.

Resultatet av den kvalitative tilnærmingen er drøftet i lys av valgt teori og dokumentstudier.

1.7 Struktur

Studien er bygget opp av tre hoveddeler og består av fem kapitler.

Den første delen presenterer valgt teoretiske retning basert på relevant litteratur som er funnet hensiktsmessig i lys av problemstillingen. Denne delen fokuserer først og fremst på, og er ment å belyse, hvordan Cyberforsvarets organisasjonsstruktur kan påvirke organisasjonens felles forståelse for oppgaver. Videre tar den for seg relevante begreper som er av betydning for å besvare forskningsspørsmålene og problemstillingen.

Den andre hoveddelen av utredningen forklarer den metodiske tilnærmingen i studien. Kapittel tre går i dybden på hvorfor den metodiske tilnærmingen er valgt, og hvordan forskningen har blitt gjennomført.

Den tredje hoveddelen er kapittel fire som presenterer de empiriske funnene som er gjort på bakgrunn av den metodiske tilnærmingen. Videre analyseres og drøftes de empiriske funnene i lys av den teoretiske tilnærmingen. Kapittelet vurderer altså om det er samhandling i Cyberforsvaret, og om avdelingene har felles forståelse for organisasjonens oppgaver.

Til slutt presenteres en endelig konklusjon i kapittel fem. Her blir besvarelsen av problemstillingen sett i sammenheng med relevant forskningslitteratur presentert i kapittel to. Videre vurderes styrker og svakheter ved forskningen i dette studiet, og om resultatet har implikasjoner for fremtidig forskning.

2 Teoretisk tilnærming og utvalg av forskningslitteratur

Dette kapittelet vil innledningsvis presentere litteratur som har stått sentralt i studien. Jeg vil så gi en generell kort introduksjon av formelle offentlige organisasjoner. Hensikten er å etablere en forståelse for de grunnleggende tankene om en formell organisasjon. Deretter vil det bli redegjort for valgt teori, med teoretiske forventninger og antagelser tilknyttet studiens problemstilling og forskningsspørsmål. Forventningene og antagelsene vil senere prøves mot empirien i analysedelen. Dette vil gjøre studien valid og reliabel. Avslutningsvis vil kapittelet se på relevante begreper i sammenheng med valgt teoretisk retning, og definere hva som legges til grunn i faktorene tilhørighet, ansvar og prestasjon.

2.1 Litteraturoversikt

Det er ikke gjennomført forskning innen felles forståelse for organisasjonens oppgaver i Cyberforsvaret. Det tilsier begrenset tilgang på litteratur og empiri som kan knyttes direkte til problemstillingen. En organisasjonsteoretisk tilnærming til problemformuleringen åpner imidlertid for omfattende tilgjengelig teoretisk litteratur. Mye av denne teorien omhandler direkte eller indirekte studiens tema. For å beskrive og analysere relevante områder innen denne studiens tema vil jeg benytte etablert teori og etablerte teoretiske begreper.

Sentralt i denne studien har blant annet Tom Christensen, Morten Egeberg, Per Lægreid, Paul G. Roness og Kjell Arne Røviks bok *Organisasjonsteori for offentlig sektor* stått. Teorien som presenteres baseres på empiri fra norsk offentlig sektor og er faglig tilknyttet statsvitenskap. Bokens forankring er en faglige tradisjon som kombinerer organisasjonsteori, demokratiteori og studiet av beslutningsadferd i formelle organisasjoner (Christensen, Egeberg, Lægreid, Roness, & Røvik, 2015). Boken har stått sentralt av flere årsaker; det har vært nødvendig å tilegne seg kunnskap om organisasjonsteori generelt for å kunne anvende utvalgte deler av den, siden boken gir en grundig innføring har den bevisstgjort meg hva jeg har måttet se videre på og jeg har spesielt brukt kapittelet 2; Det instrumentelle perspektivet.

Jeg har også benyttet Ulla Eriksson-Zetterquist, Thomas Kalling, Alexander Styhre og Kristin Wolls bok *Organisasjonsteori*, som presenterer organisasjonsteoriens utvikling fra en skandinavisk synsvinkel (Eriksson-Zetterquist, Kalling, Styhre, & Woll, 2014).

Kjell Arne Røvik har forsket på moderne organisasjoner, hvordan de bør ledes og være utformet for å fungere, være effektive og tidsriktige. Boken *Trender og translasjoner; ideer som former det 21. århundrets organisasjoner* har gitt meg innsikt i idéstrømmer som setter sitt preg på utformingen av vår tids organisasjoner (Røvik, 2007).

For å definere samhandling har jeg tatt utgangspunkt i Glenn-Egil Torgersen og Trygve J. Steiros bok *Ledelse, samhandling og opplæring i fleksible organisasjoner*. Bokens hensikt er å gi teoretisk og handlingsorientert innsikt i hva som skal til for å lykkes med fleksibel organisering i et kompetansebasert multikulturelt samfunn i stadig endring (Torgersen & Steiro, 2009).

Disse bøkene har klart en generell innfallsvinkel og favner ulike typer organisasjoner. Til tross for at bøkene favner bredt har de stått sentralt i denne studien nettopp for å kunne se på konkrete fenomener i lys av en teoretisk innfallsvinkel. Siden det ikke tidligere er forsket på denne oppgavens problemstilling innebærer det et skille mellom valgt litteratur og denne studiens tilnærming. Litteraturen hjelper meg å sette studien i en større kontekst. Forskningen er spisset, den ser på utvalgte faktorer og har få respondenter hvor hensikten er å gå i dybden for å kunne indikere om Cyberforsvarets avdelinger har felles forståelse for organisasjonens oppgaver. Det som hovedsakelig kan sies å skille anvendt litteratur fra min tilnærming er at organisasjonsteorien favner bredt mens studien kun ser på enkelte forhold i en forholdsvis ung organisasjon. Det er også benyttet flere andre bøker som omhandler organisasjonsteori, oppslagsverk på internett og Forsvarets intranett, og artikler.

I tillegg har litteratur om metode stått sentralt. Studien har hovedsakelig lagt tre metodebøker til grunn. Dette er Dag Ingvar Jacobsens bok *Hvordan gjennomføre undersøkelser?*, John W. Creswells bok *Research Design Qualitative, Quantitative, and Mixed Methods Approaches* og Kristen Ringdals bok *Enhet og mangfold.* Bøkene beskriver og eksemplifiserer hvordan ulike undersøkelser kan gjennomføres og har blitt anvendt som en form for rammeverk for denne studien.

Det er tidligere skrevet oppgaver som omhandler Cyberforsvaret, men temaene i disse er ikke relevant for denne studien.

2.2 Organisasjonsteori

Organisasjonsteori er en betegnelse på et sett med begreper og teorier som i samfunnsvitenskapen brukes til å beskrive, forklare og gi råd om organisasjonsatferd (Berg,

2014). På slutten av 1800-tallet og begynnelsen av 1900-tallet startet man å systematisere og sammenfatte hvordan foretak skulle administreres og ledes (Eriksson-Zetterquist et al., 2014, s. 46). Henry Townee, som var et innflytelsesrikt styremedlem i American Socicty of Mechanical Engineers (AMSE) argumenterte i et intervju i Engineering Magazine i april 1916 at ”management” og ”organization” måtte utvikles til en vitenskap (Røvik, 2007, s. 77). Dette var altså organisasjonshistoriens første fase, og man kan si at teorien ble utviklet i den hensikt å gjøre foretak og organisasjoner bedre. Frem til midten av 1900-tallet ble den brukt til å se ingeniørfaget og det var nesten utelukkende ingeniørutdannelse som ga adgang til å kunne forske innen den nye vitenskapen om organisasjonsteori. Senere ble organisasjonsteorien et mer selvstendig fagområdet hvor man, i tillegg til ingeniørfaget, også hentet inspirasjon fra andre disipliner som sosiologi og statsvitenskap. Det ble stadig tydeligere at organisasjonsteoriens utfordring og hensikt var å avdekke regelmessigheter ved hjelp av en vitenskapelig tilnærming. Tydeligheten om hensikten, og den vitenskapelige ambisjonen bidro til økt anseelse og legitimitet omkring organisasjonsteoriens disiplin innenfor samfunnsvitenskapen (Røvik, 2007, s. 78-79).

En offentlig organisasjons eksistensgrunnlag kan sies å være at den skal utføre oppgaver på vegne av samfunnet. Det som kjennetegner en formell organisasjon er blant annet at den er opprettet for å ivareta kollektive interesser og oppgaver. Relativt stabile adferdsmønstre, ressurser og belønninger er etablert knyttet til den aktiviteten de utfører (Christensen et al., 2015, s. 21). En formell organisasjonsstruktur er en struktur som består av posisjoner og regler for hvem som bør eller skal gjøre hva, og hvordan de ulike oppgavene bør eller skal utføres. Organisasjoner er en systematisering av et sett av posisjoner og underenheter. Organisasjonene kan selv inngå i større enheter og organisasjonsenhetene kan være delt opp og samhandle på ulike måter. Hvordan arbeid og oppgaver fordeles tyder på et syn på organisasjoner som heterogene, med koalisjoner som har ulike mål eller interesser og ulike ressurser for interessehevding. De enkelt underenhetene og deres medlemmer kan handle formålsrasjonelt, men resultatet vil også avhenge av hva andre gjør og hvilke ressurser de har (Christensen et al., 2015, s. 35-36).

2.3 Instrumentelt perspektiv

Det instrumentelle perspektivet kan sies å ha sitt utspring fra en modernistisk organisasjonsforståelse, hvor man har en vitenskapelig tilnærming til organisasjoner (Røvik,

2007, s. 33-34). Gjennom forskning eller erfaring kan man identifisere ulike mekanismer som kan fremstå som lovmessigheter, disse ligger til grunn for utforming og utvikling av organisasjoner. Teoretikere innen det instrumentelle perspektivet understreker målspesifisering og formalisering som sentralt. Ideelt sett er et instrumentelt system basert på mål som politikere formulerer. Målene er ofte utviklet nedenfra i forvaltningsapparatet, det kan være aktivitetsmål og resultatindikatorer. Når disse målene utformes av politikere kan de få et mer teknisk preg enn idealet skulle tilsi (Christensen, Lægreid, Roness, & Røvik, 2009, s. 111). Hvordan Cyberforsvaret utformer sine mål kan betraktes på tilsvarende måte. Målspesifisering og formalisering kan sees på som viktige bidrag til rasjonalitet av organisatoriske tiltak.

Organisasjonene kan sees på redskaper eller instrumenter for å nå mål som må oppfylles. Politiske og administrative ledere kan som følge av sin hierarkiske posisjon prege beslutningsprosessene, og utforme og endre det offentlige organisasjonsapparatet (Christensen & Lægreid, 2006, s. 18). Lederne forventes å gjøre konsekvenslogiske vurderinger av alternativer eller virkemidler, i formålsrasjonelle handlinger, for å velge det alternativet som medfører at organisasjonen kan utføre sine oppgaver på en best mulig måte (Christensen et al., 2009, s. 33). Kjell Arne Røvik beskriver at den rasjonalistiske logikken skiller organisasjoner fra andre typer samhandling mellom mennesker, det være seg mellom familier eller etniske grupper (Røvik, 2007, s. 72).

Formell organisasjonsstruktur er et sentralt element i instrumentell teori. Formelle normer kan være nedfelt i organisasjonskart, reglementer og stillingsinstrukser. De spesifiserer prosedyrer og fremgangsmåter, hvilket ansvar, rettigheter og plikter som tillegges ulike enheter og stillinger (Christensen et al., 2015, s. 27). Den formelle organisasjonsstrukturen kan blant annet innebære at begrensinger i rasjonaliteten kan bli noe redusert på organisasjonsnivå i forhold til på individnivå. Hvem som skal gjøre hva i utføring av oppgaver, er fastlagt gjennom hvilke formelle roller eller posisjoner det enkelte organisasjonsmedlem har. Det vil også være fastlagt av hvilken underenhet den er tilknyttet og hvilken større enhet organisasjonen inngår i (Christensen et al., 2015, s. 38-39). Konkrete mål og en sterk formalisering vil klargjøre handlingsalternativer og gjør organisasjonen uavhengig av bestemte individer. Som definisjonskarakteristikker er den rasjonelle organisasjonen en formell struktur utformet med den hensikt å styre sine aktører på bakgrunn av rasjonell kalkulasjon hvor informasjon, effektivitet, optimalisering, implementering og design er tatt høyde for (Scott & Davis, 2003, s. 36).

Forfatterne sier videre at dette innebærer individuelle kognitive og motiverende begrensninger vedrørende valg og handlinger i organisasjonen.

Når en rasjonell organisasjon kjennetegnes ved mål- og redskapsfokusering innebærer det at organisasjoner ikke har noen verdi i seg selv utover det å være redskaper konstruert for så effektiv måloppnåelse som mulig. Rasjonelt lederskap innebærer at organisasjoner sees på som systemer hvor ledelsen utgjør et rasjonelt autorativt sentrum. Det vil si at ledelsen kombinerer kyndighet med myndighet. De besitter dyp innsikt i virksomhetens mål og har bred oversikt over tilgjengelige virkemidler og mulige konsekvenser av disse. De må også ha makt og vilje til å gjøre nødvendige endringer i organisasjonen for at den skal være optimalt tilpasset for å nå mål (Røvik, 2007, s. 72).

Innenfor det instrumentelle perspektivet er vektingen mellom alternativer og konsekvenser et sentralt element. Dette innebærer en mål-middel forståelse, et samsvar mellom handling og det organisasjonen ønsker å oppnå. For at en organisasjon skal nå sine mål må den gjennomføre konkrete handlinger. Handlingene er et resultat av valg mellom ulike alternativer av handlinger. Beslutningsregler vil binde valgene og dette bygger på om man ønsker en maksimal- eller tilfredsstillende måloppnåelse. Begrepet fullstendig formålsrasjonalitet anvendes om maksimal eller størst grad av måloppnåelse. Dette innebærer at organisasjonen har full oversikt over handlingsalternativene, mulige konsekvenser av de ulike valgene og en klar målsetning. Basert på denne innsikten kan man utforme beslutningsregler som vil gi maksimal måloppnåelse. Flere empiriske studier av hvordan organisasjoner handler viser imidlertid at dette i liten grad er realistisk. Dette er spesielt tydelig i komplekse offentlige organisasjoner hvor mange hensyn skal tas. I slike tilfeller operer organisasjoner i komplekse miljøer hvor alternativene og konsekvensene ikke er like synlige og veien til målet ikke er like klar. Organisasjonen baserer seg da på beslutningsregler som medfører god nok måloppnåelse, om dette anvendes begrepet begrenset rasjonalitet (Christensen et al., 2015, s. 36-37).

Man kan skille mellom to varianter av det instrumentelle perspektivet, dette er en hierarkisk variant og en forhandlingsvariant. Skillet mellom de to variantene kan blant annet sees på i forhold til grad av homogenitet hos ledelsen. I en hierarkisk variant ser man ledelsen som homogen, med kontroll over reformprosesser og med evne til rasjonell kalkulasjon. I en forhandlingsvariant ser man ledelsen som mer heterogen hvor ulik organisasjonstenkning,

forhandlinger og kompromisser står sentralt i en reformprosess (Christensen & Lægreid, 2006, s. 10-11).

2.3.1 Hierarkisk variant

I en hierarkisk variant ser man på organisasjonen som enhetlig og ledelsen som homogen. Kunnskap om mål-middel-sammenhenger vektlegges hos ledelsen i organisasjonen eller hos de organisasjonen er et redskap for (Christensen et al., 2015, s. 35). Organisasjonsformen er preget av hierarki, arbeidsdeling og rutiner. De formelle normene for hvem som skal eller kan gjøre hva i en hierarkisk variant kan være nedfelt i organisasjonskart, stillingsinstrukser, regler og lover. Rollene eller posisjonen i en organisasjon er avgjørende for hvem som skal eller kan gjøre hva i en formell organisasjonsstruktur. Forventningene til de som innehar rollene eller posisjonene er upersonlige, og normene for hva som skal gjøres er dermed uavhengig av de personene som innehar posisjonene. Det er også av betydning hvilken underenhet de er tilknyttet og hvilken større enhet organisasjonen inngår i. Dette innebærer at ulike oppgaver blir tillagt ulike nivåer i organisasjonen (Christensen et al., 2015, s. 38).

2.3.1.1 Forventninger og antagelser ut fra en hierarkisk variant

Fokus i en hierarkisk instrumentell variant ligger på den formelle organisasjonsstrukturen. Cyberforsvaret ledelse forventes, som følge av sine hierarkisk posisjon, å ha kontroll over de oppgaver organisasjonen skal løse. På samme måte forventes det at nivå 3 og nivå 4 i organisasjonen også har kontroll på oppgavene de ulike nivåene skal løse. Det forventes at ledelsen legger føringer og fordeler oppdrag nedover i organisasjonen, at de besitter dyp innsikt i virksomhetenes mål og at de har god oversikt over tilgjengelige virkemidler og mulige konsekvenser av disse. Det forventes også at ledelsen har makt og vilje til å gjøre nødvendige endringer i organisasjonen for at den skal være optimalt tilpasset for å nå de mål Cyberforsvaret skal. Ut fra en hierarkisk variant tar studien utgangspunkt i to antagelser til Cyberforsvarets organisasjon:

1) Cyberforsvarets ledelse kontrollerer organisasjonene oppgaver.

Cyberforsvaret ble opprettet i 2012 og organisasjonen har siden gjennomført enkelte omorganiseringer. Det antas at ledelsen har et bevisst forhold til egne kapasiteter, muligheter og begrensninger, at de følger en mål-middel tankegang og at de utviser vilje og evne til å gjøre organisatoriske endringer dersom det er nødvendig for bedre måloppnåelse. Dette innebærer at CTO og CKT utfører pålagte oppgaver i henhold til Cyberforsvarets målbilde.

2) CTO og CKT samhandler for å løse organisasjonens oppgaver.

Nivå 3 avdelingene antas å ha kunnskap og innsikt i tilgjengelige kapasiteter, internt og på tvers av avdelingene, og anvender egne avdelinger som instrumenter eller redskaper for å løse organisasjonens oppgaver. Tildeling av oppdrag og ressurser styres i stor grad av organisasjonen nivå 4 avdelingene er underenheter i. Dette innebærer at nivå 3 følger en mål-middel tankegang og søker å oppnå bestemte målsettinger. Organisasjonsstrukturen kan sådan betegnes som homogen.

2.3.2 Forhandlingsvariant

I en forhandlingsvariant ser man på organisasjonen som sammensatt av ulike underenheter og posisjoner som kan ha delvis motstridende mål, interesser og kunnskaper. Organisasjoner sees på som koalisjoner hvor hver av aktørene handler formålsrasjonelt på grunnlag av organisasjonens egeninteresse. Utfallet av måloppnåelse og ivaretagelse av interesser vil være påvirket av forhandlinger og kompromisser mellom flere aktører. Dette skyldes at ingen aktør på egenhånd kan oppnå sine mål og ivareta sine interesser (Christensen et al., 2015, s. 35). Det er stor grad av heterogenitet i interesser og målsetninger, avdelingene har ulik struktur, ulike roller og ulike funksjoner. Aktørene er på det samme hierarkiske nivå og er likeverdige spillere (Christensen & Lægreid, 2006, s. 11-12). I forhandlingsvarianten står man overfor mange aktører og organisasjonen er preget av konflikter, maktkamp og politikk. Beslutninger fattes blant grupperinger med delvis motstridende mål og interesser og aktørene er begrenset rasjonelle. Endringer i organisasjonen er et resultat av interessehevding eller kjøpslåing. Utfallet av de politiske kampene og denne kjøpslåingen avhenger av de ressursene hver aktør har for å fremme egne interesser. Organisasjonsendring er dermed et resultat av forhandlinger og tautrekking mellom aktører med ulik organisasjonsplassering. (Christensen et al., 2015, s. 45-46). I forhandlingsvarianten kan beslutninger fattes på ulike måter. For det første kan en dominerende koalisjon få gjennomslag for sine mål og interesser. For det andre kan ulike aktører forhandle seg frem til kompromisser. For det tredje kan det foretas sekvensiell løsning av konflikter hvor motstridende mål tas opp etter tur og slik sett unngår å bli konfrontert med hverandre (Christensen et al., 2009, s. 44).

2.3.2.1 Forventninger og antagelser ut fra forhandlingsvarianten

Ut fra en forhandlingsvariant kan man forvente at de ulike aktørene i Cyberforsvaret har delvis motstridene mål, interesser og kunnskaper. I dette legger jeg at de ulike aktørenes oppgaver spenner vidt, og kompleksiteten i Cyberforsvarets oppdragsportefølje innebærer ulike

motstridende mål og interesser. Det forventes at organisasjonen er preget av heterogenitet. Ut fra forhandlingsvarianten tar studien utgangspunkt i to antagelser:

1) Cyberforsvarets ledelse kontrollerer i mindre grad organisasjonenes oppgaver.

Det antas at omorganiseringer som er gjennomført siden opprettelsen av Cyberforsvaret er gjort i den hensikt å styrke de ulike avdelingenes posisjoner. Dette innebærer at ledelsen i mindre grad har innflytelse på oppdrag. Det forventes at CTO og CKT arbeider selvstendig og at de i mindre grad er avhengig av hverandre for å løse organisasjonens oppgaver.

2) CTO og CKT samhandler i mindre grad for å løse organisasjonens oppgaver.

Nivå 3 avdelingene antas i mindre grad å ha kunnskap og innsikt i tilgjengelige kapasiteter, spesielt på tvers av delingene. Forholdet mellom avdelingene preges av konkurranse. Dette gjenspeiler de ulike aktørenes interesser og maktforholdet mellom avdelingene. Heterogenitet i organisasjon medfører liten grad av samhandling mellom nivå 3 og 4 avdelingene.

Når problemstillingen drøftes i lys av det instrumentelt perspektivet antas følgende: Etableringen har innebåret stor grad av arv fra gammel organisasjonsstruktur, oppdragsporteføljen er kompleks og Cyberforsvaret preges av å være en desentralisert organisasjon. I motsetning til i en sentralisert organisasjon vil det i en desentralisert organisasjon forventes at beslutningene vil være overlatt til lavere nivå. På hvilket nivå beslutningene tas vil kunne prege organisasjonen (Christensen et al., 2015, s. 42). Det vil derfor være relevant å se på Cyberforsvarets organisasjonsstruktur og om den har konsekvenser for organisasjonens forståelse av oppgavene. Det vil også være relevant å se på i hvilken grad Cyberforsvarets ledelse har et bevisst forhold til organisasjonenes oppgaver, og hvordan dette formidles nedover i organisasjonen.

2.3.3 Samhandling

Torgersen og Steiro innleder sitt kapittel om samhandling i boken *Ledelse, samhandling og opplæring i fleksible organisasjoner* med en rekke synonymer til ordet samhandling. Ulike begreper brukes for å beskrive de samme prosesser. Eksempler på dette er samarbeid, samspill, koordinering, samordning og samvirke (Torgersen & Steiro, 2009, s. 128). En tydeliggjøring av begrepet er derfor hensiktsmessig i denne studien gitt oppgavens tittel og besvarelsen av problemstillingen. Torgersen og Steiro's definisjon av samhandling legges til grunn:

> *"Samhandling er en åpen og likeverdig kommunikasjons- og utviklingsprosess mellom aktører som kompetansemessig utfyller hverandre og utveksler kompetanse, dirkete ansikt-til-ansikt eller mediert via teknologi eller med håndkraft, som arbeider mot felles mål ,og hvor forholdet mellom aktørene til enhver tid hviler på tillit, involvering, rasjonalitet og bransjekunnskap" (Torgersen & Steiro, 2009, s. 153).*

Studiens utgangspunkt er at å samhandle er å gjøre noe sammen. I en organisasjon innebærer det å samarbeide mot et felles mål, eller i alle fall en illusjon om at man har noe til felles (Folgerø, 2000, s. 12).

Cyberforsvarets ambisjon er økt operativ evne gjennom samhandling i nettverk (Forsvarsstaben, 2016, s. 32). Cyberforsvaret skal understøtte nettverksbaserte operasjonsformer og bidra til vesentlig forbedringer innenfor operabilitet, fleksibilitet, reaksjonsevne, mobilitet og deployerbarhet. Nettverksbasert forsvar er en konseptualisering av nettverkstenkningen. Det handler om å utvikle både mennesker, organisasjon og teknologi med et mål om å organisere ressursene mest mulig effektivt for å oppnå en størst mulig effekt av de ressursene som settes inn gjennom systemintegrasjon, situasjonsbevissthet og forståelse av sjefens intensjon (Forsvarsstaben, 2014, s. 224-225). En nettverksbasert tilnærming til militære operasjoner forutsetter at datasystemene fungerer under så vel planlegging og forflytning av styrkene som under stridshandlinger. En forutsetning for situasjonsforståelse, ledelse av operasjoner og styring av våpensystemer vil være evne til kontinuerlig informasjonsutveksling. De norske cyberstyrkenes mest grunnleggende oppgave blir derfor å etablere en fleksibel og robust informasjonsinfrastruktur til støtte for land-, sjø- og luftstridskreftene (R. Johnsen, 2013, s. 247). Det er altså en samhandling i nettverk med den hensikt å bruke Forsvarets ressurser på måter som utnytter de mulighetene tilgjengelig informasjonen gir. Cyberforsvaret er en viktig aktør med tanke på hva et nettverk av plattformer vil kunne yte i forhold til hva kun en enkelt plattform vil kunne yte.

2.4 Faktorer

2.4.1 Tilhørighet

Tilhørighet er et begrep som brukes om ulike fenomener eller tilstander i ulike situasjoner. Bjørn Helge Johnsen beskriver i boken *Operativ Psykologi* at tilhørighet bygger på faktorer som

samhold og identitet (B. H. Johnsen, 2005, s. 302). Denne studiens anvendelse av begrepet tilhørighet legger til grunn to varianter med tilnærmet lik betydning. Den ene omhandler tilhørighet innad i de ulike avdelingene, den andre omhandler tilhørighet i Cyberforsvaret som organisasjon. Det vil være av betydning å avdekke begge variantene av tilhørighet for å besvare problemstillingen. Avdelingstilhørighet antas å være av betydning for hvordan avdelingen presterer og yter. Dette vil imidlertid ikke ha direkte følger for hvorvidt Cyberforsvarets avdelinger har felles forståelse for organisasjonens oppgaver eller ikke. Men om vi definerer Cyberforsvaret som avdelingen vil det kunne ha forklaringskraft. Avdelingstilhørighet i denne studien vurderes som tilhørighet mellom en person og en organisasjon. Studien var i utgangspunktet ikke ment å fokusere på tilhørighet mellom personer da det kan sies å helle mot avdelingsfølelse. Det viser seg imidlertid at tilhørighet, eller manglende tilhørighet mellom personer er et gjennomgående tema i intervjuene. Da dette ser ut til å innvirkning på besvarelsen av problemstillingen finner jeg det nødvendig å analysere og drøfte disse funnene.

2.4.2 Prestasjon

Til grunn i faktoren prestasjon legges ytelse og det som fører frem til gode resultater. I store norske leksikon beskrives prestasjon som ytelse og det som er fullført (Gundersen, 2009). En antagelse er at fokus på arbeidsoppgavene som regel gir best resultat, dette innebærer tydelige mål, hardt arbeid og stor disiplin. Det vil være relevant å avdekke om dette fokuset er gjeldende innad i de ulike avdelingene, og om det er gjeldende på tvers av avdelingene. I denne studien vil jeg ta utgangspunkt i at det avdelingene gjør er avdelingenes prestasjoner. Det er imidlertid ikke nødvendigvis samsvar mellom innsats og resultat. Og en avdelings innsats, ytelse og fullførte oppgaver har i denne sammenheng ikke nødvendigvis direkte sammenheng med organisasjonens totale innsats, ytelse og fullførte oppgaver. Her vil det være nødvendig å finne ut av om felles forståelse for organisasjonenes oppgaver påvirker de avdelingsvise prestasjonene, og dermed Cyberforsvarets prestasjoner.

2.4.3 Ansvar

Ansvar kan forstås på ulike måter. Det kan være ansvarlig overfor ulike instanser, politisk ansvar, administrativt ansvar, profesjonelt ansvar, sosialt ansvar eller legalt ansvar. Eller det kan være et spørsmål om hvem som er ansvarlig, om det er et individuelt ansvar eller om det er et kollektivt ansvar. Ansvar kan også omhandle hva man er ansvarlig for, det kan være resultater, prosesser, prosedyrer eller ytelser. I boken ”Organisasjonsteori for offentlig sektor” skilles det

mellom formelt hierarkisk ansvar og et mer uformelt sosialt ansvar (Christensen et al., 2015, s. 136). En tradisjonell forståelse for ansvar tilsier at ledere har et relativt altomfattende ansvar, med det utgangspunkt at ledere handler på basis av tillit. I et slikt tilfelle vil forvaltningen av tilliten være kjernen, innenfor et formelt system av over- og underordning. En instrumentell og administrativ forståelse av ansvar vil bære preg av å være mer formell og snever. Den som tildeles et formelt ansvar må redegjøre og rapportere for hvordan ansvaret forvaltes (Christensen et al., 2015, s. 136-137). Med dette som bakteppe vil denne studien anvende begrepet ansvar om det ansvar Cyberforsvaret har tildelt den enkelte avdeling og posisjon. Implisitt i dette ansvaret legges også myndighet. Med myndighet forstås den enkelte avdelings område hvor de har beslutningsmyndighet. Dette innebærer myndighet til å fatte beslutninger uten å avklare disse med overordnet i forkant. Studien vil se på hvordan fordeling av ansvar og myndighet er formalisert og praktiseres.

3 Metode

Metode er de teknikker som anvendes for å tilegne seg kunnskap om virkeligheten (Jacobsen, 2015, s. 23). En metode vil fungere best i en situasjon, mens en annen metode vil fungere bedre i en annen situasjon. Det er altså knyttet ulike styrker og svakheter til både det kvalitative og det kvantitative, den ene forskningsmetoden kan ikke sies å være bedre enn den andre. Kunsten er å finne den metode som passer best til den konkrete problemstillingen.

Dette kapittelet vil presentere de metodiske tilnærmingene og vurderingene som er lagt til grunn i studien. Først vil kapittelet omhandle utvikling av problemstilling og argumenter for valg av metode. Deretter redegjøres det for valg av undersøkelsesdesign. Datainnsamling og utvalgets sammensetning og metoden for bearbeidelse og analyse av data presenteres under delkapittel 3.3 og 3.4. Kapittelet avsluttes med vurderinger knyttet til validitet og reliabilitet.

3.1 Utvikling av problemstilling og valg av metode

Jeg har jobbet i Hæren, i Luftforsvaret, i FK KKIS og i Cyberforsvaret. Med dette har jeg gjort meg noen erfaringer fra ulike organisasjoner i Forsvaret, og hvordan organisasjonenes interne samhandling innvirker på de oppgaver som skal løses. Dette har skapt interesse for hvordan opprettelsen av en ny organisasjon, tuftet på arv fra gammel organisasjonsstruktur, innvirker på den daglige driften.

Oppgavens problemstilling kan sies å være motivert av egne erfaringer og forståelse av Cyberforsvaret. Utviklingen av problemstillingen er et resultat av tre forhold.

For det første en antagelse om at samhandling i Cyberforsvaret kan være en utfordring da kompleksiteten i oppdragsporteføljen og organisasjonsstrukturen kan gjøre det utfordrende å skape en felles organisasjonskultur. Cyberforsvaret er en fellesavdeling sammensatt av personell fra Hæren, Luftforsvaret og Sjøforsvaret, dette innebærer at de har ulik bakgrunn, utdanning og tjenesteerfaring. Samtidig har en stor andel av Cyberforsvaret personell sin bakgrunn fra Hærens samband og de utgjør dermed en del av arven som jeg har beskrevet tidligere. Dette innebærer at Cyberforsvaret personell kan sies å representere mangfold. Denne antagelsen omhandler tilhørighet og har til hensikt å avdekke hvorvidt det er samhandling mellom Cyberforsvarets avdelinger, og på hvilken måte og hvilke områder de samhandler. For det andre antar jeg at prestasjoner avhenger av at organisasjonsmedlemmene har en felles forståelse for

organisasjonens oppgaver. Hensikten her er å avdekke hvilke forhold som påvirker om avdelingene har forståelse for egne og andres oppgaver, eller ikke. Og for det tredje en antagelse om at en organisasjon med et bredt spekter av oppgaver vil kunne medføre utfordringer med tanke på fordeling, og praktisering av ansvar og myndighet. Her er det sentrale å avdekke hvilke forhold som påvirker ansvar og myndighet.

Jeg vil i denne oppgaven se nærmere på om Cyberforsvarets avdelinger evner å se hele organisasjonens oppgaver som et felles anliggende, eller om de er ensidig opptatt av egne operative oppgaver og utfordringer. I den sammenheng vil det være relevant å se på om etableringen av Cyberforsvaret har medført en sterk organisasjonskultur og et godt cyberforsvar. Med denne antagelsen står hypotese 1 sentralt:

Cyberforsvarets organisasjonsstruktur tilsier ikke at samhandling mellom avdelingene er nødvendig.

Eller om det er slik at organisasjonskulturen er stiavhengig[1] fra hvordan Forsvarets informasjonsinfrastruktur var organisert før og dermed er så sterk at den har vanskeliggjort forandring. Dette gjør hypotese 2 gjeldende:

En organisasjon tuftet på arv fra gammel organisasjonsstruktur vil ha utfordringer med å etablere en god organisasjonskultur i organisasjonens begynnende og formative år.

Jeg vil undersøke hvordan avdelingene sameksisterer og samhandler med hverandre, ledere og ansatte i den hierarkiske linjeorganisasjonen. I denne studien vil sameksistens og samhandling stå sentralt med tanke på det som forsøkes besvares.

For å teste hypotesene er tre forskningsspørsmål utledet for å besvare problemstillingen:

Forskningsspørsmål 1 refererer til hypotese 1 og omhandler faktoren tilhørighet:

1. Er det gjensidig avhengighet mellom avdelingene i Cyberforsvaret?

Forskningsspørsmål 2 refererer til hypotese 2 og omhandler faktoren prestasjon:

2. Har avdelingene forståelse av at de drar i samme retning?

Forskningsspørsmål 3 referer til hypotese 1 og 2 og omhandler faktoren ansvar:

3. Hvordan forstår avdelingene Cyberforsvarets målbilde?

[1] I boken *Organisasjonsteori for offentlig sektor* beskrives stiavhengighet som; de kulturelle normene og verdiene som preger en organisasjon i dens begynnende og formative år vil ha stor betydning for de utviklingsveiene den følger siden.

På bakgrunn av dette er den overordnede tittelen på denne studien:

Samhandling i Cyberforsvaret

og med hypotesene som utgangspunkt er følgende problemstilling utledet:

Har Cyberforsvaret avdelinger felles forståelse for organisasjonens oppgaver?

3.2 Valg av undersøkelsesdesign

Vitenskapelig metode er ikke et entydig begrep. Innenfor ulike vitenskapsdisipliner vil metoden variere. Et naturlig skille går mellom naturvitenskap og samfunnsvitenskap. Naturvitenskap handler om forskning av konkrete og ikke-mentale fenomener i den hensikt å avdekke lovmessigheter. Samfunnsvitenskap handler om studier av mentale fenomener og hvordan disse kommer til uttrykk i sosial kontekst (Malnes, 2012, s. 92). Med denne beskrivelsen hjelper Espen Barth Eides uttalelser under etableringen av Cyberforsvaret oss å plassere studien i kategorien samfunnsvitenskap.

Problemstillingen i denne oppgaven er uklar. Uklar på den måten at det i Cyberforsvaret er lite forhåndskunnskaper om det som skal undersøkes. For å kunne besvare problemstillingen beror valget av metodisk tilnærming på hvilken metode som er best egnet til å belyse problemstillingen. God samfunnsforskning er problemorientert og ikke metodeorientert i den forstand at den anvender de metoder, som med hensyn til en gitt problematikk, best kan besvare de relevante forskningsspørsmålene (Flyvbjerg, 2006, s. 242). Problemstillingen bærer preg av å være et åpent spørsmål og den kan derfor sies å være utforskende. Dermed er det nødvendig med et eksplorerende undersøkelsesopplegg for å oppnå mer kunnskap og klarhet. Dag Ingvar Jacobsen beskriver at eksplorerende problemstillingers første og fremste hensikt er å (Jacobsen, 2015, s. 80):

a) avdekke ny kunnskap om et fenomen ved å
b) finne ut hva fenomenet består av, dvs. konkretisere innholdet i fenomenet (variabler og verdier), for å
c) utvikle en teori om fenomenet som kan munne ut i
d) et sett hypoteser som kan testes.

For å innhente empiri i bredde og dybde vil en kombinasjon av kvantitativ og kvalitativ metode kunne være fordelaktig. Bent Flyvbjerg skriver i sin artikkel Five Misunderstandings About Case-Study Research: *"Good social science is opposed to an Either/or and stand for a both/and on the question of qualitative versus quantitative methods"* (Flyvbjerg, 2006, s. 242). Gitt denne oppgavens problemstilling er det imidlertid ikke sikkert at en kvantitativ tilnærming ville kunne bidratt ytterligere for å besvare problemstilling. I dette legger jeg at respondentene i en omfattende kvantitativ undersøkelse ikke nødvendigvis vil inneha tilstrekkelig kompetanse om det denne studien er ute etter å belyse. For å besvare forskningsspørsmålet vil det være nødvendig at respondentene innehar detaljert kunnskap om, og innsikt i Cyberforsvarets oppgaver på taktisk og operasjonelt nivå. Det er også hensiktsmessig at de innehar en viss strategisk forståelse for Cyberforsvarets oppgaver. Studiens begrensning i tid og omfang gjør det nødvendig å velge den metoden jeg mener egner seg best for å besvare problemstillingen. Jeg har derfor valgt en kvalitativ metode. Undersøkelsen er gjennomført ved studere relevante dokumenter og tekster, og ved å intervjue sentrale aktører på ledelsesnivå i to av Cyberforsvarets nivå 4 avdelinger. En kvalitativ tilnærming med semi-strukturerte dybdeintervju i kombinasjon med analyse av tilgjengelig ugradert kildemateriale er dermed grunnlaget for denne undersøkelsen.

Det er flere fordeler knyttet til kvalitative data. Det å samle inn data i form av ord vil kunne bety at forskeren går inn i en relativt naturlig relasjon med den eller de som undersøkes. Dette vil kunne innebære en form for nærhet som kan bidra til at den som undersøkes setter egne ord på sine oppfatninger. Ved å anvende semi-strukturerte intervjuer vil jeg kunne oppnå åpenhet rundt det det spørres om, intervjuobjektet står fritt til å snakke om det vedkommende mener er sentralt og graden av relevans vil dermed kunne bli høy. Det vil være de som undersøkes som i stor grad definerer hva som er den "korrekte" forståelsen (Jacobsen, 2015, s. 129).

Kvalitativ tilnærming har også ulemper. Det å samle inn kvalitative data er ressurskrevende og tar gjerne lang tid. Dette innebærer at jeg må nøye meg med få respondenter i denne undersøkelsen. Få respondenter kan medføre problemer med representativitet og den eksterne gyldigheten vil dermed kunne bli mindre god. I tillegg vil informasjonen kunne være vanskelig å tolke da nyanserikdommen i det som sies muligens er kompleks (Jacobsen, 2015, s. 131-132).

Manglende kunnskap om problemstillingen før man skal gjennomføre en undersøkelse gjør det utfordrende å formulere hensiktsmessige spørsmål. Det vil kunne være vanskelig å vite hvordan man skal utforme spørsmålene når man ikke vet hva man skal spørre om. Et fleksibelt

undersøkelsesopplegg er derfor nødvendig (Jacobsen, 2015, s. 133). For å besvare problemstillingen står forskningsspørsmålene sentralt i den empiriske analysen.

Hensikten med denne utforskende studien er å finne frem til om og hvordan samhandling oppstår eller forekommer, og om avdelingene har felles forståelse for organisasjonenes oppgave. Dette skal jeg gjøre ved å stille åpne spørsmål som åpner for nyanserikdom. Jacobsen mener utforskende studier er godt egent dersom man ønsker å avklare forståelsen av et forhold, men er usikker på hva den nøyaktige utfordringen eller problemet er (Jacobsen, 2015, s. 79-80).

Det er mange måter å gjennomføre en utforskende studie på, det kan for eksempel basere seg på litteratursøk og dokumentstudier, ansikt-til-ansikt intervju, telefonintervju, e-mail intervju, observasjoner eller audiovisuelt materiale (Creswell, 2014, s. 190-191). Dersom man benytter seg av intervjuer, vil de i en utforskende studie fordre åpenhet og bære preg av å være forholdsvis ustrukturert. Dette begrunnes med at man ønsker at intervjuobjektet skal belyse temaet for studien fra sitt ståsted. En kvalitativ tilnærming kan dermed sies å ha høy grad av relevans da man legger få føringer på den informasjonen man får inn. Respondenten står selv fritt til å formidle sine fortolkninger, og dette åpner for nyanserikdom, variasjon og kompleksitet. Det generelle fanges i mindre grad opp i en utforskende studie. Utforskende studier kan være fleksible og tilpasningsdyktige, underveis i forskningen vil ny kunnskap kunne fremkomme og man har da muligheten til å endre problemstilling og innsamlingsmetode underveis (Jacobsen, 2015, s. 129-130). Denne studien er utforskende og søker ny kunnskap på bakgrunn av ulike forhold som belyst i kapittel 1. Kapittelet reiser en viss tvil om Cyberforsvarets avdelinger har felles forståelse for organisasjonens oppgaver. Jeg antyder utfordringer ved organisasjonsstrukturen, men er usikker på om dette er et problem som påvirker forståelsen, og om en felles forståelse er av betydning for resultatet av oppgavene som skal løses. Dette innebærer at forskningsspørsmålene må fremstilles relativt åpne i den hensikt å øke forståelsen av det konkrete problemet.

Ved utvikling av undersøkelsesdesignet er det viktig å ha et bevisst forhold hva man skal undersøke. Dette henger sammen med hvilken type tilnærming man skal ha i studien. Ulike former for tilnærming er induktiv, deduktiv og abduktiv. Dersom man nytter en induktiv tilnærming vil konklusjonen hovedsakelig fremkomme på bakgrunn av de observasjonene som er gjort i studien. En induktiv studie vil ha teori eller en modell som sluttprodukt (Creswell, 2014, s. 65-66). Denne studien vil basere seg på empiriske data, innsamlet ved intervju,

sammenlignet med et teoretisk grunnlag for å kunne besvare problemstillingen. Det teoretiske utgangspunktet vil ikke bli testet og verifisert eller falsifisert. De empiriske dataene vil anvendes for å komme frem til en teori om Cyberforsvarets avdelinger har en felles forståelse for organisasjonens oppgaver. Dette innebærer at denne studien har en induktiv tilnærming.

Det finnes ulike måter å gjennomføre en casestudie på. En metode vil kunne være å studere en enkeltcase, formålet vil da være å forstå casen i seg selv eller å avdekke kausale mekanismer. En annen metode er sammenlignende casestudier. Hensikten er da å sammenligne to eller flere caser for å kunne avdekke årsakssammenhenger. En sammenlignede casestudie vil kunne øke muligheten for å generalisere (Jacobsen, 2015, s. 102-105). I følge Yin (2012) skiller man mellom fire forskjellig casestudier i to forskjellige varianter.

Den første varianten skiller mellom single-case designs og mulitple-case designs (Yin, 2012, s. 7-8). Enkelt caser vil ha et utforskende preg, hvor man leter etter noe nytt eller forsøker å forstå noe man anser som overraskende eller uforståelig (Jacobsen, 2015, s. 99). Multiple caser brukes dersom hensikten er å sammenligne funn på tvers av forskjellige caser (Yin, 2012, s. 8).

Denne studien vil anvende Cyberforsvaret som enkelt case studie med bakgrunn i empiri fra to av organisasjonenes avdelinger. Hensikten er å avdekke kausale mekanismer og å forstå casen i seg selv (Jacobsen, 2015, s. 102-105). Som jeg tidligere har beskrevet i kapittel 1.5 vil jeg hevde at å undersøke om Cyberforsvarets avdelinger har felles forståelse for organisasjonens oppgaver implisitt vil kunne belyse om Cyberforsvaret bidrar til å sikre et mer effektivt forsvar. Det er ikke et mål for denne studien å finne ut av dette, men funnene i studien vil kunne ha en form for ekstern gyldighet for Forsvaret. Jeg må se Cyberforsvaret i kontekst av Forsvaret og kunne sammenlignet Cyberforsvaret med Luftforsvaret, Sjøforsvaret eller Hæren og dermed muligens økt kvaliteten på studien. Gitt studiens begrensning i tid og omfang tilsier det at jeg må velge en metode som kan føre frem til relevante funn. Valget på enkeltcase-studie finner jeg hensiktsmessig da det tidligere ikke er forsket på denne studiens tematikk i Cyberforsvaret, og metoden vil kunne avdekke forhold for å besvare problemstillingen. Videre har jeg vist til at Cyberforsvaret er en forholdvis ny organisasjon som er tuftet på arv fra gammel organisasjonsstruktur. Hvorvidt denne stiavhengigheten har bidratt til et godt Cyberforsvar eller ikke kan ha overføringsverdi med tanke på ekstern gyldighet. En sammenligning av flere caser vil fordre et bredere empiriske grunnlag. Enkeltcase-studier egner seg til å utvikle ny forståelse og vil være hensiktsmessig i denne studien (Jacobsen, 2015, s. 99).

Sist, men ikke minst kan studiet bidrar til å øke kunnskap og bevissthet internt i Cyberforsvaret om betydningen av felles forståelse for oppgaver.

Den andre varianten skiller mellom holistiske studier som tar for seg organisasjonen, eller konteksten for casen, som helhet og integrerte casestudier. Integrerte casestudier tar for seg logisk utvalgte deler av organisasjonen og ser på disse med større grad av detaljnivå (Yin, 2012, s. 7-8). Et slikt casestudie har en induktiv logikk og vil kunne munne ut i en teoretisk konklusjon (Ringdal, 2013, s. 178). Jeg anser dette casestudiet som integrert da det vil se på to av Cyberforsvarets avdelinger for å komme frem til funn som kan gi svar på problemstillingen. Denne tilnærmingen finner jeg hensiktsmessig da avdelingene vurderes å kunne representere organisasjonen. Studiet søker å gå i dybden på hvordan avdelingene ser på egne oppgaver og om forståelsen for organisasjonens oppgaver er felles. Med studiens begrensning i tid og omfang er det nødvendig å gjøre dette utvalget, og intensjonen er at funnene vil gi tilstrekkelig dybde og kvalitet uten å studere flere avdelinger i Cyberforsvaret. Denne begrensningen innebærer også at studiet er et tverrsnittstudie. Et tverrsnittstudie innebærer at man studerer virkeligheten på kun ett tidspunkt og man kan i liten grad si noe om endring over tid (Jacobsen, 2015, s. 108-109). En annen variant er langtidsperspektivstudier eller tidsseriestudier. Denne varianten innebærer et undersøkelsesopplegg hvor man måler tilstanden på flere tidspunkter. Denne studien belyser med andre ord hvordan forholdene er i dag, og konklusjonen vil kunne medvirke til eventuell fremtidig justering i organisasjonen for å få den utviklingen organisasjonen ønsker.

3.3 Datainnsamling og utvalgets sammensetning

Gitt problemstillingen vil alle Cyberforsvarets avdelinger kunne være aktuelle å intervjue, det er imidlertid ikke mulig i denne studien. Det har derfor vært nødvendig å avgrense til å se på enkelte avdelinger. De svar jeg får fra intervjuobjektene vil være av betydning for problemstillingen (Jacobsen, 2015, s. 179-180).

Jeg har valgt intervjuobjekter som tjenestegjør i to av Cyberforsvarets tre operative avdelinger. For å unngå skjevhet i utvalget er avdelingene valgt da de er underavdelinger i Cyberforsvarets to nivå 3 avdelinger. Intervjuobjektene sees på som respondenter da de er representanter for de avdelingene jeg undersøker (Jacobsen, 2015, s. 178). Formålet med undersøkelsen har vært av betydning for hvem jeg har intervjuet. Utvalget er basert på en kombinasjon av utvalgskriterier for å ivareta bredde og variasjon, og at respondentene skal kunne gi mye og god informasjon

(Jacobsen, 2015, s. 181). Respondentene ses på som informanter med kunnskap og erfaring jeg ønsker innsikt i (Ringdal, 2013, s. 242).

Det kan være nødvendig å innhente tillatelse for å gjennomføre kvalitative intervjuer i en formell organisasjon (Repstad, 2004, s. 33-34). Jeg kontaktet sjef BKI og sjef CIS TG pr telefon og informerte de om studien, studiens hensikt og spurte om tillatelse til å gjennomføre intervjuer i avdelingene, begge stilte seg positive.[2] Videre tok jeg kontakt med aktuelle respondenter pr telefon og spurte om de var villige til å la seg intervjue. Av syv aktuelle intervjuobjekter sa seks seg villig.[3] Det ble avtalt tid og sted for de ulike intervjuene og jeg fulgte opp med mail, som en mer formell henvendelse, med forespørsel om å delta i forskningsprosjektet. I forkant av intervjuene sendte jeg mail med detaljert informasjon.[4] I tillegg til intervjuene har andre informanter bidratt med informasjon i form av avklarende tilleggsopplysninger i møter og i telefonsamtaler.

Kunnskap om Cyberforsvaret og de oppgaver organisasjonen skal løse er høyst sannsynlig tilstede flere steder i Forsvaret. Det er imidlertid kun internt i organisasjonen jeg vil kunne finne kunnskap, erfaring og opplevelser omkring avdelingens forståelse av oppgavene, og svar på om denne er felles i organisasjonen.

3.4 Bearbeidelse og analyse av data

I denne studien vil intervjuene være av essensiell betydning for tolkning og analyse. Den mest komplette formen for registering av data vil være ved å bruke både båndopptager og transkribering av intervjuene. Umiddelbart etter at intervjuene var ferdige startet jeg transkriberingen. Samtlige intervjuer er transkribert, dette har vært svært tidkrevende og samtidig nyttig for å kunne analysere data jeg har hentet inn (Jacobsen, 2015, s. 200-202). Jeg ble godt kjent med datamaterialet og dette la grunnlag for analysen. Transkripsjonene av intervjuene er gjennomsnittlig på 12 maskinskrevne sider. I alt utgjør datamateriale 69 tettskrevne sider. I tillegg til lydfilene tok jeg enkelte notater under intervjuene. Notatene var til hjelp under fortolkningen av innhentet informasjon. Når alle intervjuene og transkripsjonene var gjennomført startet jeg analysearbeidet. Jeg benyttet et Excel-ark for å strukturere informasjonen fra alle respondentene i ulike kolonner. Kolonnene var organisert med bakgrunn i

[2] Telefonsamtale med sjef BKI og sjef CIS TG 29.02.2016
[3] Respondentene er anonymisert av hensyn til åpenheten i intervjuene, jeg kan kontaktes dersom komiteen ønsker informasjon.
[4] Vedlagt i mail til intervjuobjektene var intervjuguiden (vedlegg A) og samtykkeerklæring (vedlegg B)

forskningsspørsmålene og faktorene, og ble gitt fargekoder. I transkripsjonene markerte jeg de sitatene jeg har anvendt i analysen med fargekoder som samsvarte med fargekodene i Excel-arket. På denne måten holdt jeg oversikt over hvilke intervjuer jeg hentet hva fra. Kildehenvisninger til meninger, påstander og informasjon som fremkommer i analysen er referert til ved bruk av fotnoter.

3.5 Validitet og reliabilitet

Førforståelse, respondentutvalg, datainnsamling og bearbeidelse av data er alle faktorer som kan påvirke undersøkelsens validitet. Undersøkelsen er en metode å samle inn empiri på, og den bør tilfredsstille to krav:

1) Valid: empirien må være gyldig og relevant.
2) Reliabel: empirien må være pålitelig og troverdig.

Validiteten i denne oppgaven bygger på at jeg har brukt dokumentstudie av tekster og dokumenter som er tilgjengelig for andre. Der hvor jeg har brukt dokumentstudie av tekster eller dokumenter fra Forsvarets interne datasystem har jeg gjort dette i henhold til Sikkerhetsloven. Videre bygger validiteten i denne studien på innsamling av data i form av intervjuer. Ved gjennomføring av intervju har det vært viktig å ha et bevisst forhold til å måle det jeg ønsker å måle. Det forutsetter at jeg gjennom mine spørsmål lykkes med å få frem valide og fyldige beskrivelser fra intervjuobjektene. Tradisjonelt sett kan man si at man har større tiltro til kilder som er nær det fenomenet som beskrives (Jacobsen, 2015, s. 230). Respondentene i denne studien er, som beskrevet i kapittel 3.3, ansatte på ledelsesnivå i nivå 4 avdelinger i Cyberforsvaret. Dette kan sies å innebære nærhet til Cyberforsvarets oppgaver da det er nivå 4 avdelinger som i stor grad utfører disse. Samtidig kan det innebære at respondentene kommer lenger bort fra fenomenet da det er nivåene over som fordeler oppdrag og oppgaver. Jo lengre bort fra fenomenet respondentene beveger seg jo mer må de basere seg på det de blir fortalt. Dette kan medføre at informasjonen jeg får i intervjuene ikke kommer fra en førstehåndskilde og dermed er farget av det de har blitt fortalt (Jacobsen, 2015, s. 230). Jeg har intervjuet seks respondenter. Antallet intervjuobjekter vil ikke være tilstrekkelig for å kunne generalisere konklusjonen slik at den kan sies å være representativ for hele Cyberforsvaret. De seks respondentenes uttalelser kan imidlertid indikere avdelingsvis forståelse av organisasjonens oppgaver. Dermed kan jeg indikere årsakssammenhenger.

Jacobsen skiller mellom to typer validitet, dette er intern og ekstern gyldighet. Den interne gyldigheten omhandler hvorvidt det er dekning for konklusjonene i dataene som legges til grunn for analysen. Den eksterne gyldigheten omhandler hvorvidt resultatene er gyldige i andre sammenhenger også, om et funn kan generaliseres til å gjelde i andre sammenhenger (Jacobsen, 2015, s. 17).

Med reliabilitet menes hvor pålitelig forskningen er. Høy reliabilitet skal sikre data en pålitelighet som gjør de egnet til å belyse en vitenskapelig problemstilling Med pålitelighet og troverdighet menes at undersøkelsen må være til å stole på (Jacobsen, 2015, s. 17).
Det er ikke en ambisjon at resultatene av undersøkelsen skal være overførbare til andre områder eller organisasjoner. En kvalitativ tilnærming kan ha problemer med den eksterne gyldigheten (Jacobsen, 2015, s. 131).

Ved å beskrive de metodiske tilnærmingene og hvordan undersøkelsen skal gjennomføres i dette kapittelet har jeg gjort denne studien etterprøvbar. Dette vil kunne gi svar på om arbeidet er utført med nødvendig pålitelighet og troverdighet (Den nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora, 2005, s. 26)

4 Presentasjon og drøfting av funn

Dette kapittelet presenterer og analyserer de empiriske funnene som er gjort på bakgrunn av den metodiske tilnærmingen. Funnene fra de semi-strukturerte intervjuene og dokumentstudien presenteres og drøftes i samme rekkefølge som faktorene er presentert i kapittel to, og i samme rekkefølge som intervjuguiden er bygget opp. Kapittelets struktur har dermed sitt utgangspunkt i denne studiens tittel, faktorene og forskningsspørsmålene. Analysen tar altså sikte på å sammenligne det som har fremkommet av forskningsspørsmålene med problemstillingen. Dette danner grunnlag for tolkningene som ender opp i konklusjonen i kapittel 5.

Man kan forvente at å spille på lag i Cyberforsvaret vil være hensiktsmessig med tanke på måloppnåelse. Denne studien viser derimot at organisasjonen kanskje i mindre grad er dette bevisst. Den samhandlingen som foregår ser ut til å være basert på omstendigheter som faglig gjensidig avhengighet og tilfeldigheter som bekjentskap mellom individer i ulike avdelinger. Kapittel 4.1, 4.2, 4.3 og 4.4 vil drøfte forholdet mellom samhandling, faktorene og forståelse for organisasjonens oppgaver. I delkapitlene drøftes variasjoner av samhandling mellom, og på tvers av nivåene og variasjoner av samhandling mellom personell i ulike posisjoner. Innledningsvis i delkapitlene presenteres empiri som er som er relevant for forskningsspørsmålene.

4.1 Samhandling

Funn omkrig samhandling i Cyberforsvaret er ment å danne bakteppe for å besvare forskningsspørsmål 1, 2 og 3 i de påfølgende delkapitlene.

Relevant empiri for samhandling og forskningsspørsmålet sett opp mot problemstillingen

Valgt definisjon av samhandling repeteres innledningsvis før den brytes ned og sees i lys av dokumentstudiene, valgt teoretisk retning og funnene i intervjuene.

> *"Samhandling er en åpen og likeverdig kommunikasjons- og utviklingsprosess mellom aktører som kompetansemessig utfyller hverandre og utveksler kompetanse, dirkete ansikt-til-ansikt eller mediert via teknologi eller med håndkraft, som arbeider mot felles mål, og hvor forholdet mellom aktørene til enhver tid hviler på tillit, involvering, rasjonalitet og bransjekunnskap"* (Torgersen & Steiro, 2009, s. 153).

Tilgjengelig ugradert kildemateriale kan sies å tilsi at samhandling vil være av betydning for at Cyberforsvaret skal lykkes med å løse pålagte oppgaver. Stortingsproporsjon 73 S beskriver kjernen i Cyberforsvaret som militært tilpasset og anvendt IKT (Prop. 73 S, 2011-2012, s. 102-103). De to undersøkte avdelingene har ulike oppgaver, som beskrevet i kapittel 1.2.1 og 1.2.2. Med utgangspunkt i Cyberforsvarets, og de utvalgte avdelingenes oppgaver og definisjonen av samhandling kan det trekkes paralleller mellom hva samhandling innebærer og hva som må oppfylles for at organisasjonen skal kunne løse pålagte oppgaver. *"Samhandling er en åpen og likeverdig kommunikasjons- og utviklingsprosess mellom aktører som kompetansemessig utfyller hverandre og utveksler kompetanse…".* For at Cyberforsvaret skal løse sine oppgaver vil ekstern samhandling være av betydning da oppgavene innebærer å støtte Forsvarets avdelinger i alt fra operasjonssikkerhetsvurderinger til deployering av norske styrker nasjonalt og internasjonalt. Det er ikke bare slik at den eksterne samhandlingen er av betydning for at avdelingene skal løse sine oppdrag. Den interne samhandlingen i Cyberforsvaret må antegeligvis legges til grunn for at avdelingene skal kunne være i stand til å samhandle eksternt. Det faktum at avdelingene er avhengig av egen organisasjon for å kunne prestere tilsier at ekstern samhandling kan sees på som et resultat av intern samhandling. Det instrumentelle perspektivets forhandlingsvariant innebærer at ingen aktør på egenhånd kan oppnå sine mål og ivareta sine interesser (Christensen et al., 2015, s. 35). Aktørene vil i dette tilfellet både kunne være interne aktører avdelingene er avhengig av i forberedelser til oppdrag eller operasjoner, og eksterne aktører de skal samhandle med i utførelsen.

Den støtten Cyberforsvarets avdelinger skal gi avdelingene kan foregå *"…direkte ansikt-til-ansikt eller mediert via teknologi eller med håndkraft…"* – med viten om at kjernen i Cyberforsvaret er militært tilpasset og anvendt IKT, og at Cyberforsvaret skal lede utviklingen av NbF vil en form for samhandling kunne sies å være sentralt. Her kan man se sammenheng mellom oppgavene og viktigheten av intern samhandling for å lykkes med dette i praksis. Ekstern samhandling vil være av betydning for Cyberforsvaret, som støttende organisasjon, for at Forsvaret skal løse sine oppgaver.

"…som arbeider mot felles mål, og hvor forholdet mellom aktørene til enhver tid hviler på tillit, involvering, rasjonalitet og bransjekunnskap". En rasjonell organisasjon kjennetegnes ved mål- og redskapsfokusering. Dette innebærer at organisasjonen ikke har noen verdi i seg selv utover det å være redskaper konstruert for så effektiv måloppnåelse som mulig. Et perspektiv er hva

forholdet mellom aktørene internt i Cyberforsvaret hviler på. Dersom det hviler på forhold som tillit, involvering, rasjonalitet og bransjekunnskap kan man si at forholdene ligger til rette for effektiv måloppnåelse. Om enkelte av disse forholdene ikke er gjeldende kan man derimot si at rasjonaliteten begrenses. Cyberforsvaret opererer i et komplekst miljø og alternativer og konsekvenser er ikke nødvendigvis like synlige til enhver tid. Dersom det er brister i den hierarkiske organisasjonsstrukturen og ledelsen ikke styrer sine aktører på bakgrunn av rasjonell kalkulasjon vil det kunne innebærer manglende samsvar mellom handling og det organisasjonen ønsker å oppnå. Et annet perspektiv er om forholdet mellom avdelingene Cyberforsvaret skal støtte og de støttende avdelingene hviler på tillit, involvering, rasjonalitet og bransjekunnskap. Det kan implisere at ekstern samhandling i praksis er viktigere enn intern, for å løse pålagte oppdrag. Om så er tilfelle kan kanskje ikke Cyberforsvaret beskrives som en enhetlig organisasjon hvor alle aktørene drar i samme retning. Organisasjonen bærer da mer preg av å være fragmentert, og avdelingene arbeider selvstendig og uavhengig av andre aktører i samme organisasjon.

Om BKI skal støtte Forsvarets avdelinger med operasjonssikkerhetsvurderinger og CIS TG skal støtte deployering av norske styrker nasjonalt og internasjonalt vil alle forholdene i definisjonen av samhandling være av betydning for å lykkes. Dette viser at ekstern samhandling er en essensiell del i Cyberforsvarets utførelse av de oppgaver de skal løse. Ser vi på den eksterne samhandlingen som essensiell for å nå mål kan en forutsetning sies å være intern samhandling i forkant av den eksterne.

Forholdet mellom samhandling og forståelse for organisasjonens oppgaver

Intervjuene startet med fokus på samhandling i Cyberforsvaret hvor Torgersen og Steiros definisjon av begrepet ble lagt til grunn. Det første spørsmålet var av åpen karakter og hensikten var å få samtalen i gang. Samtlige intervjuobjekter snakket om avhengigheten av andre aktører for å løse avdelingens oppgaver. Trolig er avhengigheten en konsekvens av et bevisst forhold til egne oppgaver, hvor avdelingene ser at de alene ikke kan løse oppgavene. Av intervjuene fremkommer dette blant annet med følgende uttalelse:

> … å ikke samhandle er umulig…det blir som at Hæren skal drive krigføring alene, det er umulig, vi driver joint med sjø og luft. Operasjonene vi har i dag i Afghanistan eller Irak

> - skal vi krige er det utenkelig å ikke ha med flystøtte. At vi ikke skal samhandle anser jeg som hundre prosent usannsynlig.[5]

Det er imidlertid lite som taler for at avhengigheten har med hele organisasjonens oppgaver å gjøre. Samtlige respondenter snakket om kompleksiteten i Cyberforsvaret oppdragsporteføljе og at denne kompleksiteten medfører utfordringer med tanke på kjennskap og kunnskap om andre avdelingers muligheter og begrensninger. Det kan virke som om fagmiljøer samhandler for å løse konkrete oppgaver. Der hvor fagmiljøene ikke er avhengig av hverandre er det i liten grad, eller ikke samhandling i det hele tatt.

Kompleksiteten i oppdragsporteføljen omtales slik: "… det gjør det enda mer utfordrende å ha tillit og kanskje enda viktigere. Generelt sett er tillit en utfordring".[6] Om det er slik at tillit mellom avdelingene og fagmiljøene i Cyberforsvaret er en utfordring kan det på den ene siden indikere at forholdene ikke ligger til rette for samhandling. Dette kan muligens årsaksforklares med manglende bransjekunnskap. Gitt det brede spekteret av oppgaver Cyberforsvaret har kan man på den andre siden kanskje ikke forvente at alle aktører besitter bransjekunnskap om hverandres fagområder. Dette kan muligens årsaksforklares med at å besitte bransjekunnskap om alle andre avdelinger i Cyberforsvaret ikke er nødvendig for at organisasjonen samlet sett skal løse pålagte oppgaver. Det kan imidlertid stilles spørsmål ved om utfordringer omkring tillit mellom avdelingene medfører at aktørene i mindre grad utfyller hverandre kompetansemessig. Der hvor aktørene utfyller hverandre kompetansemessige tyder uttalelsene på at avhengigheten og samhandlingen er essensiell: "…vi er helt avhengig av andre for å få gjort jobben vår og det er vi ydmyke på".[7] Det ser ut til å gjelde både intern og ekstern avhengighet. Det er imidlertid lite som tyder på at avhengigheten er total i hele Cyberforsvaret.

Variasjoner i samhandling mellom, og på tvers av nivåene

Det teoretiske utgangspunktet for det instrumentelle perspektivet kjennetegnes ved at man ser på organisasjoner som redskaper eller instrumenter for effektiv måloppnåelse (Christensen et al., 2015, s. 34). Organisasjonsstrukturen er formell med nedtegnede prosedyrer, rutiner, organisasjonskart, stillingsinstrukser, strategier og regler. Når jeg under intervjuene spurte om samhandling foregår i Cyberforsvaret var det delvis divergerende svar. Et perspektiv beskrives slik:

[5] Respondent #5: Intervju, Jørstadmoen, 1. April 2016
[6] Respondent #1: Intervju, Jørstadmoen, 16. Mars 2016
[7] Respondent #4: Intervju, Jørstadmoen, 29. Mars 2016

> …vi mangler felles målbilde og intensjon fra toppen og nedover som gir oss en ledestjerne å gå etter ... vi vet ikke hva vi skal samarbeide om, lite forståelse ned på nivå hvorfor vi skal samarbeide … å få målbilde og intensjon fra sjefen som gjennomsyrer hvert nivå i avdelingen er viktig. Jeg savner det i dag.[8]

Dette kan sies å være et tydelig signal om at målbilde og intensjoner ikke er godt nok formidlet ned på nivå fire. På den ene siden kan det være slik at Cyberforsvarets ledelse har et bevisst forhold til bruken av nivå fire avdelinger som instrumenter for effektiv måloppnåelse. Om avdelingene utfører sine oppgaver og løser pålagte oppdrag kan det bidra til effektiv måloppnåelse. Det kan imidlertid stilles spørsmål ved hvor effektiv måloppnåelse blir når målbilde og intensjoner ikke er tydelig formidlet ned i organisasjonen. På den annen siden kan man si mangelen på målbilde og intensjoner er medvirkende til mindre grad av samhandling mellom nivåene i Cyberforsvaret. Når målbilde og intensjoner ikke er tydelig formidlet ned i organisasjonen kan ikke samhandlingen sies å bære preg av *en åpen og likeverdig kommunikasjons- og utviklingsprosess.* Et annet perspektiv beskrives slik:

> …Det er en del samhandling i Cyberforsvaret, det har vært en periode med stor utvikling i en positiv retning. Tidligere var det litt mer blokkdelt mellom CTO og CKT … Samhandlingen den virket formell, og den er fortsatt det, men det har vært tonet mer ned slik at nå er det mer samhandling på tvers av strukturene. Det er fordi man har gjort, og vil gjøre, en del organisatoriske grep i løpet av inneværende år …. det gjør at vi har funnet en del samhandling, dette har vært på et "bottom-up" nivå sett fra vårt ståsted. Det har vært mindre samhandling på "top-down" perspektiv. Det som har vært av samhandling kommer fra grasrota slik jeg ser det.[9]

Om vi ser dette perspektivet i sammenheng med forrige sitat indikerer uttalelsene at samhandlingen som foregår i stor del er initiativ nedenfra i organisasjonen og at nivå 2 og 3 mindre grad fokuserer på, eller legger til rette for samhandling. Denne indikasjonen underbygges av følgende uttalelse: "…i mange sammenhenger følt meg alene om en del av de utfordringene vi har hatt med tanke på styrkeproduksjon til internasjonale- og nasjonale operasjoner …".[10] Dette kan sies å vise at samhandlingen muligens ikke er optimal internt i organisasjonen. Dette inntrykket forsterkes med følgende uttalelse: "…samhandling har vært en utfordring med tanke på forståelsen av faget. Ikke bare mot egen organisasjon, ledelsen på nivå 3, men også mot

[8] Respondent #1: Intervju, Jørstadmoen, 16. Mars 2016
[9] Respondent #4: Intervju, Jørstadmoen, 29. Mars 2016
[10] Respondent #4: Intervju, Jørstadmoen, 29. Mars 2016

Cyberforsvaret generelt og andre avdelinger".[11] Hittil indikerer funnene at samhandlingen ikke er optimal i Cyberforsvaret, spesielt ikke mellom nivåene. Det er imidlertid flere uttalelser som tyder på at samhandling mellom aktører som kompetansemessige utfyller hverandre innebærer en gjensidig avhengighet mellom konkrete fagmiljøer. Et mindre heldig utfall av kompleksiteten i Cyberforsvarets oppgaver må kunne sies å være forhold som beskrives slik;

> …det er ikke veldig stor grad av tillit mellom avdelingene, mer en form for rivalisering. Avdelingene involverer hverandre i liten grad for å trygge egen avdeling. Det medfører at man har kunnskap om eget fagområde, men tviholder på bransjekunnskapen og tilegner seg da ikke kunnskap om de andre fagområdene … Tviholder på eget fagområde og glemmer å se seg selv i det store bildet.[12]

På den ene siden ser vi altså samhandling mellom aktører internt i organisasjonen. Denne samhandling oppfattes å være lokale initiativer på lavere nivå. På den andre siden tyder uttalelser på at samhandling erstattes med rivalisering mellom aktører på lavere nivå. Dette kan sies å indikere liten grad av felles forståelse for hele organisasjonens oppgaver. Den manglende graden av involveringen mellom avdelingene som beskrives i sitatet over kan innebære at samhandling ekskluderes.

Bildet blir noe mer nyansert hvis vi ser på hvordan de ulike avdelingene utfyller hverandre kompetansemessige. Dette begrenser seg imidlertid til samhandling mellom aktører som er gjensidig avhengig av hverandre for å kunne løse de oppdrag avdelingene er satt til. Et eksempel på det er forhold som omtales slik;

> … vi som avdeling er helt avhengig av CTO i andre enden for å få gjort en jobb. Så vi har lagt effekt i å lære mer om CTO og at CTO skal lære mer om oss. Har vært proaktiv på vårt nivå for å få samhandling … Initiativet kommer fra nivå 4, men man må søke aksept på nivå 3 og de godkjenner … Min opplevelse av det er at det spranget mellom det fokuset vi har og det fokuset som cyberstaben har der blir det et for stort gap mellom. Ikke bare rent organisatorisk, men jeg tror og fokus … Konkret opplever jeg å ha støtte fra en del kontorer i cyberstaben i en del saker og jeg føler vi drar i en felles retning. I en del andre saker så stiller jeg meg undrende til hvorfor vi har så forskjellig fokus.[13]

Disse forholdene antyder at det er mindre grad av samhandling mellom aktører som ikke er gjensidig avhengig av hverandre. Implisitt i dette ligger manglende bransjekunnskap og trolig

[11] Respondent #2: Intervju, Jørstadmoen, 16. Mars 2016
[12] Respondent #1: Intervju, Jørstadmoen, 16. Mars 2016
[13] Respondent #5: Intervju, Jørstadmoen, 1. April 2016

også kunnskap eller innsikt i organisasjonens felles mål. Dette kan kanskje forklares med kompleksiteten og bredden i Cyberforsvarets oppdragsportefølje, som tilsier at samhandling ikke er nødvendig mellom alle. Slik sett kan man stille spørsmål ved om Cyberforsvarets organisasjonsstruktur er optimal for å nå mål. Som vi har sett i kapittel 1.2 er Cyberforsvaret organisert med to nivå 3 avdelinger. Gitt uttalelsen over om for stort gap mellom cyberstaben og nivå 4 avdelingen kan man stille spørsmålet; hva er nivå 3 avdelingenes rolle i organisasjonsstrukturen? Om det er slik at nivåene i organisasjonen er preget av ulikt fokus kan ikke Cyberforsvaret sies å være en enhetlig organisasjon. Med utgangspunkt i forventningene som legges til grunn for den hierarkiske varianten kan man på den ene siden si at de hierarkiske posisjonene ikke ser ut til å imøtekomme disse da de kanskje ikke har kontroll over de oppgavene som skal løses. Dette kan muligens innebære at nivå 3 i mindre grad følger en mål-middel tankegang og at organisasjonsstrukturen i mindre grad er homogen. På den andre siden kan man med utgangspunkt i forhandlingsvarianten si at Cyberforsvaret imøtekommer forventningen om at nivå 3 i mindre grad har innsikt og kunnskap om tilgjengelig kapasiteter, og bruken av disse. Heterogeniteten i organisasjonen medfører altså liten grad av samhandling mellom nivå 3 og 4.

I lys av samhandlingsdefinisjonen tilsier det jeg har beskrevet over at forhold mellom avdelingene og mellom nivåene i begrenset grad hviler på tillit, involvering, rasjonalitet og bransjekunnskap. Hvorvidt samhandlingen i Cyberforsvaret er preget av å være en åpen og likeverdig kommunikasjonsprosess mellom aktører som kompetansemessig utfyller hverandre, og utveksler kompetanse er det altså ikke et entydig svar på.

Totalt sett oppfatter jeg liten grad av samhandling som gjennomsyrer Cyberforsvaret. Det kommer tydelig frem at den samhandlingen som foregår er på lavere nivå og at det nivå 4 avdelinger samhandler om kan sies å være lokale initiativer.

Variasjoner i samhandling mellom personell i ulike posisjoner.

Hva mangelen på samhandling skyldes kan selvsagt ha ulike årsaker. Jeg har tidligere pekt på forhold som kompleksitet i oppdragsporteføljen, at avdelinger tviholder på egen bransjekunnskap og et gap mellom nivåene med tanke på fokusområder. Det viser seg også at samhandlingen kan sies å være påvirket av arv fra gammel organisasjonsstruktur. Følgende uttalelse beskriver dette:

> …det er liten grad av samhandling mellom CKT og CTO på enkelte saker. Opplever at det er personkonflikter som gjør at vi ikke klarer å samarbeide veldig godt på tvers av BRA-avdelingene i Cyberforsvaret. På *"maurenivå"*, nivå 4, 5, og 6 samarbeider vi til tider veldig godt, og vi opplever nok at det på litt høyere nivå er konflikter, derav personkonflikter, som lammer samhandlingen vår.[14]

I påvirket legger jeg i denne sammenheng at nivå 3 avdelingene tilsynelatende har arvet underavdelinger delvis basert på hvordan INI tidligere var organisert, og en form for maktkamp om hva som organisatorisk er plassert i de ulike avdelingene. Dette kan eksemplifiseres med følgende uttalelse:

> …Jeg tror at CIS TG havnet i CKT, betinget på arv, uavhengig av hva man skulle gjøre. Der er noe av stridens kjerne at man, CIS TG var en attraktiv aktør som man ville ha i CKT for enhver pris, uavhengig av å se rasjonale bak det eller ikke. Det var et flaggskip i cyfor, så tok man beslutningen om at den skulle ligge i CKT uten å se på hvor er det fornuftig at den ligger i cyfor sin organisasjon. CKT er en avdeling med mange avdelinger med et spredt spekter av oppgaver, det er vanskelig å se det totale bildet der, men at vi kanskje en mer nærliggende historie med CTO, det tenker jeg er riktig. Men organisasjonen bandt oss i feil organisasjon.[15]

Denne uttalelsen indikerer at Cyberforsvaret, i de formative årene, var preget av en forhandlingsvariant hvor ivaretagelse av interesser var påvirket av forhandlinger og kompromisser mellom aktørene. Hvor de ulike avdelingene fikk sitt organisatoriske oppheng kan se ut til å være basert på interessehevding. Videre kan følgende utsagn sies å forklare at det ikke bare er underenheter og koalisjoner som hevder sine interesser, men også ulike posisjoner:

> … jeg opplevde at samhandling mellom enkeltpersoner, lavere nivå var innforstått med at vi skal løse et oppdrag, på nivåene over var ikke så interessert i å møtes og bli enige om hvordan ting skal gjøres. Man var for steile og bandt seg opp i strukturer og formaliteter, kontra det å være interessert i å løse oppdraget. Man brukte da direktiver av diverse arter for å underbygge sine egne tilnærminger på saken. Som i det ene øyeblikket underbygget at man skulle gå for løsning A, mens i et annet øyemed brukte man et annet dokument for å underbygge sin egen posisjon i strukturen.[16]

Dette indikerer at samhandlingen mellom nivåene ikke bærer preg av å være en åpen og likeverdig kommunikasjonsprosess. Dette kan muligens ha med kompleksiteten og at arbeidsoppgavene spenner vidt å gjøre.

[14] Respondent #5: Intervju, Jørstadmoen, 1. April 2016
[15] Respondent #6: Intervju, Jørstadmoen, 6. April 2016
[16] Respondent #6: Intervju, Jørstadmoen, 6. April 2016

Det faktum at Cyberforsvaret er en ung organisasjon ser ut til å prege den på flere områder. For det første er den preget av arv fra gammel organisasjonsstruktur. For det andre ser organisasjonsstrukturen og desentraliseringen ut til å innvirke på hvordan og i hvilken grad ulike aktører samhandler. For det tredje er kompleksiteten i oppdragsporteføljen trolig medvirkende til varierende grad av intern samhandling:

> …vi kan konkludere med at det er en ung DIF, en kompleks DIF og cybermakt som fagfelt er veldig ungt. Det gjør at vi bør være enda flinkere til å bruke tid på oss selv og utvikle produkter i form av ordrer, direktiver og retningslinjer for hva dette skal være … Da må man bringe forståelsen til torgs og lage arenaer hvor man kan få det på plass, det er noe jeg savner stort. Jeg tror at hvis vi ikke klarer det i løpet av tre til fire år våger jeg den påstanden at Cyberforsvaret er borte som DIF i neste omstillingsrunde. Da sitter man kanskje igjen med BKI.[17]

Ut i fra disse uttalelsene ser vi på den ene siden en erkjennelse av at Cyberforsvaret er en ung organisasjon som skal utføre oppgaver og oppdrag innen et ungt og relativt nytt fagfelt. Denne kombinasjonen kan sies å legge til grunn at ledelsen bør utforme tydelig mål. Det instrumentelle perspektivets system understreker viktigheten av målspesifisering og formalisering. Respondentene kan samlet sies å etterlyse ordrer, direktiver og retningslinjer. Dette tilsier at formaliseringen kan være mangelfull. Dersom dette kan forklares med at organisasjonen og fagfeltet er ungt er det desto viktigere at dette kommer på plass for at Cyberforsvaret skal ha livets rett.

4.1.2 Delkonklusjon

Hensikten med dette delkapittelet har vært å etablere en forståelse for hvordan samhandling foregår i Cyberforsvaret, med den intensjon å danne et bakteppe for videre presentasjon av funn omkring de utvalgte faktorene. De empiriske funnene tilsier at organisasjonen er avhengig av samhandling for å kunne løse pålagte oppgaver. Samhandling er av spesielt stor betydning med eksterne aktører da avdelingenes oppgaver generelt sett kan sies å være at de skal støtte Forsvaret. Den interne samhandlingen ser imidlertid ut til å være basert på tilfeldigheter i form av personlige relasjoner og faglig gjensidig avhengighet. Det ser ut til at intern samhandling er initiativer på lavere nivå, og ledelsen virker i liten grad å ha interesse eller innvirkning på hvordan den interne samhandlingen oppstår og foregår. Det kommer tydelig frem at det er begrenset tillit mellom nivåene i organisasjonen og at dette påvirker samhandling og

[17] Respondent #4: Intervju, Jørstadmoen, 29. Mars 2016

avdelingenes utførelse av oppgaver. Organisasjonen er preget av arv fra gammel organisasjonsstruktur og det ser ikke ut til at ledelsen har klart å formidle et felles mål som alle aktørene samhandler om å nå. Videreføringen av INI ser ut til å prege Cyberforsvaret i større grad enn tilpasning til cyberdomenet. Den varierende graden av samhandling mellom og på tvers av nivåene ser ut til å være en konsekvens av en kompleks oppdragsportefølje. Det kan se ut til at samhandling ikke er nødvendig mellom samtlige aktører. Dette kan imidlertid være en begrensende faktor for felles forståelse av organisasjonenes oppgaver.

4.2 Tilhørighet

Med utgangspunkt i hypotese 1 har dette delkapittelet til hensikt å besvare forskningsspørsmål 1; Er det gjensidig avhengighet mellom avdelingene i Cyberforsvaret?

Relevant empiri for tilhørighet og forskningsspørsmålet sett opp mot problemstillingen

I begrepet tilhørighet legger jeg til grunn to varianter med tilnærmet lik betydning. Den ene omhandler tilhørighet innad i de ulike avdelingene, den andre omhandler tilhørighet i Cyberforsvaret som organisasjon. Det vil være av betydning å avdekke begge variantene av tilhørighet for å besvare problemstillingen. Til grunn i avdelingstilhørighet legges en persons tilhørighet til avdelingen. Tilhørighet kan være av betydning for hvordan avdelingen og Cyberforsvaret presterer og yter. Tilhørighet internt i en avdelingen er imidlertid ikke ensbetydende med tilhørighet mellom avdelingene, og til Cyberforsvaret som helhet.

Som beskrevet i kapittel 2.4.2 kan tilhørighet bygge på faktorer som samhold og identitet (B. H. Johnsen, 2005, s. 302). Under intervjuene har jeg forsøkt å avdekke hvorvidt intervjuobjektene har tilhørighet i egen avdeling, i Cyberforsvaret og om det er tilhørighet mellom avdelingene. De ulike avdelingenes prestasjoner vil kunne være av betydning for hvordan Cyberforsvaret i helhet presterer. Avdelingenes og Cyberforsvarets prestasjoner kommer jeg nærmere inn på i neste delkapittel.

I en hierarkisk variant av det instrumentelle perspektivet ser man på organisasjonen som enhetlig. I lys av denne varianten er mitt utgangspunkt at en enhetlig organisasjon innebærer tilhørighet mellom aktørene i organisasjonen, det være seg mellom individer og avdelinger, og på tvers av nivåene i hierarkiet.

I en forhandlingsvariant ser man på organisasjonen som sammensatt av ulike underenheter og posisjoner som kan ha delvis motstridende mål, interesser og kunnskaper. Utfallet av

måloppnåelse og ivaretagelse av interesser vil være påvirket av forhandlinger og kompromisser mellom flere aktører. Dette skyldes at ingen aktør på egenhånd kan oppnå sine mål og ivareta sine interesser. Mitt utgangspunkt i forhandlingsvarianten er at man i mindre grad er avhengig av tilhørighet mellom avdelinger for å løse organisasjonens oppgaver.

Forholdet mellom tilhørighet og forståelse for organisasjonens oppgaver

I samtlige intervju snakket vi om på hvilken måte intervjuobjektene har tilhørighet til egen avdeling og Cyberforsvaret. Hensikten var å avdekke om tilhørighet, eller mangel på tilhørighet, påvirker forståelsen for de oppgavene organisasjonen skal løse. I de undersøkte avdelingene stilles det høye krav til faglig dyktighet, presise leveranser og evne til å håndtere oppdukkende situasjoner. Samtlige respondenter uttrykte en form for sterk tilhørighet til egen avdeling og de anerkjenner avdelingens faglige leveranser. Med det utgangspunkt at tilhørighet kan bygge på faktorer som samhold og identitet spurte jeg under intervjuene om respondentene kunne si noe om dette. Følgende uttalelse setter dette i perspektiv:

> …identifiserer meg ikke med nivå 3 avdelingen vi tilhører eller Cyberforsvaret, jeg føler ikke at Cyberforsvaret er enhetlig…Karrieremessige føles det som et blindspor å være i Cyberforsvaret, min bakgrunn er fra Hæren, men siden jeg har jobbet lenge i Cyberforsvaret er jeg glemt av Hæren…Jeg føler meg ikke hjemme i Cyberforsvaret, hva annet er det enn et blindspor?.[18]

På den ene siden kan dette sees på som manglende evne til ivaretagelse av eget personell i Cyberforsvaret. Man kan dermed anta at manglende ivaretagelse av eget personell reduserer graden av internt samhold i Cyberforsvaret, og at den enkelte dermed i mindre grad ønsker å identifisere seg med organisasjonen. På den andre siden tilsier respondenten sitt svar på spørsmål om avdelingen er en del av en helhet at avdelingens faglige leveranser er av betydning for helheten;

> …Vi er helt klart en del av en helhet. Vi er en operativ avdeling som er til støtte for Forsvaret. Vi har i bakhodet til enhver tid å "sikre Forsvarets operative handlefrihet" alt vi gjør skal være til støtte. Vi gjør ingenting for vår egen del. Vi bruker mye tid på å heve personellets kompetanse, trener prosesser for å levere en god tjeneste til Forsvaret, for å sikre Forsvarets systemer. Dette gjør vi også sammen med andre deler av Cyberforsvaret. Jeg ser helt klart at vi er en liten brikke av det store puslespillet, men vi er en viktig brikke.[19]

[18] Respondent #1: Intervju, Jørstadmoen, 16.03.2016
[19] Respondent #1: Intervju, Jørstadmoen, 16.03.2016

Det som fremkommer kan innebære en form for divergerende tilhørighet. Respondentenes tilhørighet virker å være sterk i egen avdeling, begrenset overfor nivået over og tilstedeværende i en større sammenheng. Avdelingskulturen ser ut til å være av avgjørende betydning for hva respondentene ønsker å identifisere seg med. Samtidig fremstår samtlige som lojale overfor systemet de er en del av og dermed forholder seg profesjonelt til helheten. På den ene siden kan kanskje den sterke graden av tilhørighet til egen avdeling sies å være en medvirkende faktor til god forståelse for egen avdelings oppgaver. Det kan imidlertid reises tvil om hvorvidt en felles forståelse for organisasjonens oppgaver er tilstedeværende gitt det faktum at respondentene uttrykker mindre grad av tilhørighet til nivå 3. På den andre siden kan det at respondentene uttrykker tilhørighet til Cyberforsvaret som helhet være en medvirkende faktor til felles forståelse for hele organisasjonens oppgaver. Om disse antagelsen stemmer er det derimot vanskelig å se for seg at en felles forståelse kan være gjeldende da avdelingen de undersøkte enhetene er underlagt i begrenset grad ser ut til å styre underenhetene. På bakgrunn av det som fremkommer av intervjuene, kan det virke som at organisasjonen ikke har et klart og tydelig skille mellom organisatorisk oppheng og hvem som er oppdragsgiver.

> … Nå har jeg måtte forholde meg til to kommandolinjer som tidvis har gått i hver sin retning. Det har vært slitsomt for avdelingen. Når det har vært sånn må man justere og være kritisk til de signalene som kommer, så sluttresultatet blir nok ganske bra, men prosessen blir slitsom… kommandolinjene har ikke satt oss opp for suksess, men for feil. Som gjør at du må forholde deg til mange aktører og her har vi nok følt på kroppen på aktører som ikke har hatt tillit til hverandre. Det er min klare erfaring at her har det vært en del revirtenkning som har preget Cyberforsvaret. Kanskje sterkt å si at det har preget Cyberforsvaret, men det har i alle fall preget vår hverdag i avdelingen, og det har vært utfordrende å håndtere i en periode.[20]

Med utgangspunkt i McKinsey-rapporten hvor det fastslås at forsvarssektoren har valgt en uegnet organisering av IKT (McKinsey & Company, 2015, s. 51), har jeg tidligere sagt at det kan være grunn til å reise en viss tvil om Cyberforsvaret er ideelt organisert. Det faktum at hele forsvarssektorens organisering av IKT vurderes som uegnet er ikke nødvendigvis ensbetydende med at dette er gjeldende for Cyberforsvaret også. Uttalelsen over indikerer imidlertid utfordringer for avdelingen som en konsekvens av ulike kommandolinjer. Gitt det som fremkommer av intervjuene er kanskje den sterkt begrensede graden av tilhørighet til nivå 3 en medvirkende faktor til at en felles forståelse for Cyberforsvarets oppgaver er vanskelig å oppnå.

[20] Respondent #5: Intervju, Jørstadmoen, 01.04.2016

Variasjoner i tilhørighet mellom, og på tvers av nivåene

På utdypende spørsmål om tilhørigheten til Cyberforsvaret, påpekes det igjen, fra flere av intervjuobjektene, at tilhørigheten til Cyberforsvaret skyldes at avdelingen de jobber i er en del av en større helhet. Tilhørigheten i Cyberforsvaret beskrives slik; "…Jeg går ikke rundt og sier jeg jobber i Cyberforsvaret, jeg jobber her, men som en del av noe større. Det er avdelingen jeg fremmer pr i dag".[21] Dette utdypes på følgende måte; "… vi føler oss mer knyttet til cyberstaben og føler ikke tilhørighet til nivå 3. Nivå 3 har aldri favnet om oss, de er et forsinkende ledd, og jeg tror at avdelingen for nivå 3 er et støyende ledd".[22] Det fremkommer, i samtlige intervjuer, at tilhørigheten til egen avdeling er sterk. Imidlertid er den enkeltes tilhørighet til avdelingen nivå 3 i langt mindre grad til stede. Det kan virke som om dette kan årsaksforklares med både Cyberforsvarets organisasjonsstruktur og Cyberforsvarets komplekse oppdragsportefølje. Organisasjonsstrukturen beskrives slik: " … er av den oppfatning at slik den er i dag er den ikke god. Den er dysfunksjonell med tanke på måloppnåelse. Det er tiltak på gang for å gjøre organisasjonsstrukturen mer funksjonell, det blir nok bra".[23] Denne uttalelsen kan sies å bekrefte tvilen jeg tidligere har reist om Cyberforsvaret er ideelt organisert. Om dette er tilfellet ser vi altså en sammenheng mellom funn i McKinsey-rapporten og i Cyberforsvaret som en av aktørene innen IKT i forsvarssektoren. Videre beskrives kompleksiteten i Cyberforsvarets oppgaver slik: "…når det gjelder utdanning og avdelinger som vi på en måte burde vært knyttet nærmere til så opplever vi at vi blir såpass forskjellige at jeg ikke tror vi har noen "å sitte i samme båt" følelse innen den organisasjonen vi er i, i dag".[24]

Flere av respondentene uttrykte at utfordringer de to nivå tre avdelingene har hatt seg imellom har påvirket avdelingenes daglige virke. Det kan synes som om interne utfordringer mellom avdelingene på nivået over har medført liten grad av samhold og lite ønske om å identifisere seg med avdelingen de er underlagt. Som en konsekvens av dette er det flere indikasjoner på at avdelingene jeg har undersøkt i større grad vil identifisere seg med organisasjonen som helhet, og dermed hopper over, eller unngår nærmeste nivå. Samarbeidsutfordringene som beskrives mellom nivå tre avdelingene synes å forsterke dette;

> …slik jeg hører enkelte uttaler seg er det ikke alltid man i CTO har hatt tillit til hva CKT driver med. Sikkert motsatt. Vi på nivå 4 ser bare prosessene og det er ikke alltid sikkert vi er del av de, men at det til tider er manglende tillit og uenigheter det fremstår av

[21] Respondent #5: Intervju, Jørstadmoen, 01.04.2016
[22] Respondent #1: Intervju, Jørstadmoen, 16.03.2016
[23] Respondent #4: Intervju, Jørstadmoen, 29.03.2016
[24] Respondent #6: Intervju, Jørstadmoen, 06.04.2016

> enkelte prosesser det siste året. Tidligere også ser jeg at uenighetene mellom CTO og CKT er dirkete lammende for Cyberforsvaret og Forsvaret som helhet.[25]

Om vi ser denne uttalelsen i lys av det instrumentelle perspektivet kan man stille spørsmål ved mål-middel forståelsen, om den er felles i organisasjonen. Manglende tillit og uenigheter mellom nivå 3 avdelingene kan innebære mindre grad av samsvar mellom handling og det organisasjonen som helhet ønsker å oppnå. Dersom vi ser det i lys av forhandlingsvarianten kan det imidlertid være slik at utfallet av måloppnåelse og ivaretagelse av interesser er påvirket av forhandlinger og kompromisser mellom nivå 3 avdelingene. Dette kan imidlertid innebære at forhandlingsvarianten hemmer hierarkisk styring. Flere uttrykte manglende forståelse for avdelingenes fagområder og viktigheten av kunnskap og innsikt i muligheter og begrensninger fra nivået tre. Det indikeres også at det mellom de ulike avdelingene internt i CKT og CTO er manglende forståelse for hverandre.

Variasjoner i tilhørighet mellom personell i ulike posisjoner

Som jeg har vært inne på tidligere legges tilhørighet mellom en person og en avdeling til grunn for avdelingstilhørighet. Flere av respondentene snakket imidlertid om utfordringer mellom posisjoner på nivåene over. Disse utfordringer virker å være av en slik karakter at de har påvirket personellets og nivå 4 avdelingenes tilhørighet på ulike måter. Da det ser ut til at dette er en medvirkende årsak til den varierende graden av tilhørighet internt i Cyberforsvaret er funnene relevante for problemstillingen.

Tilhørigheten internt i avdelingene virker sterk og avdelingskulturen fremstår som en medvirkende årsak til dette. Det er imidlertid lite som tyder på tilhørighet til nivå 3:

> …nei, jeg ser ikke noen knagger jeg kan henge meg opp i, i nivå 3 avdelingen vi tilhører … Vi sitter ikke i samme båt. Vi gjør ting i den beste hensikt, men så blir det bare støy av det … det er dysfunksjonelt, personkjemien har ødelagt mye av dette.[26]

Samtlige intervjuobjekter kom i flere sammenhenger inn på personkonflikter og hvordan dette har påvirket avdelingene og Cyberforsvaret;

> … Lojalitetsfølelsen den er om ikke fraværende så er den til tider manglende. Når en beslutning er tatt forventer jeg at man forholder seg til den, men her oppleves det som om man kjører en omkamp når det passer.[27]

[25] Respondent #5: Intervju, Jørstadmoen, 01.04.2016
[26] Respondent #6: Intervju, Jørstadmoen, 06.04.2016

Denne uttalelsen kan sees i lys av forhandlingsvarianten i det instrumentelle perspektivet. Dersom den dominerende koalisjonen får gjennomslag for sine mål og interesser ser det ut til at en sekvensiell løsning av konflikter praktiseres for å senere endre på det man ikke innledningsvis fikk gjennomslag for. Derimot kan respondenten sin forventning om at man skal forholde seg til en beslutning når den er fattet sees i lys av en hierarkisk variant. I praksis betyr det at Cyberforsvaret som organisasjon praktiserer eller lever opp til ulike varianter på de ulike nivåene. Dette underbygges på følgende måte:

> … Jeg tror at man innerst inne har en intensjon om å være løsningsorientert og få til gode løsninger. Men på grunn av personkjemi og organisasjonsstruktur så har det gått helt i stå. Det har vært en utfordring. Organisasjonen har brukt personkonflikter som argumenter mot å da ikke få til noen gode prosesser oppi dette. Selv om intensjonen til den enkelte har vært at "*jeg vil være med på å skape interoperabilitet og skape gode løsninger*". Men den enkelte skal ha mer ære av produktene og det har slått beina under prosessen … Den enkelte har hatt gode tanker om hvordan det skal løses, men det har blitt problematisk med personkonflikter, så kommer organisasjonsstrukturen som nummer to. Jeg tror man kunne løst dette greit, selv om organisasjonen er som den er, men personkonfliktene har overdøvd organisasjonsoppheng også.[28]

Samlet sett gir respondentene uttrykk for at de identifiserer seg med, og kjenner tilhørighet til egen avdeling, delvis til Cyberforsvaret og i liten grad til CKT og CTO. En slik vekslende tilhørighet internt i organisasjonen antyder at Cyberforsvaret i liten grad er en enhetlig organisasjon preget av samhold, og hvor personellet i mindre grad ønsker å identifiserer seg med noe felles. Ut i fra dette ser vi altså at tilhørigheten mellom individ og organisasjon er gjeldende for samtlige intervjuobjekter på ulikt vis.

På spørsmål om forholdet mellom avdelingene hviler på tillit synes dette å bero på tilfeldigheter. Tilfeldigheter i form av personlige relasjoner og faglig tilknytning. Det kan impliserer at samarbeidsarenaer uteblir og at organisasjonen ikke utnytter avdelingene på en optimal måte med tanke på måloppnåelse. Det faktum at flere av intervjuobjektene uttrykker å oppfatte mistillit mellom personer i cyberstaben, i CKT og i CTO ser altså ut til å ha en lammende effekt på organisasjonen som helhet. Dette gjelder spesielt i de tilfeller hvor mangelen på tilhørighet er av en slik karakter at den ender opp i konflikter. Tillit mellom avdelingene i Cyberforsvaret beskrives slik:

[27] Respondent #5: Intervju, Jørstadmoen, 01.04.206
[28] Respondent #6: Intervju, Jørstadmoen, 06.04.2016

> …har en ørliten følelse av at tilliten til hverandre er litt manglende…har opplevd stor grad av mistillit mot den avdelingen jeg jobber i, og det resulterte i en større sak. Tror mye av det er basert på manglende tillit, en form for mistillit hvor det ble tillagt andre hensikter og antakeligvis også manglende kunnskap. Manglet grunnleggende kunnskap om hva man gjorde. Det gjelder avdelingen over.[29]

Uttalelsene fra respondentene indikerer at samhandlingen mellom nivå 3 avdelingene er mindre god på enkelte områder. Et perspektiv er manglende tillit som kan påvirke tilhørigheten på tvers av avdelinger og nivåer. Dette er imidlertid ikke gjeldene for de lavere nivåene:

> … På maurenivå, nivå 4, 5 og 6 samarbeider vi til tider veldig godt, og vi opplever nok at det er på litt høyere nivå er konflikter, derav personkonflikter, som lammer samhandlingen vår.[30]

På spørsmål om det er tillit mellom nivå 3 avdelingene fremkommer imidlertid et annet perspektiv:

> Ja, det hviler på tillit, helt klart. En ting er kunnskap og kompetanse om hverandre og hva man jobber med, og ha kjennskap til det … På den annen side har vi sett at manglende tillit mellom personer i cyberstaben, CKT og CTO og en organisatorisk tilnærming nå når vi har innført det med cyfor takled har gjort at det har vært vanskelig å fremme tillit. Fordi kommandolinjene har ikke satt oss opp for suksess, men for feil. Som gjør at du må forholde deg til mange aktører og her har vi nok følt på kroppen på aktører som ikke har hatt tillit til hverandre.[31]

På den ene siden kan dette indikere at tillit mellom avdelingen er basert på kunnskap og kompetanse. Slik sett samsvarer dette med deler av definisjonen av samhandling hvor forholdet mellom aktørene beskrives å hvile på tillit, involvering, rasjonalitet og bransjekunnskap. På den andre siden kan det imidlertid reises tvil omkring involvering og rasjonalitet gitt manglende tillit mellom personer i cyberstaben, CKT og CTO. Det kan altså se ut til at det er en form for tillit relatert til fag og kompetanse, men begrenset tillit mellom personer og posisjoner.
Dette inntrykket forsterkes med følgende uttalelse:

> …Ja, det er for så vidt det, rent kompetansemessig. Det som mangler litt er gjensidig forståelse. For avdelingen er det greit, men resten av organisasjonen mangler en forståelse for hva fagfeltet

[29] Respondent #2: Intervju, Jørstadmoen, 16.03.2016
[30] Respondent #5: Intervju, Jørstadmoen, 01.04.2016
[31] Respondent #4: Intervju, Jørstadmoen, 29.03.2016

til avdelingen er. Hvis gjensidig forståelsen for hva man holder på med er kunnskap så er det forbedringspotensial.[32]

4.2.2 Delkonklusjon

Hensikten med dette delkapittelet har vært å besvare forskningsspørsmål 1 og å teste hypotese 1. For å kunne besvare den overordnede problemstillingen har denne studien fokusert på tilhørighet innad i avdelingene og tilhørighet internt i Cyberforsvaret. Funnene fra intervjuene viser tydelig at det er stor grad av tilhørighet mellom intervjuobjektene og avdelingen de tilhører. Tilhørigheten til avdelingen på nivå 3 er imidlertid begrenset. Dette ser ut til å skyldes flere forhold. Det være seg organisasjonsstruktur, organisasjonsoppheng og personkonflikter på nivåene over som har virket lammende på organisasjonen i helhet. Intervjuobjektene uttrykker nesten entydig at de ikke ønsker å identifisere seg med nivå 3. Samtidig anser de eget virke og avdelingens oppdrag som en del av en større helhet og de identifiserer seg dermed i større grad med Cyberforsvaret enn med nivå 3 avdelingene. Den varierende graden av tilhørighet mellom, og på tvers av nivåene ser ut til å være en begrensede faktor med tanke på hvorvidt avdelingene i organisasjonen kan ha felles forståelse for Cyberforsvarets oppgaver. Funnene indikerer at hypotese 1 kan bekreftes. Samhandlingen som foregår i Cyberforsvaret ser ut til å være uavhengig av organisasjonsstrukturen. Funnene tilsier at samhandlingen er en konsekvens av gjensidig avhengighet mellom aktører for å løse konkrete oppgaver.

4.3 Prestasjon

Med utgangspunkt i hypotese 2 har dette delkapittelet til hensikt å besvare forskningsspørsmål 2; Har avdelingene forståelse av at de arbeider mot felles mål?

Empiri som er relevant for prestasjon og forskningsspørsmålet sett opp mot problemstillingen

Cyberforsvaret oppgaver spenner vidt og oppdragsporteføljen er kompleks. Det innebærer at organisasjonen har mange ulike fagmiljøer. Systemene Cyberforsvaret skal drifte og tjenestene de skal levere medfører stor grad av samhandling med eksterne aktører. Som jeg tidligere har vært inne på antas at for å lykkes med ekstern samhandling, må en form for intern samhandling ligge til grunn. Det viser seg imidlertid at den interne samhandling begrenser seg til å gjelde avdelinger og aktører som en kompetansemessige avhengig av hverandre for å utføre oppgavene de skal løse. Hvorvidt den interne samhandling kun er begrenset til aktører som er gjensidig

[32] Respondent #2: Intervju, Jørstadmoen, 16.03.2016

avhengig av hverandre har trolig innvirkning på forståelse for andre avdelingers oppgaver, og dermed også felles forståelse for hele organisasjonens oppgaver. Dette påvirker trolig avdelingsvise prestasjoner og dermed også hele organisasjonenes prestasjoner. Det faktum at Cyberforsvaret er en ung organisasjon vil kunne innebære at den må gjennom en del omstrukturering før den er optimalt tilpasset for å nå mål. Det innebærer at det ikke er utenkelig at den siden opprettelsen og navneendringen i 2012 er sterkt preget av arv fra gammel organisasjonsstruktur.

Forholdet mellom prestasjoner og forståelse for organisasjonens oppgaver

Funn i intervjuene indikerer at de ulike avdelingene arbeider forholdsvis selvstendig og løser oppgavene de er satt til kun avhengig av enkelte andre aktører. Avhengigheten til de andre aktørene er imidlertid avgjørende for at de skal kunne løse sine oppdrag. Funnene kan derimot ikke sies å ha avdekket en logikk i hvilke andre aktører avdelingene er avhengige av utover teknisk avhengighet. I teknisk avhengighet legger jeg at systemer avdelingene opererer fungerer, at utstyr og materiell er tilgjengelig. Funnene indikerer at avhengigheten ikke er logisk med tanke på organisasjonsstruktur eller organisasjonsoppheng. Til tross for dette ser det ut til at de ulike avdelingene løser sine oppdrag mer eller mindre selvstendig og delvis uavhengig av organisasjonen. Det som fremkommer kan kanskje påvirke Cyberforsvarets totale prestasjoner. På spørsmål om avdelingene arbeider mot felles eller motstridende mål kan svarene sies å representere ulike perspektiver:

> …Det er ikke felles, men ikke motstridende … Det er litt tilfeldig hvilken avdelinger som ligger i organisasjonene. Det tror jeg er historiske betinget, det er samleposter fra historie, nyvinninger, lokasjoner og så videre … Det har på en måte bare blitt en organisasjon.[33]

Denne uttalelsen bekrefter delvis hypotese 2. Cyberforsvaret kan sies å være en organisasjon tuftet på arv fra gammel organisasjonsstruktur. Hvorvidt organisasjonsstruktur og organisasjonsoppheng kan ses i lys av den hierarkiske varianten kan det imidlertid stilles spørsmål ved. Av uttalelsen over fremkommer det at hvilken større enhet avdelingen inngår i ser ut til å være basert på tilfeldigheter. I lys av forhandlingsvarianten kan det forklares med at organisasjonsstrukturen er et resultat av interessehevding eller kjøpslåing. Et annet perspektiv er:

> … Har forståelse av at avdelingene drar i samme retning og arbeider mot et felles mål. Organisasjonen preges av å være tuftet på arv fra gammel organisasjonsstruktur, mye har

[33] Respondent #6: Intervju, Jørstadmoen, 06.04.2016

> blitt videreført og vi utfører fremdeles de samme oppgavene som vi gjorde før Cyberforsvaret ble etablert. For enkelte mindre avdelinger i CTO er det av mindre betydning hvor de organisatorisk hører hjemme for å utføre oppgaver ... Hva avdelingen presterer påvirkes ikke i nevneverdig grad av arv.[34]

Denne uttalelsen indikerer en forståelse for at avdelingene arbeider mot et felles mål. På den enes siden kan det at avdelingene gjør de samme oppgavene som de gjorde før Cyberforsvaret ble etablert, indikere at opprettelsen av Cyberforsvaret kun var en navneendring. Det at organisasjonsoppheng er av mindre betydning kan innebære at Cyberforsvaret består av avdelinger som utfører sine oppgaver som selvstendige enheter. Om det er slik at avdelingene utfører sine oppgaver som selvstendige enheter kan det på den andre siden indikere at enhetene ikke må se seg selv som del av en større enhet. "… vi driver med tilnærmet det samme som det vi gjorde før navneendringen. For mange var det vel stort sett bare en navneendring".[35] Gitt påvirkning gammel organisasjonsstruktur har på den nye ser det altså ut til at den har vanskeliggjort endring. Om så er tilfelle samsvarer dette med hypotese 2. På utdypende spørsmål om Cyberforsvaret har klart å etablere en god organisasjonskultur indikerer funnene at organisasjonen er preget av å være en fellesavdeling. Samlet sett gir respondentene uttrykk for at avdelingskulturen er sterk og at den er av betydning for avdelingens prestasjoner. Det er imidlertid lite som tyder på at Cyberforsvaret har evnet å etablere en felles organisasjonskultur. Cyberforsvaret ser ut til å være sterkt preget av at de er en fellesavdeling. Det at personellet har ulike bakgrunner og ulike kulturer med seg inn i Cyberforsvaret fremstår som en positiv konsekvens av opprettelsen. Til tross for at organisasjonen er tuftet på arv fra gammel organisasjonsstruktur ser det ut til at mangfold, i form av bakgrunn, verdsettes:

> … vi er en avdeling tuftet på gamle Hærens samband. Det fremstår klart, det bærer preg av det. Vi har for få luft og sjø mennesker. Vi er en fellesavdeling. De første årene avdelingen eksisterte var det bare hær-sjefer. Det var veldig behagelig å få en sjef som hadde tjenestegjort et annet sted enn Jørstadmoen. Det er en berikelse og det er veldig bra for avdelingen. Få andre meninger, andre erfaringer, tørre å utfordre ting på en annen måte i stedet for at vi bare gjør det på den ene måten. Det gjelder sikkert for andre også. Det er ingen fordel at vi er så mange hær-mennesker, snarere tvert imot. Det er det ikke bare jeg som mener.[36]

Med denne uttalelsen kan man si at organisasjonenes personellsammensetning er medvirkende til bedre prestasjoner.

[34] Respondent #3: Intervju, Jørstadmoen, 17.03.2016
[35] Respondent #5: Intervju, Jørstadmoen, 01.04.2016
[36] Respondent #5: Intervju, Jørstadmoen, 01.04.2016

Variasjoner i prestasjoner mellom, og på tvers av nivåene

I intervjuene fremkommer det at avdelingene har et sterkt fokus på faglige leveranser. Begge avdelingene opererer innen konkrete fagområder og de leverer i stor grad nisjeprodukter. "…Cyberforsvarets fokus er faglig rettet … Det har imidlertid ikke vært tilstrekkelig forståelse for avdelingens oppgaver, og viktigheten av de på nivået over".[37] Denne uttalelsen indikerer at det ikke bare er slik at avdelingene har fokus på faglige prestasjoner, men også slik at Cyberforsvaret har det. Likevel kan det stilles spørsmål ved om fokuset er felles når avdelingen over ikke har tilstrekkelig forståelse for avdelingens oppgaver, og viktigheten av de. Det kan i praksis bety at nivået avdelingen er underlagt ikke er medvirkende til avdelingens prestasjoner. Om så er tilfelle kan man anta at dette påvirker hele organisasjonens oppgaver. I en hierarkisk organisasjonsstruktur er ulike oppgaver tillagt ulike nivåer. Om det er slik at avdelingen over mangler forståelse kan ikke organisasjonsstrukturen sies å være hensiktsmessig med tanke på prestasjoner og leveranser. Denne antagelsen underbygges av følgende uttalelse:

> ... Vi skal egentlig snakke med FOH gjennom organisasjonen vi er underlagt, men på nivå 3 er det ingen med kompetanse innen vårt fagområde. Det medfører at krav eller dialog med FOH ikke kan synliggjøres og styres nedover gjennom nivå 3. Avdelingen driver voksenopplæring i to retninger, det er krevende og vi føler oss satt på siden, vi blir ikke integrert i organisasjonen vi tilhører.[38]

Det at avdelingen ikke blir integrert i organisasjonen de tilhører kan indikere at de ikke føler de arbeider mot et felles mål. I lys av disse uttalelsene, og med det instrumentelle perspektivet som bakteppe, tyder mye på at ledelsen ikke i tilstrekkelig grad besitter dyp innsikt i virksomhetens mål. Ei heller at de har god oversikt over tilgjengelig virkemidler og mulige konsekvenser av disse. Ut i fra dette kan man på den ene siden hevde at om en avdeling på nivå 4 må drive voksenopplæring for få utført sine oppgaver kan ikke avdelingen sess på som et effektiv instrument mot måloppnåelse. Dette kan delvis forklares i lys av forhandlingsvarianten i det instrumentelle perspektivet – avdelingen må fremme eget fagområdet for å ha livets rett. En annen forklaring kan være at fagområdet er så komplekst at det ikke kan forventes at nivået over innehar dyp innsikt i faget. På den andre siden kan man hevde at avdelingen er konstruert for så effektiv måloppnåelse som mulig, og at det forventes at de løser sine oppdrag uten å bli detaljstyrt. Detaljstyring har imidlertid flere sider: "… noen ganger føler jeg nivåene over styrer i detaljer som helt klart et mitt domene. Andre ganger pekes det eksempelvis på personell i min

[37] Respondent #3: Intervju, Jørstadmoen, 17.03.2016
[38] Respondent #1: Intervju, Jørstadmoen, 16.03.2016

avdeling uten at jeg får være med, andre ganger føler jeg at de burde tatt tak".[39] Denne uttalelsen antyder at organisasjonsstrukturen bærer preg av manglende tillit. For det første kan man anta at tillit mellom nivåene er av betydning med tanke på avdelingens prestasjoner. Om avdelingen ikke vises tillit og detaljstyres i enkelte situasjoner og i andre ikke vil det kanskje være vanskelig å forholde seg til nivået over. For det andre kan man anta at manglende tillit til nivået over påvirker hele organisasjonenes prestasjoner. Om avdelingene ikke vises tillit kan det medføre mistillit til oppdragsgiver og at avdelingene isolerer seg. Organisasjonen kan da ikke ses på som enhetlig, men som sammensatt av aktører med delvis motstridende mål. Dette er i så fall i samsvar med forhandlingsvarianten i det instrumentelle perspektivet.

En respondent tegnet en skisse over organisasjonsstrukturen i Cyberforsvaret og forklarte, med skissen som utgangspunkt, hvordan oppdrag fordeles, føringer og justeringer formidles og hvordan informasjonsflyten mellom de ulike nivåene foregår. Av samtalen kom det tydelig frem at organisasjonsstrukturen og nivåene avdelingen må forholde seg til ikke bidrar til effektiv måloppnåelse. Før opprettelsen av Cyberforsvaret hadde avdelingen en tettere dialog med FOH.

> … så var det omorganisering som gjorde at FOH fortsatt var "der" opp, så fikk man inn cyberstaben, CTO og CKT og avdelingen vår her ned. Det medførte fra mitt ståsted en del utfordringer i forhold til hvordan man skulle håndtere informasjon og de oppdrag som kom fra toppnoden (FOH) ned til nivået som skulle gjøre tilsvarende oppgaver som før.[40]

I lys av det instrumentelle perspektivet kan dette tyde på at Cyberforsvarets ledelse har gjort endringer i organisasjonen for at den skal være optimalt tilpasset for å nå mål. På den ene siden kan man stille spørsmål ved om endringene medførte at organisasjonen ble optimalt tilpasset gitt de utfordringene respondenten beskriver. På den andre siden må man kanskje være åpen for at organisatoriske endringer innebærer enkelte utfordringer i overgangsfaser. Videre beskrives utfordringene med omorganiseringen slik:

> … Det som da kunne skje var at ting gikk fra FOH og inn i cyberstaben som sendte oppdragene ut både i CTO-søylen og CKT-søylen og ned til avdelingen. Så fra å på en måte være direkte underlagt og koordinering der så fikk man plutselig et og to ledd mellom seg selv og oppdragsgiver ... Man visste på en måte ikke hvordan man skulle angripe denne situasjonen, og noe havnet kanskje urettmessig i den ene søylen CTO, og andre ting i den andre søylen CKT og noe kom ned til oss. FOH var også preget av den gamle organiseringen og så at ting tok for lang tid, det ble for uryddig hvordan ting gikk

[39] Respondent #4: Intervju, Jørstadmoen, 29.03.2016
[40] Respondent #6: Intervju, Jørstadmoen, 06.04.2016

> nedover i organisasjonen … og da gikk pilene (oppdrag, føringer, informasjon) også begge veier. Det var ikke alltid at nivåene var innforstått med hva som skjedde.[41]

Disse uttalelsene kan sies å bekrefte antagelsen om at Cyberforsvaret har vært preget av arv fra gammel organisasjonsstruktur. Om vi ser uttalelsen i lys av en hierarkisk variant antyder den at Cyberforsvarets ledelse har forsøkt å gjøre en form for arbeidsdeling. Cyberforsvarets ledelse og den større enheten avdelingen er tilknyttet kan sies å forsøke å tillegge oppgaver til de ulike nivåene. Det er imidlertid lite som tyder på at organisasjonskart, stillingsinstrukser og regler for hvem som skal gjøre hva har vært på plass.

På spørsmål om det er slik at nivå 3 avdelingene sitter på sin egen tue og ikke ser organisasjonens beste sies: "…det er en veldig god påstand om jeg sier meg enig i. Det fremstår for meg som at det er enklere å snakke med den nivå 3 avdelingen vil ikke tilhører og samhandle med de enn det til tider er å samhandle med sin egen nivå 3 stab".[42] Det faktum at det for enkelte oppleves som utfordrende å samhandle med den organisasjonen de selv er en del av kan peke i retning av en mindre enhetlig organisasjon med manglende tillit mellom aktørene i hierarkiet. I lys av det instrumentelle perspektivet kan dette for det første innebære at organisasjonen ikke evner å anvende aktørene på en hensiktsmessig måte med tanke på effektiv måloppnåelse. Det kan delvis forklares med at om samhandlingen ikke er optimal, og om avdelingene ikke evner å se organisasjonens beste, vil det kunne ha innvirkning på den enkelte avdelings prestasjoner og Cyberforsvarets totale prestasjoner. For det andre kan dette innebære at forholdet mellom aktørene i liten grad er bygget på rasjonalitet, og ledelsen i mindre grad styrer sine aktører på bakgrunn av rasjonell kalkulasjon hvor informasjon, effektivitet, optimalisering, implementering og design er tatt høyde for.
Uttalelsene kan sies å indikere at organisasjonsstrukturen i Cyberforsvaret ikke er ideell med tanke på hva avdelingene og organisasjonen som helhet presterer. Dersom dette er tilfelle samsvarer det med McKinsey-rapporten hvor det fastslås at IKT-virksomheten i Forsvaret ikke leverer tilfredsstillende resultater.

Variasjoner i prestasjoner mellom personell i ulike posisjoner

Det viser seg også at organisasjonsendringene tidvis har vært påvirket av forholdet mellom ulike posisjoner eller personer;

[41] Respondent #6: Intervju, Jørstadmoen, 06.04.2016
[42] Respondent #5: Intervju, Jørstadmoen, 01.04.2016

> … den røde tråden manglet på hvordan oppdrag har kommet inn i Cyberforsvaret. Hva som er årsaken til det har jeg bare en hypotese om – jeg tror at når det er snakk om operasjoner så er det såpass "hot stuff" så det ønsker alle å ha en bit i. Uavhengig om det har noen merverdi, man ønsker å være i loopen når ting skal deployeres til utlandet eller i større øvelser – at dette ønsker jeg på mitt nivå å ha en bit av. Derfor ble det innviklet noen ganger.[43]

Dette utsagnet tyder på at Cyberforsvaret organisasjon bærer preg av en forhandlingsvariant i det instrumentelle perspektivet. Det kan muligens være sterkt å påstå at organisasjonen er preget av konflikter, maktkamp og politikk, men at den bærer preg av en form for maktkamp og interessehevding forsterkes av uttalelsen over.

4.3.2 Delkonklusjon

Hensikten med dette delkapittelet har vært å besvare forskningsspørsmål 2 og å teste hypotese 2. For å kunne besvare den overordnede problemstillingen har denne faktorens hensikt vært å avdekke om felles forståelse for organisasjonenes oppgaver påvirker de avdelingsvise prestasjonene, og dermed også Cyberforsvarets prestasjoner. I faktoren prestasjon legger studien til grunn det avdelingene gjør, og som fører frem til gode resultater. Avdelingene jeg har undersøkte opererer begge innen konkrete fagområder. Fagområdene kan sies å representere ytterpunkter og dermed bredden i Cyberforsvarets oppdragsportefølje. Man kan muligens ikke forvente at Cyberforsvarets ledelse besitter dyp innsikt i alle fagområder gitt de ulike oppgavene. Man kan imidlertid forvente at nivå 3, som de undersøkte avdelingene sorterer inn under besitter dyp innsikt i egne avdelingers oppgaver. Enkelte funn indikerer derimot manglende kunnskap og forståelse for fagområdene til avdelinger på nivå 4. Når dette innebærer at avdelinger på nivå 4 ikke føler seg integrert kan det i praksis bety at det er manglende forståelse for at avdelingene, uavhengig av nivå, arbeider mot et felles mål. Videre kommer det frem at forholdet mellom nivåene og delvis avdelingene er preget av konflikter og maktkamper, dette indikerer at de ikke arbeider mot et felles mål hvilket kan ha innvirkning på den enkelte avdelings prestasjoner. Dette forholdet antas å påvirke Cyberforsvarets totale prestasjoner. Det faktum at det for enkelte oppleves som utfordrende å samhandle med den organisasjonen de selv er en del av kan peke i retning av en mindre enhetlig organisasjon med manglende tillit mellom aktørene i hierarkiet. Om det er slik at dette skyldes at organisasjonen opererer i tråd med forhandlingsvarianten i det instrumentelle perspektivet vil dette kunne hemme den hierarkiske styringen. Cyberforsvaret kan dermed sies å i mindre grad arbeide mot et felles mål. Funnene indikerer at hypotese 2 kan

[43] Respondent #6: Intervju, Jørstadmoen, 06.04.2016

bekreftes. Empirien tilsier at avdelingene i stor grad gjør det samme som før opprettelsen av Cyberforsvaret og at organisasjonen ikke har klart å etablere en god organisasjonskultur.

4.4 Ansvar

Med utgangspunkt i hypotese 1 og 2 har dette delkapittelet til hensikt å besvare forskningsspørsmål 3; Hvordan forstår avdelingene Cyberforsvarets målbilde?

Empiri som er relevant for ansvar og forskningsspørsmålet sett opp mot problemstillingen

Ansvar forstås på ulike måter. En tradisjonell forståelse for ansvar tilsier at ledere har et relativt altomfattende ansvar, med det utgangspunkt at ledere handler på basis av tillit. I et slikt tilfelle vil forvaltningen av tilliten være kjernen, innenfor et formelt system av over- og underordning. En instrumentell og administrativ forståelse av ansvar vil bære preg av å være mer formell og snever. Den som tildeles et formelt ansvar må redegjøre og rapportere for hvordan ansvaret forvaltes (Christensen et al., 2015, s. 136-137).

I studien anvender jeg begrepet ansvar om det ansvar Cyberforsvaret har tildelt den enkelte avdeling. Implisitt i dette ansvaret legges også myndighet. I intervjuene har jeg forsøkt å avdekke hvordan fordeling av ansvar og myndighet er formalisert og hvordan det praktiseres. I og med at Cyberforsvaret er en organisasjon med et system av over- og underordningen, vil det også være av betydning å avdekke hvordan ledelsen i Cyberforsvaret forvalter tilliten fordelingen av ansvar og myndighet bærer med seg.

Forholdet mellom ansvar og forståelse for organisasjonens oppgaver

Det er noe divergerende svar på hvorvidt ansvar og myndig er tydelig avklart i Cyberforsvaret. Det ble uttalt at dette ikke er tydelig avklart og at dette har medført en del utfordringer internt og eksternt i forhold til aktører de er avhengig av å samhandle med. Noe ansvar og myndighet er avklart og synliggjort i styrende dokumenter, men ikke tilstrekkelig for effektiv måloppnåelse. Det eksemplifiseres med følgende uttalelse; "… Sender frem en forespørsel og får ikke svar".[44] På den ene siden påvirker dette antageligvis arbeidsprosessene internt i avdelingen og produktiviteten antas dermed å bli noe redusert. I så måte kan bruken av avdelingen som et instrument for effektiv måloppnåelse sies å ikke være optimal. På den andre siden kan man anta at om en avdelingen sender frem en forespørsel og ikke får svar påvirker det tilliten til nivåene over. Det kan bety at ledere ikke handler på basis av tillit. I en forhandlingsvariant kan dette

[44] Respondent #1: Intervju, Jørstadmoen, 16.03.2016

forklares med at aktørene ikke har felles mål, interesser eller kunnskaper. Man kan dermed anta at situasjoner som beskrevet over medfører at aktører tilskriver seg egne ansvarsområder og beslutningsmyndighet. Dette viser seg imidlertid å ikke være gjeldende. På oppfølgende spørsmål om enkelte sjefer tar ansvar og tilskriver seg selv myndighet svares; "… tror heller det er motsatt og at man har beslutningsvegring … dersom man ikke er pekt på er det mange som ikke tør ta beslutninger".[45] Denne uttalelsen tyder på at Cyberforsvarets ledelse ikke i tilstrekkelig grad kontrollerer organisasjonens oppgaver. Om ikke ansvar og myndighet er tydelig avklart kan muligens ikke organisasjonen sies å anvende sine avdelinger som instrumenter eller redskaper for effektiv måloppnåelse. Dersom aktører har beslutningsvegring kan det på den ene siden medføre mindre grad av effektivitet. Det kan innebære at om ansvar og myndighet ikke er tydelig avklart og avgjørelser må tas vil dette kunne være en forsinkende faktor. På den andre siden kan det tyde på at ledelsen i mindre grad kontrollerer organisasjonens oppgaver og at et form for vakuum oppstår i enkelte situasjoner.

> …vi har å gjøre med en ny organisasjon og et nytt fagfelt, dette er det utfordrende å håndtere. Måten vi jobber på innebærer håndtering av sensitiv informasjon, der har ikke ansvar og myndighet vært tydelig definert. Dette har ført til at ingen tør å ta beslutninger på noe som helst.[46]

I lys av McKinesy-rapporten kan dette bety at ansvarspulveriseringen og uklarheter i ansvarsforhold gjelder i så vel Cyberforsvaret som i IKT-virksomheten i helhet i forsvarssektoren.

Videre ser det ut til at Cyberforsvaret har visse organisatoriske utfordringer med tanke på den brede oppdragsporteføljen og oppfølging av de ulike fagmiljøene:

> …avdelingen har blitt til nedenfra og opp, vi har definert vårt eget ansvarsområde og fått veldig lite føringer ovenfra. Oppgavene har oppstått nedenfra og blitt en del av Forsvarets oppgaver. Myndighet og ansvar fulgte ikke med, det har ikke vært forankret og det har medført at det har vært vanskelig å få beslutninger, det har vært en kamp.[47]

Det faktum at Cyberforsvaret er en ung organisasjon kan delvis forklare at organisasjonskart, stillingsinstrukser, lover og regler for hvem som skal eller kan gjøre hva ser ut til å være

[45] Respondent #1: Intervju, Jørstadmoen, 16.03.2016
[46] Respondent #2: Intervju, Jørstadmoen, 16.03.2016
[47] Respondent #2: Intervju, Jørstadmoen, 16.03.2016

mangelfullt, eller ikke har kommet helt på plass. Fordeling av ansvar og myndighet i Cyberforsvaret omtales slik:

> … Ansvar og myndighet er ikke tydelig avklart i Cyberforsvaret. Det jobbes med dette og jeg har tro på at det skal bli bedre. På hvilket nivå ulike beslutninger skal fattes og så videre jobbes det med og det kommer til å bli tydeligere i fremtiden … Etter at arbeidet med på hvilket nivå ulike former for myndighet og ansvar skal ligge vil det dermed være delegert til hensiktsmessig nivå.[48]

På den ene siden kan dette indikere at beslutningsregler ikke er utformet og måloppnåelsen blir dermed ikke maksimal. Dette kan innebære begrenset mål-middel forståelse som kan påvirke samsvaret mellom handling og det organisasjonen ønsker å oppnå På den andre siden opererer Cyberforsvaret i et komplekst miljø hvor alternativer og konsekvenser ikke alltid er like synlige. Dette innebærer at veien til målet ikke alltid er like klar og indikerer at organisasjonen baserer seg på begrenset rasjonalitet med god nok måloppnåelse..

Om vi ser tilbake på uttalelsen om at avdelingen har blitt til nedenfra og at eksempelvis beslutninger har vært en kamp tyder mye på at organisasjonen bærer preg av forhandlingsvarianten i det instrumentelle perspektivet. Med andre ord tyder disse forholdene på at mangelfull fordeling av ansvar kan være medvirkende til redusert tillit til ledelsen.
Videre i intervjuene snakket vi om hvordan avdelingene forstår Cyberforsvarets målbilde. Svarene fra intervjuobjektene var svært divergerende. "…avdelingen løser oppdrag med utgangspunkt i Cyberforsvaret målbilde, og de oppdragene avdelingen løser er av betydning for at Cyberforsvaret skal oppnå sitt målbilde".[49] Dette svaret kan sies å indikere at Cyberforsvarets målbilde er kjent og at avdelingene løser sine oppgaver i tråd med dette. Det er imidlertid flere uttalelser som tyder på at Cyberforsvarets målbilde ikke er kjent i organisasjonen:

> … vi mangler felles målbilde og intensjon fra toppen og nedover som gir ledestjerne å gå etter. Hvorfor skal vi gå i samme retning, hva skal vi samarbeide om og så videre. Vet ikke hva vi skal samarbeide om, lite forståelse ned på nivå med tanke på hvorfor vi skal samarbeide … det å få målbilde og intensjon fra sjefen som gjennomsyrer hvert nivå i avdelingen er viktig. Jeg savner det i dag.[50]

Vi ser altså at respondentene har svært ulik oppfattelse av Cyberforsvarets målbilde. Dette tyder på det ikke er formidlet ned i organisasjonen på en komplementær måte. I praksis betyr det at det

[48] Respondent #3: Intervju, Jørstadmoen, 17.03.2016
[49] Respondent #3: Intervju, Jørstadmoen, 17.03.2016
[50] Respondent #1: Intervju, Jørstadmoen, 16.03.2016

er like lite sannsynlig at det er allment kjent i organisasjonen som at det er det. Denne påstanden kan jeg underbygge med følgende uttalelse;

> …Det vet jeg ikke … Det er for mange som har forskjellig målbilde for hva som er viktig for den enkelte avdeling kontra det at vi er en avdeling som skal nå det samme målet. Jeg pleier å si at vi er et flerhodet troll, i den forstand at vi har så mange oppgaver som skal løses i de forskjellige avdelingene som ikke har en felles grunnplattform for enheten vi jobber i. Da tenker jeg ikke vår avdeling, eller andre avdelinger i samme organisasjon, da tenker jeg at vi ikke har den felles bærebjelken som er felles for alle avdelingene i nivå 3 avdelingen.[51]

Med andre ord kan dette bety at de ulike avdelingene har ulike målbilder og at felles målbilde i mindre grad er kjent i hele organisasjonen.

Variasjoner i ansvar mellom, og på tvers av nivåene

Som jeg har vært inne på tidligere fremkommer det av intervjuene at ansvar og myndighet i varierende grad ser ut til å være tydelig fordelt. I lys av en hierarkisk variant bør dette være tydelig avklart mellom nivåene. En forventning må kunne være at avdelinger som tilhører samme nivå 3 avdeling har felles mål og interesser. I lys av forhandlingsvarianten vil organisasjonen i mindre grad kontrollerer egne avdelingers oppgaver. Det forventes med andre ord at avdelingene arbeider selvstendig og løser oppgaver formålsrasjonelt på grunnlag av avdelingens egeninteresse. Følgende uttalelse tilsier at fordeling og praktisering av ansvar og myndighet kan sies å være mangelfull**;**

> … det er veldig enkelt på nivå 4, her har man tillit, en intensjon å lede ut ifra, veldig enkelt, min oppriktige mening er at nivå 3 knapt nok vet hva vår avdeling driver med og bryr seg lite om det. Den skarpeste avdelingen i Cyberforsvaret blir særdeles lite fulgt opp. Det er knapt nok så de vet hvor vi har personell i internasjonal operasjoner i dag, faktisk. Så det er nok en del vanskelig prosesser.[52]

Dersom det faktum at personell på ledelsesnivå i en nivå 4 avdelingen opplever forholdet til overordnet avdeling på denne måten peker det i retning av mangelfull tillit til ledelsen. Dessuten tyder dette på at samhandlingen mellom nivåene ikke virker å være optimal. Derimot kan det at intervjuobjektet sier man har tillit og en intensjon å lede ut i fra på nivå 4 tyde på at ledelsen i avdelingen tar ansvar for egne oppgaver, og at de i mangel på tillit til nivået over evner å beholde tilliten internt i avdelingen.

[51] Respondent #6: Intervju, Jørstadmoen, 06.04.2016
[52] Respondent #5: Intervju, Jørstadmoen, 01.04.2016

Ut fra forventningen til en hierarkisk variant ser det ikke ut til at nivå 3 har kontroll over oppgavene nivå 4 skal løse. Uttalelsen over tyder på at overordnet avdeling i liten grad legger føringer, fordeler oppgaver, besitter dyp innsikt i virksomhetens mål og at de har oversikt over tilgjengelige virkemidler og konsekvensene av disse. I så måte kan ikke avdelingen sies å bli anvendt som et instrument eller et redskap for effektiv måloppnåelse. Eventuell effektiv måloppnåelse kan i alle fall ikke årsaksforklares med samhandling mellom nivåene. Ut fra forventningen i forhandlingsvarianten ser vi imidlertid at de imøtekommes med tanke på liten grad av samhandling mellom nivå 3 og 4.

Samlet sett kan altså fordeling av ansvar og myndighet sies å ikke være tydelige avklart:

> …Nei, årsaken til det er at i noen situasjoner mener jeg at som nivå 4 sjef har jeg ansvar for en gitt oppgave eller er tillagt en viss myndighet. Jeg blir overrasket over at det tydeligvis er andre som har en annen oppfatning og i andre situasjoner så forventer jeg at nivåene over tar tak og løser oppgaven – hvor jeg opplever at de ikke gjør det. Kan være min tolkning av den, det er ikke nødvendigvis noe feil med organisasjonen, men noen ganger føler jeg nivåene over styrer i detaljer som helt klart er mitt domene … Det er rom for å bli tydeligere på hva de ulike nivåenes roller, ansvar og myndighet er.[53]

Dette kan bety at Cyberforsvaret ikke har klart å etablere en god kultur for samhandling mellom nivåene. Det kan forklares med at organisasjonen en ung og fremdeles i sine formative år. De ulike nivåene trenger tid for blir optimalt tilpasset for effektiv måloppnåelse. En annen forklaring kan være at organisasjonen er sterkt preget av arv fra gammel organisasjonsstruktur, at aktørene i mindre grad evner å tilpasse seg nye oppgaver og at samhandling mellom nivåene ikke prioriteres. Dette kan på den ene siden skyldes svært ulike fagområder og at nivåene ikke utfyller hverandre kompetansemessig. På den andre siden kan dette forklares i lys av forhandlingsvarianten hvor avdelingene sees på som koalisjoner hvor hver av aktørene handler formålsrasjonelt på grunnlag av avdelingens egeninteresse. I denne sammenheng ser egeninteressen ut til å være divergerende mellom nivåene. I så måte bruker ikke overordnet nivå underlagte avdelinger som redskaper eller instrumenter for effektiv måloppnåelse.

Jeg har vært inne på divergerende svar på hvorvidt Cyberforsvarets målbilde er kjent eller ikke. Med tanke på fordeling av ansvar og myndighet ser målbildet ut til å være av betydning for samhandling mellom og på tvers av nivåene;

[53] Respondent #4: Intervju, Jørstadmoen, 29.03.2016

> … ledergruppen i avdelingen er klar over hva vi skal bidra med og hva vi skal oppnå på vegne av Forsvaret. Vi vet hva vi skal bidra med … Kulturen, budskapet om hva vi skal oppnå, det blir formidlet for dårlig fra sjefsnivået på nivå 3 og ned til ansatte i organisasjonen, der burde det vært noe som blir presentert med mer "svung" som fenger og treffer oss som jobber her … å vise noe plansjer og prate løst er lett, men det når ikke målgruppen … Der har man ikke lykkes.[54]

Dette indikerer på den ene siden at Cyberforsvarets målbilde er formidlet fra nivå 3 og ned til nivå 4. På den andre siden indikerer det imidlertid at det er en brist mellom nivå 3 og avdelinger på nivå 4 i sin helhet. Dette kan implisere at det er personavhengig på ledelsesnivå i nivå 4 avdelingene hvordan den enkelte løser dette. Det er i så måte ikke i tråd med den hierarkiske varianten i det instrumentelle perspektivet som tilsier at forventningene til de som innehar rollene eller posisjonene er upersonlige, og normene for hva som skal gjøres er dermed uavhengig av de personene som innehar posisjonene. Samtidig kan man si at nivå 3 ikke fyller definisjonskarakteristikkene for en rasjonell organisasjon med formell struktur da aktører ikke styres på bakgrunn av rasjonell kalkulasjon hvor informasjon, effektivitet, optimalisering, implementering og design er tatt høyde for. Hvis nivå 3 ikke evner å informere underenhetene om noe så sentralt som målbilde tilflyter ikke essensiell informasjon organisasjonsmedlemmene. Mangelen på informasjon vil kunne påvirke effektiviteten, optimaliseringen og implementering i organisasjonen.

Variasjoner i ansvar mellom personell i ulike posisjoner

Den manglende tilliten til personer eller posisjoner på nivåene over de undersøkte avdelingene kan blant annet skyldes forhold som arv fra gammel organisasjonsstruktur.

> …På lavere nivå snakker vi sammen, hjelper hverandre der det er mulig og kampen mellom CTO og CKT den er vanskeligere … Det som er viktig å spørre seg om er om vi er til for nivå 3 eller er nivå 3 til for oss. Min mening, oppfattelse er at vi er til for nivå 3 … Staber i Cyberforsvaret gir ikke merverdi, det er en knallhard påstand, men den står jeg inne for.[55]

Denne uttalelsen kan analyseres på flere måter. For det første kan den sees i lys av forhandlingsvarianten hvor opprettelsen av Cyberforsvaret, og det faktum at CTO og CKT har arvet avdelinger synes å være delvis basert på tilfeldige resultater av maktkamper. For det andre kan det innebære at nivå 3 avdelingene fremstår som overflødige. Dette samsvarer i så fall med områder jeg har vært inne på tidligere hvor nivå 3 avdelingene kan sies å være avdelinger

[54] Respondent #5: Intervju, Jørstadmoen, 01.04.2016
[55] Respondent #5: Intervju, Jørstadmoen, 01.04.2016

respondentene ikke ønsker å identifisere seg meg, eller føler tilhørighet til. Det har også vist seg i enkelte situasjoner forbigås nivå 3 i utførelsen av oppdrag. For det tredje kan dette innebære at de personkonflikter og den posisjoneringen, som beskrives i intervjuene, medføre en dysfunksjonell organisasjonsstruktur hvor den hierarkiske organisasjonen fremstår som lite enhetlig og homogen. Dette kan sies å medvirke til begrenset samhandlingen mellom nivåene og at måloppnåelsen påvirkes av dette. Uttalelser som at organisasjonsstrukturen er dysfunksjonell kan muligens være en medvirkende faktor til at målbilde i mer eller mindre grad er kjent blant intervjuobjektene. Til tross for at respondentene er på ledelsesnivå i avdelingene kan det for det første se ut til at kjennskap og forståelse for Cyberforsvarets målbilde er påvirket at den enkelte respondents posisjon. For det andre kan forståelsen trolig ha med den enkeltes engasjement i en større sammenheng å gjøre. Om dette stemmer kan man på den ene siden si at Cyberforsvarets ledelse i for liten grad har evnet å engasjere og formidle målbilde ned i organisasjonen. På den andre siden kan det bety at Cyberforsvarets aktører har så forskjellige oppgaver at de er seg selv nærmest, utfører sine oppgaver og i mindre grad er avhengig av forståelse for hele organisasjonenes oppgaver.

… Cyberforsvaret består av en del avdelinger som i seg selv er sterke enheter, kanskje selvstyrte enheter som har fått en stab over som ikke helt har den forankringen ned i organisasjonen som man kanskje kunne forventet. Cyberstaben blir noe litt eget, litt på siden eller der borte.[56]

Dette kan ha innvirkning på den totale måloppnåelse da heterogeniteten medfører liten grad av samhandling mellom nivå 3 og 4.

4.4.2 Delkonklusjon

Hensikten med dette delkapittelet har vært å besvare forskningsspørsmål 3 og å teste hypotese 1 og 2. For å kunne besvare den overordnede problemstillingen har denne faktorens hensikt vært å avdekke hvordan avdelingene forstår Cyberforsvarets målbilde.

Det fremkommer, i samtlige intervjuer, at ansvar og myndighet ikke er tydelig avklart i Cyberforsvaret. Det ser ut til at der hvor ansvar og myndighet er avklart er det manglende grad av lojalitet når beslutninger er fattet. Dette kommer til syne ved at det kjøres omkamper og at nivå 3 i enkelte situasjoner blander seg inn i underliggende avdelingers domene. I tilfeller hvor ansvar og myndighet ikke er avklart indikerer funnene en form for beslutningsvegring. Som jeg har vært innen på tidligere er ikke samhandlingen mellom avdelingene optimal. Dette kan

[56] Respondent #2: Intervju, Jørstadmoen, 16.03.2014

årsaksforklare med blant annet organisasjonsstrukturen. I forrige delkapittel siterte jeg et intervjuobjekt som sier kommandolinjene impliserer at organisasjonen ikke er satt opp for suksess, men for feil. I så måte kan jeg hevde at organisasjonsstrukturen ikke tilsier at samhandling mellom avdelingene er nødvendig. Samtlige intervjuobjekter omtaler kulturen innad i egen avdeling som god, det er imidlertid lite som tyder på at Cyberforsvaret har klart å etablere en egen organisasjonskultur. Det ser ut til at organisasjonen er sterkt preget av arv fra gammel organisasjonsstruktur og at dette har vanskeliggjort endring. Funn omkring hvorvidt Cyberforsvarets målbilde er kjent eller ikke er divergerende. Til tross for at samtlige intervjuobjekter er på ledelsesnivå i avdelingene varierer uttalelsene om Cyberforsvarets målbilde fra at de ikke er kjent med det, eller vet om det eksisterer til at målbildet er kjent. Dette er et tydelig tegn på at Cyberforsvarets målbilde ikke er formidlet ned i organisasjonen på en tilfredsstillende måte. Hvorvidt målbilde er kjent eller ikke indikerer at organisasjonen i helhet er mindre kjent Cyberforsvarets målbilde. Dette kan innebære begrenset mål-middel forståelse som kan påvirke samsvaret mellom handling og det organisasjonen ønsker å oppnå. Empirien indikerer at hypotese 1 og 2 også kan bekreftes med hensyns til denne faktoren. Dataene indikerer at organisasjonsstrukturen er dysfunksjonell, dette ser ut til å innvirke på fordeling og praktisering av ansvar og myndighet og begrenser dermed samhandlingen. Avdelingskulturen ser ut til å stå sterkt, det er imidlertid lite som tyder på at Cyberforsvaret har klart å etablere en enhetlig organisasjonskultur. Mangelen på en enhetlig organisasjonskultur ser ut til å være en medvirkende faktor på manglende lojalitet når beslutninger er fattet og beslutningsvegring når ansvar og myndighet ikke er tydelig avklart.

5 Konklusjon

Dette kapittelet har til hensikt å besvare problemstillingen med bakgrunn i anvendt forskningslitteratur og innsamlet empiri. Slik kommer jeg frem til denne studiens endelige konklusjon. Videre vurderes styrker og svakheter ved forskningen, og til slutt mulige utviklingstrekk og videre forskning.

5.1 En endelig konklusjon

Jeg har i denne studien vist at samhandling forekommer mellom aktører og nivåer der hvor man er gjensidig avhengig av hverandre for å utføre konkrete oppgaver. Funnene i studien indikerer at forståelse for organisasjonens oppgaver ikke er felles. Jeg har benyttet to former for kvalitativ metode. Den ene er dokumentstudier hvor jeg har beskrevet Cyberforsvarets organisasjon og oppgaver med utgangspunkt i tilgjengelig ugradert kildemateriale. Den andre er semi-strukturerte intervjuer hvor jeg har innhentet empiri med fokus på faktorene for å kunne besvare forskningsspørsmålene. Med utgangspunkt i Cyberforsvaret som organisasjon har jeg analysert og drøftet funnene i lys av det instrumentelle perspektivet.

For å sette studien i en større kontekst har jeg benyttet to kilder. Den ene er hva daværende forsvarsminister Espen Barth Eide uttalte under etableringen av Cyberforsvaret . Den andre er utdrag av McKinsey-rapporten hvor det blant annet fastslås at IKT-virksomheten i Forsvaret ikke leverer tilfredsstillende resultater, og at sektoren har valgt en uegnet organisering av IKT (McKinsey & Company, 2015, s. 51). Den første av disse to kildene er fra Cyberforsvarets etablering og kan sies å representere den opprinnelige intensjonene med Cyberforsvaret. Den andre er et resultat av en uavhengig vurdering gjort med den hensikt å identifisere, kvantifisere og beskrive potensiale for ytterligere modernisering og effektivisering av utvalgte forvaltningsområder og funksjoner i forsvarssektoren (McKinsey & Company, 2015, s. 7). Med dette som bakteppe har jeg i intervjuene fokusert på intern samhandling i Cyberforsvaret og om avdelingene har felles forståelse for organisasjonens oppgaver. Det har imidlertid ikke vært mulig å fullstendig utelate ekstern samhandling, da avdelingene jeg har undersøkt samhandler med eksterne for å løse sine oppgaver. Dette har vært et sentralt aspekt i samtlige intervjuer.

Ved analyse av data som er innhentet gjennom hovedsakelig semi-strukturerte intervjuer og dokumentstudier, har jeg kommet frem til et svar på problemstillingen for denne studien. Konklusjonen på problemstillingen er at Cyberforsvarets avdelinger ikke ser ut til å ha felles forståelse for organisasjonens oppgaver. Dette skyldes ulike forhold innhentingen av empiri har avdekket.

Samhandling i Cyberforsvaret foregår tilsynelatende kun mellom aktører som er gjensidig avhengig av hverandre. Data fra intervjuene tyder på at organisasjonsstrukturen ikke er optimal med tanke på effektiv måloppnåelse. Dette funnet kan sies å støtte forhold McKinsey-rapporten påpeker. Organisasjonsstrukturen legger heller ikke til rette for samhandling mellom avdelingene, uavhengig av nivå. Mye tyder på at den samhandlingen som foregår er resultater av lokale initiativer på lavere nivå. Disse initiativene ser ut til å være en konsekvens av nødvendigheten av samhandling for å løse konkrete oppgaver. Videre indikerer funn at Cyberforsvarets ledelse og avdelingene på nivå tre ikke utnytter de ulike avdelingene optimalt som instrumenter eller redskaper for effektiv måloppnåelse. Funnene indikerer at forholdet mellom avdelingen hviler på tillit når avdelingene er gjensidig avhengig av hverandre, og utfyller og utveksler kompetanse. Dette ser imidlertid ut til å være basert på personlig kjennskap mellom enkeltindivider og er gjeldende der hvor avdelingene har faglig forankring og tilknytning. Funnene indikerer ellers begrenset tillit innad i organisasjonen, uttalelser tyder på at dette skyldes uenigheter på nivåene over.

Om tilhørighet tilsier dataene at tilhørigheten mellom avdelingene gjør seg gjeldende i de tilfeller hvor de er gjensidig avhengig av hverandre. Det er imidlertid få avdelinger i Cyberforsvaret de undersøkte avdelingene er gjensidig avhengig av. Dette kan indikere at gjensidig tilhørighet og avhengighet ikke er gjennomgående i Cyberforsvarets organisasjon. Samlet sett uttrykker intervjuobjektene sterk tilhørighet til egen avdeling. Derimot tilsier funnene at det er svært begrenset tilhørighet til nivå 3. Flertallet av intervjuobjektene uttrykker at som en konsekvens av oppgavene avdelingen utfører anser de seg som en del av en større helhet, og de identifiserer seg derfor delvis med Cyberforsvaret. Dette indikerer at Cyberforsvarets organisasjon består av selvstendige enheter som operer uavhengig av organisasjonen, kun avhengig av enkelte interne og eksterne aktører. Dataene tilsier at Cyberforsvaret ikke har klart å etablere en enhetlig organisasjonskultur, imidlertid viser det seg at avdelingskulturen er sterk og hensiktsmessig med tanke på avdelingsvis måloppnåelse.

Den sterke tilhørigheten til egen avdelingen kan ha positiv betydning for avdelingens prestasjoner. Dette kan i sum påvirke Cyberforsvarets prestasjoner i sin helhet. Men prestasjonene kan ikke sies å være enhetlig. Mye tyder på at Cyberforsvaret er sterkt preget av arv fra gammel organisasjonsstruktur. Uttalelser fra enkelte intervjuobjekter peker i retning av at flere avdelinger gjør det samme som før opprettelsen av Cyberforsvaret. Organisasjonsstrukturen omtales som dysfunksjonell, og at den og personkonflikter på ledelsesnivå har virket lammende på organisasjonen. Dette indikerer at organisasjonen i begrenset grad er optimalt tilpasset for å effektiv måloppnåelse. Her kan man trekke paralleller og se likheter mellom Cyberforsvaret som en av Forsvarets IKT-enheter og hva som fastslås i McKinsey-rapporten.

Dataene tilsier at fordeling og praktisering av ansvar og myndighet ikke er tydelig avklart. Imidlertid indikerer funnene at i situasjoner hvor ansvar og myndighet er avklart bærer organisasjonen preg av manglende lojalitet til beslutninger når de er fattet. I situasjoner hvor ansvar og myndighet ikke er avklart indikerer funnene en form for beslutningsvegring i organisasjonen. Det fremkommer tydelig at et omforent felles målbilde ikke eksisterer. Kunnskapen om Cyberforsvaret målbilde er ser ut til å være manglende og synes å være basert på det enkelte intervjuobjekts stilling og egeninteresse. Mye tyder på at Cyberforsvarets ledelse ikke har evnet å formidle målbildet nedover i organisasjonen. Dette indikerer at Cyberforsvaret som organisasjon mangler en felles forankring for de oppgaver organisasjonen skal utføre.

Samlet sett indikerer funnene at Cyberforsvaret står overfor utfordringer forbundet med manglende felles forståelse for organisasjonens oppgaver. Dataene indikerer at avdelingene, isolert sett, presterer godt og utfører sine oppgaver hvilket impliserer måloppnåelse i Cyberforsvaret. Gitt den komplekse oppdragsporteføljen og manglende beslutningsregler kan det imidlertid se ut til at Cyberforsvaret baserer seg på begrenset rasjonalitet og dermed ikke har maksimal måloppnåelse. Funnene tyder ikke på at organisasjonene presterer i fellesskap. Hvorvidt måloppnåelsen kan sies å være effektiv kan det stille spørsmål ved gitt den manglende forståelsen for hele organisasjonens oppgaver. Det fremkommer av intervjuene at flere av respondentene ser på organisasjonsstrukturen som dysfunksjonell, utfordringer på nivået over og mellom nivåene preger samhandlingen. Dette påvirker tilhørigheten mellom person og avdeling og mellom avdelingene i Cyberforsvaret. Ansvar og myndighet er ikke tydelig avklart, dette impliserer på den ene siden mindre lojalitet til beslutninger når de er fattet og på den andre siden

en form for beslutningsvegring. Funnene indikerer en dysfunksjonell organisasjonsstruktur og dette ser ut til å være en medvirkende årsak til at forståelsen for organisasjonens oppgaver ikke er felles.

5.2 Styrker og begrensninger ved forskningen

Denne studien har ulike styrker og begrensninger som må tas i betraktning ved tolkningen av funnene. For det første kan det relativt begrensede antall respondenter i studien begrense muligheten til å generalisere. Størrelsen på utvalget kan imidlertid være tilstrekkelig stort til å identifisere årsakssammenhenger. Hensikten med intervjuene har vært å få kunnskap om interne forhold i Cyberforsvaret. For å få et pålitelig analysegrunnlag har jeg intervjuet seks respondenter på ledelsesnivå i to av tre operative avdelinger på nivå 4. Antallet respondenter kunne vært flere, men jeg vurderer antallet tilstrekkelig gitt studiens formål (Ringdal, 2013, s. 242). Fremgangsmåten, ved bruk av dokumentstudier og semi-strukturerte intervjuer, har gitt en fleksibilitet som har muliggjort å oppnå tilstrekkelig dybde for å belyse forskningsspørsmålene på en hensiktsmessig måte. Samtidig har tilgang til graderte dokumenter gjort det mulig å sette seg inn i slik som Cyberforsvarets, CTOs og CKTs virksomhetsplan, Forsvarssjefens direktiv for operative krav og andre styrende dokumenter for å kunne verifisere informasjon som fremkom under intervjuene.

Denne utredningen har to store svakheter. Den største er at jeg kun har intervjuet personell fra to avdelinger på nivå 4. Cyberforsvaret er en organisasjon bestående av mange avdelinger, utvalget kan være for smalt og snevert til å kunne gi et representativt svar på problemstillingen. Det har derfor kun vært mulig å indikere om forståelsen for organisasjonens oppgaver er felles. I tillegg har jeg kun intervjuet seks respondenter, det lave antallet har vært nødvendig gitt studiens begrensning i tid og omfang. Et større antall respondenter ville kunnet gi et bedre analysegrunnlag. Den andre svakheten er lav ekstern validitet. Kvalitativ forskningsmetode er ikke er ikke egnet til generalisering utover det som studeres (Creswell, 2014, s. 203-204). Funnene kan ikke generaliseres til andre enn de jeg faktisk har undersøkt (Jacobsen, 2015, s. 237). Funnene kan imidlertid være relevante med hensyn til å øke kunnskap og bevissthet om de utfordringer opprettelsen av en ny organisasjon, som er tuftet på gammel organisasjonsstruktur, innebærer.

5.3 Mulige utviklingstrekk og videre forskning

Jeg har i denne studien belyst implikasjoner ved opprettelsen av Cyberforsvaret og enkelte utfordringer i organisasjonens formative år. Utviklingstrekkene i Cyberforsvaret kan være etableringen av organisasjonen og oppgavene som utføres i et stadig mer aktuelt domene. Enkelte forhold som arv fra gammel organisasjonsstruktur og den komplekse oppdragsporteføljen ser ut til å være av betydning for mangelen på felles forståelse for organisasjonens oppgaver. Det faktum at organisasjonen er ung og arbeidsoppgavene i stor grad befinner seg i et forholdsvis nytt domene, som cyberdomenet er, innebærer nødvendigvis en viss prøving og feiling i de formative årene. Det kan imidlertid være relevant å forske videre på om det er hensiktsmessig at Cyberforsvarets oppgaver favner så bredt som de gjør, og om en annen organisasjonsstruktur er mer hensiktsmessig. I det legger jeg at drift og vedlikehold av eksempelvis sensorer og systemer ikke nødvendigvis bør være en del av en organisasjons oppgaver som skal drive med cyberkrigføring.

6 Litteraturliste

Berg, O. T. (2014). Organisasjonsteori. *Store norske leksikon*. fra https://snl.no/organisasjonsteori

Christensen, T., Egeberg, M., Lægreid, P., Roness, P. G., & Røvik, K. A. (2015). *Organisasjonsteori for offentlig sektor*. Oslo: Universitetsforlaget.

Christensen, T., & Lægreid, P. (2006). *The Whole-of-Government Approach - Regulation, Performance, and Public-Sector Reform*. Paper presented at the "A Performing Public Sector: The Second Transatlantic Dialogue" - Workshop 2 - Performance of Regulation and Regulation of Performace, Leuven June 1-3 2006. https://bora.uib.no/handle/1956/1893

Christensen, T., Lægreid, P., Roness, P. G., & Røvik, K. A. (2009). *Organisasjonsteori for offentlig sektor*. Oslo: Universitetsforlaget.

Creswell, J. W. (2014). *Research Design, Qualitative, Quantitative, and Mixed Methods Approaches* (Vol. 4th edition). California: SAGE.

Den nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora. (2005). Forskningsetiske retningslinjer for samfunnsvitenskap, humaniora, juss og teologi. Hentet 20.04, 2016, fra https://www.etikkom.no/globalassets/documents/publikasjoner-som-pdf/forskningsetiske-retningslinjer-for-samfunnsvitenskap-humaniora-juss-og-teologi-2006.pdf

Eriksson-Zetterquist, U., Kalling, T., Styhre, A., & Woll, K. (2014). *Organisasjonsteori*. Cappelen Damm Akademisk.

Flyvbjerg, B. (2006). Five Misunderstandings about Case-Study Research. *Qualitative Inquiry, vol. 12*(no. 2), 219-245.

Folgerø, I. S. (2000). *Samhandling på arbeidsplassen - fornøyde kunder, klienter og kolleger*. Oslo: Gyldendal Akademisk AS.

Forsvaret. (2015). Forsvarets årsrapport 2014 *Verden i endring* Hentet fra https://forsvaret.no/fakta_/ForsvaretDocuments/Forsvarets Aarsrapport 2014.pdf

Forsvaret. (2016). Cyberforsvaret. Hentet 23.01, 2016, fra https://forsvaret.no/cyberforsvaret

Forsvarsdepartementet. (2012). Cyberforsvaret offisielt etablert i dag. fra https://www.regjeringen.no/no/aktuelt/cyber/id699271/

Forsvarsstaben. (2010). *Vedlegg C til Direktiv for virksomhets- og økonomistyring i Forsvaret (DIVØ)*. Oslo: Forsvaret.

Forsvarsstaben. (2014). Forsvarets fellesoperative doktrine. fra https://brage.bibsys.no/xmlui/bitstream/id/317149/FFOD 2014.pdf

Forsvarsstaben. (2016). Forsvarets kommunikasjonsplan 2016. Oslo: Forsvaret.

Gundersen, D. (2009). Prestasjon. *Store norske leksikon*. fra https://snl.no/prestasjon

Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser?* Oslo: Cappelen Damm.

Johnsen, B. H. (Red.). (2005). *Operativ psykologi*. Bergen: Fagbokforlaget.

Johnsen, R. (2013). Cyberkrigføring og Forsvarets operative evne. *Internasjonal Politikk, 21*(02/2013), 221-228.

Knudsen, H., & Flåten, B.-T. (2015). *Strategisk ledelse*. Oslo: Cappelen Damm AS.

Malnes, R. (2012). *Kunsten å begrunne*. Oslo: Gyldendal Norsk Forlag.

McKinsey & Company. (2015). Modernisering og effektivisering av stabs-, støtte- og forvaltningsfunksjoner i forsvarssektoren Hentet fra https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/rapporter-og-regelverk/150317-modernisering-og-effektivisering-av-forsvarssektoren_nyversjon.pdf

Meld. St. 14. (2012-2013). *Kompetanse for en ny tid*. Oslo: Forsvarsdepartementet.
Prop. 73 S. (2011-2012). *Et forsvar for vår tid*. Oslo: Forsvardepartementet Hentet fra https://www.regjeringen.no/no/dokumenter/prop-73-s-20112012/id676029/?ch=1.
Repstad, P. (2004). *Mellom nærhet og distanse* (4 utg.). Oslo: Universitetsforlaget.
Ringdal, K. (2013). *Enhet og mangfold*. Bergen: Fagbokforlaget.
Røvik, K. A. (2007). *Trender og translasjoner : ideer som former det 21. århundrets organisasjon*. Oslo: Universitetsforlaget.
Scott, W. R., & Davis, G. F. (2003). *Organizations and Organizing, Rational, Natural, and Open System Perspectives*. Upper Saddle River, N.J.: Pearson Prentice Hall.
Torgersen, G.-E., & Steiro, T. J. (2009). *Ledelse, samhandling og opplæring i fleksible organisasjoner*. Stjørdal: Læringsforlaget.
Yin, R. K. (2012). A (very) brief refresher on the case study method. *Applications of Case Study Research*, 3-20.

Vedlegg A: Forkortelser

ATJ	- Arkivtjenesten
BKI	- Avdeling for beskyttelse av kritisk infrastruktur
CIS TG	- Communication Information Systems Task Group
CKT	- Cyberforsvarets kompetanse- og transformasjonsavdeling
CTO	- Cyberforsvarets avdeling for cybertjenester og operasjoner
CYFOR	- Cyberforsvaret
DVU	- Avdeling for drift og videreutvikling
FAS	- Forsvarets alarmsentral
FIH	- Forsvarets ingeniørhøgskole
FK KKIS	- Forsvarets kompetansesenter for kommando og kontroll- informasjonssystemer
FSP	- Forsvarets sikre plattformer
HR	- Human Resources
HRM	- Human Resource Management
INI	- Informasjonsinfrastruktur
MDM	- Master Data Management
MKS	- Meldingskontroll senter
NbF	- Nettverksbasert forsvar
NK CTO	-Nestkommanderende Cyberforsvarets avdeling for cybertjenester og operasjoner
NKS	. Nettkontrollsenter
NK/STSJ	- Nestkommanderende/stabssjef
NOBLE	- Norwegian Battle Lab & Experimentation
NSM	- Nasjonal sikkerhetsmyndighet
SB SKV	- Sambandsskvadron
Sj CKT	- Sjef Cyberforsvarets kompetanse- og transformasjonsavdeling
Sj CTO	- Sjef Cyberforsvarets avdeling for cybertjenester og operasjoner
Stabsavd	- Stabsavdeling
TDL	- Taktisk datalink-skvadron

Vedlegg B: Informasjon om forskningsprosjekt

Forespørsel om å delta i forskningsprosjektet:
"Samhandling i Cyberforsvaret"

Cyberforsvaret ble etablert 18.september 2012. Det er en videreføring av Forsvarets informasjonsinfrastruktur med stab på Jørstadmoen. Militære operasjoner i det digitale rom har både beskyttende, etterretningsmessige og offensive siktemål. Dette har blitt en tilleggsdimensjon ved militære operasjoner og dermed et nytt krigføringsområde hvor både evnen til defensive og offensive operasjoner vil kunne være avgjørende i fremtidige konflikter. Denne studien vil fokusere på samhandling i Cyberforsvaret og søker å besvare følgende problemstilling; *Har Cyberforsvarets avdelinger en felles forståelse for organisasjonens oppgaver?*

Jeg er student ved Forsvarets høgskole – Masterstudiet. Denne undersøkelsen gjennomføres for å fremskaffe informasjon til bruk i min masteroppgave. Jeg ønsker derfor å intervjue inntil 6 personer som har kunnskaper om Cyberforsvarets oppgaver.

Spørsmålene vil omhandle dine erfaringer og opplevelser om forståelsen av Cyberforsvarets oppgaver i CTO og CKT, representert ved avdelingene BKI og CIS TG. I oppgaven vil jeg forsøke å finne viktige sammenhenger mellom organisasjonens oppgaver og avdelingenes forståelse av de.
Det er frivillig å stille til intervju og det er muligheter for å trekke seg underveis uten at det er nødvendig å begrunne dette. Dersom du trekker deg vil alle innsamlede data fra deg bli anonymisert. Opplysningene vil bli behandlet konfidensielt, og ingen enkeltpersoner vil kunne gjenkjennes i den ferdige oppgaven. Opplysningene anonymiseres når oppgaven er ferdig, innen utgangen av 2016. Eventuelle personopplysninger sladdes fra lydopptakene og transkripsjonen.

Undersøkelsen er finansiert av Forsvarets høgskole. Sjef CIST TG og sjef BKI er informert om undersøkelsen og de har gitt sin tillatelse til å gjennomføre intervjuer i avdelingene.

Viser til telefonsamtale og ber deg bekrefte at du har sagt deg villig til å la deg intervjue
Dersom du er villig til å la deg intervjue ber jeg deg om å gi meg tilbakemelding på e-post om dette. Svar gjerne på sivil e-post da jeg ikke har daglig tilgang til FISBasis. Jeg tar deretter kontakt for å avtale tidspunkt for intervjuet.

Hvis det er noe du lurer på kan du ringe meg på 40031225, eller sende mail til nythun@me.com.
Du kan også kontakte min veileder Hanne Eggen Røislien i Cyberforsvaret pr mail; hanne.roislien@gmail.com eller på telefon 95792828.

Studien er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste A/S.

Vennlig hilsen
Silje Nythun
Student Masterstudiet, Forsvarets høgskole

Vedlegg C: Intervjuguide

Respondentene er offiserer som arbeider på ledelsesnivå i CIS TG og BKI, henholdsvis i CKT og CTO i Cyberforsvaret.

Informasjon til respondentene
Bakgrunnen for denne undersøkelsen er masteroppgaven jeg skriver ved Forsvarets høgskole. Hensikten er å finne ut om Cyberforsvarets avdelinger har en felles forståelse for organisasjonens oppgaver.

- Du kan velge å ikke svare på spørsmål som du enten ikke har konkrete opplysninger om eller som du av andre grunner ikke ønsker å besvare.
- Du står fritt til å beskrive de forhold du mener er viktige. Dersom du har utfyllende kommentarer er det ikke nødvendig at du begrenser deg til kun å besvare spørsmålene jeg stiller under intervjuet.
- Samtalen vil ha en varighet på en til en og en halv time.

Samtykke
Forskningsetiske retningslinjer i Norge bygger på tre krav som regulerer forholdet mellom forsker og dem det forskes på. Disse kravene er informert samtykke, krav på privatliv og krav på å bli korrekt gjengitt. Dette skal beskytte respondenten mot uetisk bruk av den informasjonen som fremkommer.

Det er derfor nødvendig å innhente respondentenes samtykke for deltagelse i prosjektet. Dette gjøres ved at intervjuer gir deltakerne nødvendig informasjon før respondent og intervjuer underskriver samtykkeerklæring før samtalen/intervjuet gjennomføres.

Studien er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste AS.

Organisatorisk forankring
Studien er godkjent og finansiert av Forsvarets høgskole.
Sjef CIS TG og sjef BKI er informert om denne undersøkelsen. De har gitt sin støtte til at undersøkelsen gjennomføres.

Gjennomføring
Det legges opp til et semi-strukturert intervju, med middels strukturingsgrad, hvor respondentene oppfordres til å fortelle om egne erfaringer, meninger og syn på hvorvidt det er en felles forståelse for Cyberforsvarets oppgaver. Målsettingen er å få utfyllende beskrivelser om hvordan respondentene opplever Cyberforsvarets organisasjonsstruktur, avdelingenes og underavdelingenes oppgaver, og om det er samhandling i Cyberforsvaret.
Oppfølgingsspørsmål benyttes underveis for å kvalitetssikre og effektivisere innsamling av data i forhold til problemstillingen.

Det vil bli brukt diktafon under intervjuet, samtalen skal være ugradert og intervjuet vil bli transkribert etter at det er gjennomført. Dersom respondenten ønsker vil det være mulig å lese gjennom og kommentere transkripsjonen.
Intervjuet
Samtalen vil innledningsvis omhandle samhandling og deretter innrettes mot 3 hovedtemaer:

1. Ansvar
2. Tilhørighet
3. Prestasjon

Strukturerte spørsmål:

Utredningen har samhandling i Cyberforsvaret som overordnet tema. Sett i lys av organisasjonsteori, det instrumentelle perspektivet, skal den besvare følgende problemstilling:

Har Cyberforsvarets avdelinger felles forståelse for organisasjonens oppgaver?

Samtalen vil fokusere på de 3 hovedtemaene som er listet over, hvert med tilhørende spørsmål. Intervjuet gjennomføres som en ledet samtale og spørsmålene under er kun veiledende.

SAMHANDLING

Torgersen og Steiro har følgende definisjon på samhandling:

Samhandling er en åpen og likeverdig kommunikasjons- og utviklingsprosess mellom aktører som kompetansemessig utfyller hverandre og utveksler kompetanse, direkte ansikt-til-ansikt eller mediert via teknologi eller med håndkraft, som arbeider mot felles mål, og hvor forholdet mellom aktørene til enhver tid hviler på tillit, involvering, rasjonalitet og bransjekunnskap

- Hvordan synes du samhandling fremkommer i Cyberforsvaret?
    - Er det samhandling mellom avdelingene? Hvorfor/hvorfor ikke?
    - Utfyller avdelingene hverandre kompetansemessig? Hvorfor/hvorfor ikke?
- I hvilken grad opplever du at avdelingene arbeider mot felles mål?
    - Er felles mål av betydning for å utføre de oppgaver Cyberforsvaret skal? Hvorfor/hvorfor ikke?
- Vil du si forholdet mellom avdelingene hviler på tillit, involvering, rasjonalitet og bransjekunnskap?
    - Er det noe ved Cyberforsvarets oppgaver og organisasjonsstruktur som tilsier at dette ikke er nødvendig mellom avdelingene?

TILHØRIGHET

Er det gjensidig tilhørighet mellom avdelingene i Cyberforsvaret?

- Cyberforsvarets organisasjon er desentralisert. Hvordan synes du dette påvirker din tilhørighet til organisasjonen?

    - Identifiserer du deg med din avdeling (BKI eller CIS TG), høyere avdelingen (CKT eller CTO), Cyberforsvaret eller egen forsvarsgren? Hvorfor/hvorfor ikke?
    - Vil du si din avdeling utfører oppgaver avhengig eller uavhengig av den andre avdelingen?
    - Brukes avdelingene på en hensiktsmessig måte i forhold til Cyberforsvarets oppgaver?
- Vi du si organisasjonsstrukturen er god med tanke på måloppnåelse?
    - Har ledelsen i Cyberforsvaret makt og vilje til å gjennomføre endringer i organisasjonen dersom det vil medføre bedre forutsetninger for effektiv måloppnåelse?
    - Legger organisasjonsstrukturen til rette for samhandling?
- På hvilke områder vil du si det er av betydning å samarbeide med den andre avdelingen? Uavhengig av om det samarbeides på disse områdene eller ikke, hva skyldes det?
    - Hvis avdelingene har et utpreget samarbeid på enkelte områder, og mindre grad av samarbeid på andre områder – hva skyldes dette?

PRESTASJON

Har du forståelse av at avdelingene drar i samme retning/arbeider mot felles mål?

Det instrumentelle perspektivet understreker målspesifisering og formalisering som sentralt. En mål-middel forståelse er essensielt, det vil si samsvar mellom handling og det organisasjonen skal oppnå. Maksimal måloppnåelse er i liten grad realistisk – begrenset rasjonalitet innebærer en god nok måloppnåelse.

Til grunn for prestasjon legges ytelse og det som fører frem til gode resultater.

- Cyberforsvaret er en forholdsvis ny organisasjon, tuftet på arv fra gamle avdelinger. På hvilken måte påvirker det hva din avdeling presterer/gjør?
    - Påvirker en desentralisert organisasjonsstruktur dette? Hvorfor/hvorfor ikke?

- Ser du på din avdeling som en del av en helhet eller som selvstendig og uavhengig av den andre avdelingen?
- Hvilke forhold påvirker avdelingenes forståelse av avdelingsvise-, felles-og organisasjonenes oppgaver?
- Vil du si felles forståelse for organisasjonens oppgaver, eller mangel på felles forståelse påvirker din avdelings prestasjoner? Hvorfor/hvorfor ikke?

ANSVAR

Hvordan forstår avdelingen Cyberforsvarets målbilde?

Ansvar kan omhandle hva man er ansvarlig for, det kan være resultater, prosesser, prosedyrer eller ytelser. Denne studien vil anvende begrepet ansvar om det ansvar Cyberforsvaret har tildelt den enkelte avdeling. Implisitt i dette ansvaret legges også myndighet. Med myndighet forstås den enkelte avdelings område hvor de har beslutningsmyndighet. Dette innebærer myndighet til å fatte beslutninger uten å avklare beslutningen med over eller sideordnede i forkant. Studien vil se på hvordan fordeling av ansvar og myndighet er formalisert og praktiseres.

- Har du og din avdeling en klar forståelse for Cyberforsvarets målbilde?
    - På hvilken måte er dette formidlet til din avdeling?
    - Er målbilde av betydning for de oppgaver din avdeling skal løse?
    - Mener du din avdelings oppgaver er av betydning for at Cyberforsvaret skal løse målbilde?
- Synes du ansvar og myndighet er tydelig avklart i Cyberforsvaret?
    - Har avdelingene selv definert sine ansvarsområder og dermed også hvilken myndighet de har, eller er dette føringer fra høyere hold?
    - Er ansvar og myndighet delegert til hensiktsmessig nivå?
    - Følges ansvaret opp fra nivået det er delegert til, og korrigerer eventuelt ledelsen?
- Om vi sier at Cyberforsvaret er preget av å være tuftet på gammel organisasjonsstruktur – på hvilken måte preger dette fordeling og praktisering av ansvar og myndighet?

    - Har Cyberforsvaret klart å etablere en egen organisasjonskultur? Hvorfor/hvorfor ikke?
- Anser du organisasjonen sammensatt av flere underenheter med motstridende eller felles mål, interesser og kunnskaper?

Avslutning
Takke for intervjuet.
Har du forslag til skrevne kilder?
Andre jeg bør snakke med?
Spørre om det er noe som savnes, burde berøres, i lys av oppgavens problemstilling. Avslutte lydopptaket.

Fortelle om veien videre herfra, og om muligheten til å lese transkripsjon og rapport om dette er ønskelig.

Vedlegg D: Samtykkeerklæring

Samhandling i Cyberforsvaret
"Har Cyberforsvarets avdelinger felles forståelse for organisasjonens oppgaver?"

Bakgrunn og formål
Jeg skriver masteroppgave ved Forsvarets høgskole.
Cyberforsvaret ble etablert i 2012 og er dermed en forholdsvis ny organisasjon, det er en videreføring av Forsvarets informasjons- og infrastruktur. Organisasjonen er desentralisert og i stor grad tuftet på arv fra gammel organisasjonsstruktur. Cyberforsvarets oppgaver er komplekse og omfattende. Organisasjonenes korte levetid tilsier at det i liten grad er forsket på Cyberforsvaret, og tidligere forskning er i svært begrenset grad relevant for denne studien. Denne studiens tittel og problemstilling innebærer innsamling av relevante data for å besvare problemstillingen. Oppgaven har til hensikt å finne ut av om Cyberforsvarets avdelinger har felles forståelse for organisasjonens oppgaver. Studien er vitenskapelig og praktisk relevant da det ikke finnes liknende studier om dette i Cyberforsvaret.

Hva innebærer deltakelse i studien?
Med din bakgrunn i, og kjennskap til Cyberforsvaret ønsker jeg å intervjue deg. Intervjuet krever ingen forberedelser. Intervjuet estimeres å ta 1 – 1 ½ time. Jeg vil ta opp samtalen og transkribere den i etterkant. Dersom jeg finner det nødvendig å ta notater underveis vil jeg gjøre det.

Hva skjer med informasjonen om deg?
Alle personopplysninger vil bli behandlet konfidensielt. Sitater og utsagn vil bli anonymisert i oppgaven. Prosjektet skal etter planen avsluttes i juni 2016. All informasjon innhentet i forbindelse med intervjuene vil bli slettet etter at sensuren på oppgaven har falt i juni 2016.

Frivillig deltakelse
Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi noen grunn. Dersom du ønsker å delta eller har spørsmål til studien, ta kontakt med Silje Nythun
Studien er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste AS.

Samtykke til deltakelse i studien

Jeg har mottatt informasjon om studien, og er villig til å delta

---
(Signert av prosjektdeltaker, dato)

☐ Jeg samtykker til å delta i intervju

Vedlegg E: Godkjenning fra NSD

Norsk samfunnsvitenskapelig datatjeneste AS
NORWEGIAN SOCIAL SCIENCE DATA SERVICES

Harald Hårfagres gate 29
N-5007 Bergen
Norway
Tel: +47-55 58 21 17
Fax: +47-55 58 96 50
nsd@nsd.uib.no
www.nsd.uib.no
Org.nr. 985 321 884

Kåre Dahl Martinsen
Forsvarets stabsskole Forsvarets Høgskole
Postboks 800, Postmottak
2617 LILLEHAMMER

Vår dato: 04.03.2016 Vår ref: 47033 / 3 / BGH Deres dato: Deres ref:

TILBAKEMELDING PÅ MELDING OM BEHANDLING AV PERSONOPPLYSNINGER

Vi viser til melding om behandling av personopplysninger, mottatt 28.01.2016. Meldingen gjelder prosjektet:

47033	*Samhandling og samhold i Cyberforsvaret*
Behandlingsansvarlig	*Forsvarets høgskole, ved institusjonens øverste leder*
Daglig ansvarlig	*Kåre Dahl Martinsen*
Student	*Silje Nythun*

Personvernombudet har vurdert prosjektet og finner at behandlingen av personopplysninger er meldepliktig i henhold til personopplysningsloven § 31. Behandlingen tilfredsstiller kravene i personopplysningsloven.

Personvernombudets vurdering forutsetter at prosjektet gjennomføres i tråd med opplysningene gitt i meldeskjemaet, korrespondanse med ombudet, ombudets kommentarer samt personopplysningsloven og helseregisterloven med forskrifter. Behandlingen av personopplysninger kan settes i gang.

Det gjøres oppmerksom på at det skal gis ny melding dersom behandlingen endres i forhold til de opplysninger som ligger til grunn for personvernombudets vurdering. Endringsmeldinger gis via et eget skjema, http://www.nsd.uib.no/personvern/meldeplikt/skjema.html. Det skal også gis melding etter tre år dersom prosjektet fortsatt pågår. Meldinger skal skje skriftlig til ombudet.

Personvernombudet har lagt ut opplysninger om prosjektet i en offentlig database, http://pvo.nsd.no/prosjekt.

Personvernombudet vil ved prosjektets avslutning, 31.12.2016, rette en henvendelse angående status for behandlingen av personopplysninger.

Vennlig hilsen

Katrine Utaaker Segadal

Belinda Gloppen Helle

Kontaktperson: Belinda Gloppen Helle tlf: 55 58 28 74
Vedlegg: Prosjektvurdering

Dokumentet er elektronisk produsert og godkjent ved NSDs rutiner for elektronisk godkjenning.