FORSVARET
Forsvarets høgskole

IKT-samarbeid

Faktorer som påvirker IKT-samarbeid mellom Forsvaret og Politiet

Arve Christensen

Masteroppgave
Forsvarets høgskole
Vår 2018

Forord

Denne studien ble gjennomført som en del av samlingsbasert master i militære studier ved Forsvarets høgskole i 2018.

Jeg vil først og fremst takke min arbeidsgiver Forsvaret som har gitt meg muligheten til å være student. Og ikke minst velvilje til å tilpasse min arbeidssituasjon for å kunne få nødvendig tid til å gjennomføre denne utdanningen.

Takk til respondentene fra både Forsvaret og politiet som har stilt opp til intervju, og gjort denne oppgaven mulig.

I tillegg må jeg rette en takk til mine veiledere Ingerid Maria Opdahl og Magnus Håkenstad ved Institutt for forsvarsstudier for faglig støtte og metodisk veiledning.

Takk også til Karen-Annette for lesing av korrektur og all annen støtte.

Alle vurderinger i denne oppgaven står for min egen regning.

Kolsås 15. mai 2018

Arve Christensen

Sammendrag

Hensikten med denne oppgaven har vært å finne ut hvordan Forsvaret og politiet ser på muligheten for et økt samarbeid innenfor IKT. Dette er gjort ved å finne de faktorene som påvirker et eventuelt økt samarbeid innenfor IKT. I tillegg er de områdene som etatene ser for seg vil være hensiktsmessig å samarbeide om i fremtiden analysert. Dette er et tema som det i svært liten grad har blitt forsket på tidligere, og det er lite litteratur som omhandler samarbeid mellom etatene ut over operativt samarbeid. Formålet er derfor å bidra til økt forståelse, og etablere empiri for samarbeid mellom Forsvaret og politiet innenfor IKT. Gjennom i hovedsak intensivt forskningsdesign, med ekspertintervjuer, har oppgaven avdekket hvordan Forsvaret og politiet ser på et økt samarbeid innen IKT. Det ble i oppgaven drøftet åtte ulike faktorer. Et av hovedfunnene er at en rekke av faktorene bærer med seg elementer som både fremmer og hemmer et samarbeid. Samtidig som en ser at flere av faktorene vil påvirke hverandre.

De faktorene som påvirker samarbeidet mest er svært sammenfallene fra respondentene i begge etater. Både Forsvaret og politiet mener at økonomi og operativ evne er de viktigste faktorene som fremmer samarbeid, samtidig som ledelse og styring er den faktoren som hemmer mest. Faktoren kompetanse fremmer et samarbeid, da begge etater har utfordringer knyttet til små fagmiljøer og rekrutering. Faktoren media er svakt hemmende da håndtering av media kan komplisere samarbeidet. Kulturfaktoren hemmer for samarbeid mellom etatene, samtidig som den fremmer et samarbeid mellom dem på grunn av mange fellestrekk i kulturen. Lover og regelverk kan være en kompliserende faktor for samarbeid, samtidig som offentlige myndigheter ønsker et økt samarbeid. Organisatoriske implikasjoner, var en faktor som respondenten ikke mente var en faktor av avgjørende betydning på nåværende tidspunkt.

Det er i tillegg avdekket en rekke områder som både Forsvaret og politiet ser for seg et økt samarbeid. Dette er i hovedsak områder for å dekke fremtidige behov for digitalisering, men det er også konkrete forslag til samarbeid om nåværende kapasiteter.

Summary

The purpose of this thesis has been to find out how the Norwegian Armed Forces and the police are looking at the possibility of increased cooperation within ICT. This has been researched by finding the factors that influence the possibility of an increased cooperation within ICT. In addition, the areas of that the agencies consider being useful to collaborating with in the future has been are analyzed. This is a topic that has not been researched in the past, and there is little literature dealing with cooperation between the agencies beyond operational cooperation. The purpose is therefore to contribute to increased understanding, and to establish empirical co-operation between the Armed Forces and the police within ICT. Through intensive research design, with expert interviews, the thesis has revealed how the Armed Forces and the police are looking for increased cooperation in ICT.

The thesis discussed eight different factors. One of the main findings is that several of the factors has elements that both promote and inhibit cooperation. The factors will also affect each other. The factors that affect cooperation are the same with respondents in both agencies. Both the Armed Forces and the police believe that economics and operational ability are the most important factors that promote cooperation, while the factor management and governance inhibits the most.
Knowledge is the last factors that promotes cooperation, as both agencies have challenges related to small academic environments and the recruitment of competent ICT personnel. The media factor is poorly inhibited as media handling can complicate cooperation. The culture factor can be a barrier to cooperation between the police and the Armed Forces, while promoting cooperation between them because they have several similarities in their culture. Laws and regulations can be a complicating factor for cooperation, while public authorities wish an increased cooperation. Organizational implications was a factor that the respondent did not think was a factor that was crucial at this time.

It has also revealed a number of areas that both the Armed Forces and the police are looking for increased cooperation. These are essentially areas to meet future digitalization needs, but there are also concrete proposals for collaboration on current capacities.

Innholdsfortegnelse

1 Innledning

1.1 Bakgrunn

Utviklingen av både datamaskiner og forløperen til dagens internett, er teknologi som ble utviklet for militære formål. Militære var i front av utviklingen innenfor dette området. I dag er ikke dette tilfelle. Det er en voldsom teknologisk utvikling innenfor IT som er drevet av det private næringsliv og industrien. Dette blir ofte beskrevet som den tredje industrielle revolusjon. Utviklingen har ført til at alle deler av samfunnet har blitt stadig mer integrert med ulike IKT-systemer og applikasjoner. Kostnadene for datamaskiner og annen forbrukerelektronikk har gått kraftig ned, men kompleksiteten på systemene og ikke minst mengden av utstyr som er tilkoblet de ulike IKT-baserte tjenester, er kraftig økt. Både anskaffelser, drift og utvikling av IKT har derfor blitt en betydelig kostnad for de fleste bedrifter og offentlige instanser. Et samarbeid innenfor flere områder knyttet til IKT vil kunne gi økonomiske gevinster.

Denne økte avhengigheten har også ført til at IKT har blitt en sårbarhet for samfunnet. I langtidsplanen for Forsvaret står det: «Regjeringen vil fortsette å videreutvikle forsvarssektorens evne til å bistå sivile myndigheters ivaretakelse av samfunnssikkerheten» (Forsvarsdepartementet, 2016, s. 48). Det står videre at det skal gjøres vurderinger om hvordan og i hvilken grad dette skal gjelde IKT støtte. Jeg ønsker derfor i denne studien å se på hvilke muligheter Forsvaret har for et samarbeid med andre offentlige etater innenfor IKT.

I denne studien har jeg valgt å se på et samarbeid med politiet fordi de har en del likhetstrekk med behovene Forsvaret har til IKT. Både politiet og Forsvarets har egne IKT-avdelinger som leverer IKT-tjenester til ulike avdelinger rundt om i hele landet. Begge aktørene har behov for graderte systemer. I tillegg har begge krav med hensyn til beredskap og sikkerhet. Hensikten med denne induktive studien vil derfor være å undersøke muligheter og begrensninger for samarbeid mellom Forsvaret og politiet innen IKT i Norge. Dette gjøres ved a finne de viktigste faktorene som fremmer eller hemmer et økt samarbeid innenfor IKT mellom etatene.

I langtidsplanen for Forsvaret (Forsvarsdepartementet, 2016, s. 72) står det at Cyberforsvaret skal utrede om det er mulig å levere graderte og robuste IKT-tjenester til andre samfunnssektorer. Videre står det i mandatet for utredning og videreutvikling av cyber- IKT området i forsvarssektoren at det skal utredes hvilken bistand og støtte til aktører utenfor forsvarsektoren innenfor cyber -og IKT området som Forsvaret skal kunne gi. I dette dokumentet står det videre at samarbeidet mellom politiet og Forsvaret innenfor IKT området skal videreutvikles for å understøtte samhandling innenfor totalforsvaret, og samtidig bidra til effektiv utnyttelse av de samlede IKT-ressursene.

Politiet benytter i dag i stor grad Telenor sin infrastruktur for sine IKT-systemer. Politiet har høye operative krav og behov for en redundant infrastruktur ut over det Telenor tilbyr. Avhengigheten til Telenors infrastruktur er nevnt som et kritisk sårbarhet i Lysneutvalget (Justis- og beredskapsdepartementet, 2015, s. 115) ,da det ikke er andre aktører som kan tilby en samlet landsdekkende infrastruktur.

I tillegg til dette er det flere likhetstrekk mellom politiet og Forsvaret som gjør at jeg mener det er større muligheter for samarbeid enn med andre etater. Dette er momenter som krav til sikkerhet av selve systemene, viktigheten av oppe tiden og krav til redundante løsninger i beredskapssammenheng. Forsvaret og politiet har også det til felles at det er lokalisert over store deler av landet. I tillegg har politiet og Forsvaret i senere tid hatt et økt samarbeid innenfor flere fagfelt. Dette gjelder til en viss grad IKT, men i stort er dette knyttet til operativ overvåkning og bekjempelse av ulike typer for Cyberkriminalitet.

1.2 Problemstilling

Det er lite erfaringer og litteratur, som vist i kapittel 3, som beskriver samarbeid mellom etatene Forsvaret og politiet innenfor IKT, utenom det operative samarbeidet innen Cyberkriminalitet og cybersikkerhet. Samtidig er det et uttrykt ønske fra Forsvarsdepartementet om at Forsvaret skal samarbeide mer med andre offentlige etater for å kunne oppnå synergier. Med bakgrunn i dette kan det være interessant å finne ut hvordan Forsvaret og politiet ser på et økt samarbeid innenfor IKT. Det vil være en rekke faktorer

som påvirker et samarbeid mellom etatene. I tillegg vil det være interessant å se på hvilke IKT områder det vil være mest hensiktsmessig å samarbeide om.

Problemstilling: Hvordan vil Forsvaret og politiet beskrive muligheten for samarbeid innenfor IKT?

Det som søkes besvart i denne undesøkelse er:

- Hvilke faktorer fremmer et samarbeid mellom Forsvaret og politiet innenfor IKT?
- Hvilke faktorer hemmer et samarbeid mellom Forsvaret og politiet innenfor IKT?
- Hvilke områder innenfor IKT ser Forsvaret og politiet for seg som mulige samarbeidsområder i fremtiden?

1.3 Begrepsavklaringer

IKT

IKT er en forkortelse for informasjon og kommunikasjonsteknologi. Informasjons- og kommunikasjonsteknologi er en samlebetegnelse for teknologi for innhenting, overføring, bearbeiding, lagring og presentasjon av informasjon (Store Norske Leksikon, 2018). Begrepet er en videreutvikling av informasjonsteknologi (IT) og kommunikasjon. I dag henger dette ofte sammen, da IT-systemene vanligvis er integrerte i en eller annen form for nettverk som krever kommunikasjon mellom de forskjellige IT systemene. Begrepet blir i mange sammenhenger delt i tre ulike lag. Øverste lag omhandler de tjenestene som blir brukt. Dette er tjenester som e-post, tilgang til internett med mer. Under her ligger programmer og utstyr. Det vil si selve pc-en og de programmer som er installert. Nederst har vi kommunikasjons-infrastrukturen. Det er linjer eller trådløse løsninger som mobiltelefoni eller wifi som kobler dette sammen. Det finnes derfor flere ulike fagområder innenfor begrepet IKT.

Sivilt-militært samarbeid

I Forsvaret blir samarbeid med andre aktører som ikke er en del av militære styrker i andre nasjoner, definert som sivilt militært samarbeid. Begrepet sivilt–militært samarbeid omfatter i

prinsippet alt sivilt–militært samarbeid på alle nivåer, og spenner over et svært bredt felt med mange ulike aktører. Begrepets innhold er i stor grad situasjonsbetinget. «I noen tilfeller støtter Forsvaret sivil virksomhet, mens Forsvaret i andre situasjoner støttes av sivile ressurser» (Justis- og beredskapsdepartementet, 2015, s. 64). For Forsvarets side vil dette også inkludere politiet, da politiet regnes som en del av Norges sivile myndigheter, og som har som primær oppgave å ivareta samfunnssikkerheten i Norge. Forsvaret har ansvar for statssikkerheten, ivaretagelse av suverenitet, territoriell integritet og politisk handlefrihet. Politiet er også som Forsvaret en uniformert etat, og omtaler andre deler av samfunnet som sivile, så begrepet kan derfor misforstås. Samtidig er dette begreper som det refereres til i en rekke offentlige rapporter og utredninger, men har i disse et fokus for å støtte opp under den totale samfunnssikkerheten, og går i liten grad ut over operativt samarbeid. I et mer IKT rettet perspektiv, der Forsvaret og politi samarbeider om konkrete løsninger eller konkrete prosjekter innenfor fagfeltet IKT, er det mindre skille mellom sivil og militær.

Graderte systemer

Graderte IKT-systemer er systemer som inneholder gradert informasjon. Det skal foretas en verdivurdering og en sikkerhetsgradering ut fra informasjonens skadepotensialet. Denne informasjonen skal så behandles etter sikkerhetsloven. Det er §11 i loven som definerer de fire nasjonale nivåene. STRENGT HEMMELIG (avgjørende skade), HEMMELIG (alvorlig skade) KONFIDENSIELT (kan skade), BEGRENSET (i noen grad kan skade) mot Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende (Forsvarsdepartementet, 2016, s. 149).

For informasjon som ikke graderes etter sikkerhetsloven, men der informasjonen kan skade offentlige interesser, en bedrift eller institusjon eller enkeltmennesket, benyttes beskyttelsesinstruksen. Den opererer med 2 grader: STRENG FORTROLIG og FORTROLIG. Dokumenter gradert etter denne instruksen skal så langt det passer, behandles som BEGRENSET (Statsministerens kontor, 2009). IKT-systemer som håndterer slik informasjon bør derfor være graderte, men det er ikke et krav.

I denne oppgaven omtaler jeg derfor graderte systemer, som IKT-systemer som er godkjent etter sikkerhetsloven.

1.4 Avgrensning

Justis- og beredskapsdepartementet (JBD) og Forsvarsdepartementet (FD) har samarbeid både på politisk og mer operasjonelt plan. Nasjonal sikkerhetsmyndighet(NSM) er et eksempel. Etaten er underlagt FD, med utfører også oppgaver for Justis- og beredskapsdepartementet. I denne oppgaven ønsker jeg å se på samarbeidet innenfor IKT mellom etatene politiet og Forsvaret. Samarbeid på departementsnivå er derfor ikke inkludert i oppgaven.
Politiet og Forsvaret samarbeider i dag på en rekke områder. I hovedsak er dette knyttet opp mot operativ samarbeid. Innenfor IKT er dette operative samarbeidet betydelig. Etterretningstjenesten har tett samarbeid med Politiets Sikkerhetstjeneste (PST) innenfor cyberdomenet, og Cyberforsvaret og politiet har et tett samarbeid med NorCERT (Norwegian Computer Emergency Response Team) med tanke på beskyttelse mot ulike trusler fra internett. Denne studien omhandler ikke operative forhold, men operative forhold vil påvirke hvilke samarbeidsformer som er mulig, da hensikten med et eventuelt økt samarbeid også er å bedre den operative evnen for begge etatene.

I tillegg velger jeg å se bort fra tekniske utfordringer knyttet til de ulike IKT-systemene etatene benytter, fordi jeg antar dette i mindre grad er utslagsgivende. Noen av systemene som benyttes, som for eksempel tilgang til internett, vil være like.

1.5 Oppgavens struktur

Kapittel 1 setter rammene for oppgaven og redegjør for oppgavens bakgrunn, relevans og problemstilling. I tillegg blir noen sentrale begreper definert, samt en avgrensing av oppgaven.

Kapittel 2 gir en innføring i oppgavens valgte metode med undersøkelsesdesign, utvalgsstrategi, datainnsamlingsprosessen og forskningskvalitet.

Kapittel 3 er en gjennomgang av aktuell litteraturer og en presentasjon av aktørene i studien.

Kapittel 4 presenterer funnene i undersøkelsen. De ulike faktorene som kom frem gjennom intervjuene blir analysert. Til slutt i kapittelet vil de anbefalte samarbeidsområdene som kom frem gjennom intervjuene bli analysert.

Kapittel 5 konkluderer og besvarer oppgavens problemstilling. I tillegg diskuteres studiens relevans og tanker rundt videre forskning.

2 Metode

2.1 Valg av Undersøkelsesdesign

Problemstillingen som skal undersøkes er: Hvordan vil Forsvaret og politiet beskrive mulighetene for samarbeid innenfor IKT? Mulighetsrommet for samarbeid mellom to ulike etater, og forskjellige departementer er fenomenet som skal undersøkes. Det er små erfaringer og lite empiri på et samarbeid mellom politiet og Forsvaret ut over operativt samarbeid. Under operativt samarbeid finnes det mengder av offentlige dokumenter og undersøkelser. Dette fikk et økt fokus etter terrorangrepet 22. juli. Undersøkelsen vil gå i dybden for å avdekke de viktigste faktorene som påvirker dette samarbeidet. Siden undersøkelsen vil begrense seg til kun politiet og Forsvaret som er få enheter, vil det være et intensivt design. Fordelen med et intensivt design er at det tar inn over seg kontekst og dybde. Påliteligheten av en slik undersøkelse regnes som stor. Ulempen med et intensivt design er at det ikke egner seg til generalisering. Den eksterne gyldigheten er med andre ord liten (Jacobsen, 2015, s. 237).

Yin sier at en skal tilstrebe å benytte en casestudie når man søker å forklare et fenomen om nåtid, og når problemformuleringen har spørsmål som hvordan og hvorfor (Yin, 2014). I Jacobsens beskrivelse av en casestudie settes fokuset på en spesiell enhet, som gjerne avgrenses i tid og rom, og som studeres i den konteksten fenomenet utvikler seg, eller der en spesiell hendelse finner sted (Jacobsen, 2015, ss. 97-99). Denne undersøkelsen omhandler mer enn en enhet, men samtidig er den begrenset i å omhandle kun to enheter, politiet og Forsvaret. Men i denne oppgaven er det fenomenet samarbeid som er i fokus, og da anbefaler Jacobsen at små N-studier bør benyttes. I små N-studier tones betydningen av et spesielt sted eller hendelse ned, mens betydningen av fenomenet blir større (Jacobsen, 2015, s. 106) . Små

N-studier egner seg derfor godt når en ønsker en rik og detaljert beskrivelse av et fenomen (Jacobsen, 2015, s. 107)

For valg av forskningsmetode som best svarer på min problemstilling må en velge en kvantitativ, kvalitativ eller en kombinasjon av disse som metode. En kvantitativ tilnærming er gjerne hensiktsmessig når vi blant annet ønsker å beskrive hyppigheten eller omfanget av et fenomen, når vi ønsker mange enheter og en bredde i undersøkelsen, og når generalisering blir et mål (Jacobsen, 2015, ss. 136-137). En kvalitativ strategi tar utgangspunkt i at den sosiale verden er konstruert og at dette skjer gjennom individers handlinger. Dermed egner en kvalitativ tilnærming seg bedre når man skal gå i dybden på et fenomen, og samtidig få ulike nyanser, og flere individers tolkning av en spesiell kontekst (Ringdal, 2013, s. 104). En kombinasjon av kvalitativ og kvantitativ metode, metodetriangulering for innhenting av empiri både i bredde og dybde kan i flere tilfeller være hensiktsmessig og fordelaktig, og kanskje også idealet (Jacobsen, 2015, ss. 138-139). I denne studien vil fokuset være å finne de ulike faktorene som påvirker samarbeidet mellom Forsvaret og politiet. Det er derfor behov for å gå i dybden, finne de ulike aktørenes tolkninger av eksisterende lovverk og nyansen for hvilke muligheter etatene ser i et slike samarbeid. Studiene vil derfor basere seg på kvalitativ forskningsmetode med bruke av en N-studie for å svare på problemstillingen.

2.2 Utvalgsstrategi

For å kunne få belyst problemstillingen fra flere ulike vinkler som valget at metoden små N-studie krever, vil jeg intervjue personer som sitter på ulike posisjoner i de to forskjellige etatene. Hvis fenomenet er samarbeid mellom organisasjoner, må vi ha informanter/respondenter fra flere organisasjoner, men også fra ulike avdelinger i de enkelte organisasjonene. (Jacobsen, 2015, s. 108). Ved å se på organiseringen av Forsvaret og politiet kommer det frem at det er en god del likheter i organiseringen. Under Justis -og beredskapsdepartementet ligger Politidirektoratet (POD), mens for Forsvarsdepartementet har vi Forsvarsstaben. Begge disse avdelingene har en mindre IKT-avdeling som har som formål å samordne, og følge opp drift og utvikling av IKT i etatene. Det var derfor naturlig å få en fra hver av disse avdelingene til intervju.

Politiets IKT-tjenester (PIT) drifter, utvikler og forvalter IKT-systemene til politiet. I Forsvaret er dette ansvaret delt mellom Cyberforsvaret og Forsvarets Materielletat- IKT kapasiteter (FMA IKT-Kap), men det er Cyberforsvaret som skal være den styrende aktøren, og legge føringer for IKT til Forsvaret. Jeg ønsket derfor en aktør fra Politiets IKT-tjenester og Cyberforsvaret.

For å få finne det rette utvalget av respondenter har jeg valgt en kombinasjon av ulike metoder. På grunn av begrensninger i tid og ressurser vil jeg ikke ha anledning til å intervjue mer enn 4-6 personer. Siden metoden krever å få belyst fenomenet fra flere ulike synspunkter var det viktig at minst en fra hver av avdelingene ble representert. Dette for å ivareta bredden og variasjonen i undersøkelsen. I følge Jacobsen (Jacobsen, 2015, s. 181) skal en trekke ut tilfeldige personer fra hver av undergruppene. I denne studien ble respondenter fra de ulike gruppene valgt med tanke på hvem som kan gi god informasjon. For å finne den rette personen i de ulike avdelingene, har jeg kontaktet tidligere bekjentskaper både i Forsvaret og politiet om hvem jeg burde intervjue. Det var ønskelig at personen som ble intervjuet skulle ha kjennskap til problemstillingen, eller erfaringer fra arbeid med samarbeid med andre etater. Det var viktig at personen som ble intervjuet skal kunne svare på vegne av avdelingen, men samtidig var det et ønske om at det skulle være rom for personlige betraktinger om temaet. Respondentene fra Forsvaret og PIT ble strategisk valgt ut etter telefonsamtaler med mine bekjentskaper. Respondenten fra POD ble tildelt etter en henvendelse på mail til POD. Under selve intervjuet ble også informantene forespurt om forslag til andre respondenter som kunne belyse problemstillingen ytterligere. Dette er i henhold til det Jacobsen kaller snøballmetoden (Jacobsen, 2015, s. 182). Respondenten fra PIT anbefalte samme person som jeg fikk tildelt fra POD som den rette personen å intervjue hos POD. Jeg fikk også forslag til andre personer, som ble kontaktet via telefon eller mail. Disse personene gjennomførte jeg ikke dybdeintervju med, men de ble kontaktet for å få tilgang til empiri, eller som kunne svare på enkelte tema. De er ikke sitert i oppgaven.

2.3 Datainnsamlingsprosessen

I denne studien ble det i hovedsak benyttet primærdata. Primærdata er opplysninger direkte fra mennesker eller grupper av mennesker (Jacobsen, 2015, s. 139). Dette innebærer at forskeren samler inn opplysninger for første gang. Dette ble utført ved ansikt til ansikt

intervju. Det åpne individuelle intervjuet egner seg ifølge Jacobsen godt når det er relativt få enheter som skal undersøkes, når vi er interessert i hva det enkelte individ sier, eller når vi er interessert i hvordan den enkelte fortolker og legger mening i et spesielt fenomen (Jacobsen, 2015, s. 146). I denne studien er det kun to enheter, politiet og Forsvaret, som undersøkes. Individuelle synspunkter kan også få frem holdninger og synspunkter på problemstillingen. Det mest interessante er å finne ut hvordan den enkelte fortolker og legger mening i fenomenet samarbeid mellom politiet og forsvaret.

Respondentene ble kontaktet på telefon og per mail. Intervjuene ble gjennomført i perioden 6.mars til 4. april 2018. Alle respondentene fikk et informasjonsskriv med samtykkeerklæring, se vedlegg C, der det var mulig å krysse av dersom de ønsket å være anonyme. I utgangspunktet er det ikke ønskelig at respondentene skal være anonyme da jeg ønsket å intervjue personer som både hadde egne meninger om temaet, samt kunne uttale seg på vegne av den enheten de representerer. Det ble benyttet diktafon under intervjuene for å sikre at samtalene ble så åpne som mulig, men dette var frivillig om noen av respondentene ikke ønsket dette. Alle respondentene samtykket i bruk av diktafon. Ingen av respondentene hadde behov for anonymitet. Intervjuene ble senere transkribert.

Det ble utarbeidet en intervjuguide med en middels strukturingsgrad (Jacobsen, 2015, s. 151) med åpne spørsmål relatert til ulike temaer. Dette for å sikre at informantene ble stilt tilnærmet samme spørsmål, samtidig som det er mulig å stille oppfølgingsspørsmål med utgangspunkt i det respondentene beskriver for videre utdyping og avklaring. Dersom respondenten ikke virket til å kunne svare utfyllende, ble også oppfølgingsspørsmål benyttet. Eksempler på dette er beskrevet i intervjuguiden. Siden jeg har litt kjennskap til problemstillingen er det også viktig å benytte åpne spørsmål, slik at respondenten selv skulle svare på spørsmålene uten at min kjennskap og erfaringer påvirket svarene.
Oppgaven har som hensikt å finne faktorer som fremmer eller hemmer et samarbeid mellom politiet og Forsvaret innenfor IKT. Både intervjuguide, oppfølgingsspørsmål og senere data-analyse vektla søken etter slike faktorer.

Intervjuene ble gjennomført på respondentenes arbeidsted, og intervjuene ble tatt opp på diktafon. Intervjuene hadde en avsatt varighet på 1-1,5 time. I praksis varte intervjuene mellom 1,5 -2 timer. Dette inkluderte en presentasjon av meg selv og oppgaven, samt en

gjennomgang av samtykkeerklæringen før selve intervjuet med lydopptaker. Lydopptakene er på mellom 45-60 minutter. Det ble også ført en diskusjon i etterkant av alle intervjuene. Dette var i førte rekke tenkt til å omhandle eventuelt gradert informasjon, da lydopptakeren og selve oppgaven er ugradert. Dette er ikke benyttet i oppgaven. Det kom også opp annen aktuell informasjon i denne diskusjonen, men det er ikke referert til noe av dette i oppgaven.

Metoden som ble benyttet for analyse er Jacobsens fire forholds modell for praktisk analyse av kvalitative data (Jacobsen, 2015, s. 199). Først ble intervjuene transkribert. Så ble utskriftene med data utforsket. Oppgaven hadde til hensikt å finne faktorer som påvirket et samarbeid mellom etatene, så analysen vektla søken etter slike faktorer. Punkt tre er å systematisere og kategorisere. Her ble elementer av dataene fra de ulike intervjuene kategorisert etter hvilken faktor de påvirket. Det sist punktet er å sammenbinde de ulike kategoriene. I dette tilfelle faktorene. Denne viser at flere at dataene vil kunne ha innvirkning på flere faktorer, men i drøftingen er det tilstrebet at dataene er hengt opp i den faktoren de påvirker mest direkte.

I tillegg vil jeg gjennomføre en dokumentundesøkelse for å kunne sammenligne med tilegnet empiri. Dette vil være lover, og politiske føringer. I tillegg finnes det kilder som omhandler samarbeid mellom politi og Forsvar på operasjonelt nivå. Boken «Strategisk Ledelse i krise og krig» (Dyndal, 2010) bidrar med kunnskap om utfordringer knyttet til sivil- militært samarbeid: Denne boken har fokus på lovverket knyttet til bruk av militære styrker og hvordan Forsvaret kan samarbeide operasjonelt om håndtering av kriser. Det er ingen ting som omhandler et daglig praktisk samarbeid om IKT. Det er flere offentlige utredninger og stortingsproposisjoner som omhandler både IKT og samarbeid mellom ulike offentlige og private aktører. Majoriteten av disse omhandler IKT-sikkerhet og samarbeid for å redusere sårbarheten i samfunnet ved økt bruk av IKT. Dette er nærmere beskrevet i kapittel 3.
For å underbygge påstander fra respondentene i intervjuene og de utledede faktorene, er det benyttet annen litteratur eller teorier som underbygger dette. Eksempler er litteratur om kompetanse innfor IKT, og teorier for hvordan media fungerer. Denne litteraturen eller teorier er ikke drøfte i oppgaven.

2.4 Gyldighet og pålitelighet

Gyldighet

Hver metode for innsamling av empiri skal tilfredsstille to krav. Empirien skal være gyldig og relevant(valid), og den skal være pålitelig og troverdig(reliabel) (Jacobsen, 2015, s. 16). For at undersøkelsen skal være valid må det være dekning for empirien og konklusjonene i oppgaven. Resultatet av studien skal derfor oppfattes som rimelig og kunne testes. Et utkast av empirien og analysen ble derfor oversendt respondentene. Hensikten med dette var at respondentene skulle kunne gi tilbakemeldinger på om det var feil, misforståelser eller uklarheter knyttet til empirien eller analysen. «Denne formen for validering skjer ved at flere enkeltpersoner uttaler seg om undersøkelsens innhold uavhengig av hverandre» (Jacobsen, 2015, s. 233). Respondentene i denne undersøkelsen kommer fra ulike etater og avdelinger som i stor grad er uavhengige av hverandre. Den interne gyldigheten i oppgaven er validert gjennom tilbakemeldinger fra respondentene i undersøkelsen. Utfordringen med denne type validering er at undersøkelsen kan avdekke forhold eller konklusjoner som respondenten selv ikke er klar over, eller kjenner seg igjen i selv om dette er gyldig. Respondentvalidering er derfor alene ikke tilstrekkelig.

Selv om det er lite tidligere forskning på dette området er det gitt ut en del offentlige rapporter, føringer og lovverk som er brukt for å underbygge, eller avkrefte eventuelle faktorer som kom frem i analysen. I tillegg er andre teorier benyttet for å støtte opp og forklare respondentenes sine utsagn i forbindelse med intervjuet.

«Ekstern gyldighet og relevans går på om resultater fra et avgrenset område- f.eks. en organisasjon på et gitt tidspunkt- er gyldig også i andre sammenhenger (f.eks. andre organisasjoner)» (Jacobsen, 2015, s. 17). Ved et lite utvalg av respondenter med et så spesifikt område og etatenes særegenhet vil resultatene i denne undersøkelsen i liten grad kunne generaliseres til andre enheter. Men flere av de avdekkede faktorene er generelle av karakter, og vil derfor også kunne gjelde for samarbeid mellom andre etater. Utfordringer knyttet til

lovverket f.eks. sektorprinsippet vil også kunne være overførbar til andre fagområder enn IKT.

Pålitelighet

«Med pålitelighet og troverdighet mener vi at undersøkelsen må være til å stole på» (Jacobsen, 2015, s. 17). For at studien skal være etterprøvbar er intervjuguiden vedlagt oppgaven. I tillegg er intervjuene transkribert og tilgjengelig på forespørsel. Samme intervjuguide ble benyttet i alle intervjuene, men alle spørsmålene ble ikke stilt da respondentene ofte gikk videre over til neste spørsmål uten at spørsmålet måtte stilles. Enkelte ganger gikk også respondenten tilbake til et tidligere stilt spørsmål for å komme med utfyllende kommentarer.

«Intervjusituasjonen kan påvirke, og enhver undersøkelse må inneholde en diskusjon om hvordan intervjueffekter kan påvirke resultatet» (Jacobsen, 2015). Derfor ble intervjuene gjennomført på respondentens normale arbeidssted, enten på kontoret eller tilhørende møterom, for å gi så normal situasjon som mulig. Respondentene fikk også tilbud om å gjennomføre intervjuet uten bruk av lydopptaker, dersom dette var til hinder for selve intervjuet. Ingen valgte å benytte seg av dette tilbudet. I tillegg til dette fikk respondentene mulighet til å anonymiseres i oppgaven. Dersom en av respondentene ønsket dette, måtte det vært vurdert om alle respondentene måtte anonymiseres. Ingen av respondentene valgte å være anonyme. Siden jeg jobber i Cyberforsvaret vil min rolle som intervjuer kunne påvirke respondentene ulikt. Ingen av respondentene fra Forsvaret var personer jeg kjente fra tidligere, men vi har mange felles kjente i virksomheten noe som kan føre til et mer kollegialt intervju. Jeg valgte derfor å gjennomføre alle intervjuene kledd i sivilt, og benyttet en lik intervjuguide for alle respondentene.

2.5 Etiske betraktninger

Prosjektet er meldt til Personvernombudet ved Norsk senter for Forskningsdata AS (NSF) med prosjektnummer 58487. Hensikten med dette er at alle personvernopplysninger blir behandlet i henhold til personopplysningsloven og god forskningsetikk. Prosjektet ble godkjent 26.01 2018. Prosjektet er gjennomført etter forskningsetiske retningslinjer. Alle

respondenter fikk tilsendt eller presentert et informasjonsskriv i forkant av selve intervjuet. Respondentens rettigheter ble også gjennomgått i innledningen av intervjuet. Se vedlegg B. Alle respondentene fikk i samtykkeerklæringen, se vedlegg C, mulighet til anonymisering og eventuelt muligheten til å frastå fra bruk av lydopptaker. Alle innsamlede personopplysninger og empiri som lydfiler, transkripsjoner og renskrivende notater fra intervjuene er oppbevart elektronisk i henhold til NSF's sine retningslinjer.

3 Litteratur og introduksjon av undersøkelsens aktører

Det er, som nevnt tidligere, skrevet lite om temaet IKT-samarbeid mellom Forsvaret og politiet. «I Norge har ikke sivil-militære relasjoner stått særlig sterkt som akademisk forskningsfelt» (Dyndal, 2010, s. 77). Det meste av litteraturen som omhandler samarbeid mellom Forsvaret og politiet omhandler operative forhold. Terrorangrepet 22. juli 2011 førte til økt fokus på hvilken bistand Forsvaret kunne gi til politiet. Det ble blant annet utarbeidet en ny bistandsinstruks, og gjort endringer i politiloven slik at denne støtten skulle bli avklart lovmessig. Ingenting av dette omhandler et gjensidig samarbeid mellom etatene innenfor IKT.

Boken «Balansegang» tar for seg Forsvarets omstilling fra den kalde krigen fram til 2014 og har et fokus på «Forsvarets vanskelige balansegang mellom militær beredskap og økonomisk bærekraft» (Bogen, 2015). Men denne har ikke et fokus opp mot andre enn Forsvaret selv. Bøkene «Strategisk ledelse i krise og krig» (Dyndal, 2010) og «Mellom fred og krig» (Heier, 2013), omhandler det norske systemet for krisehåndtering og forholdet mellom Forsvaret og politiet. Begge bøkene gir et innblikk i hvilke operative ressurser Forsvaret har som kan støtte samfunnet ved kriser. Disse bøkene inneholder lovhjemler og erfaringer som har innvirkning på det operative samarbeidet mellom Forsvaret og politiet. Det er ingenting i disse bøkene som omhandler et gjensidig samarbeid innenfor fagfeltet IKT mellom etatene.

Lovverket som vil legge føringer for et eventuelt samarbeid mellom Forsvaret og politiet, vil i dette kapittelet kun bli nevnt overordnet. Hvordan disse lovene påvirker et eventuelt økt samarbeid kommer frem i drøftingen senere i oppgaven. Andre offentlige utredinger (NOU) og stortingsdokumenter som omhandler samarbeid og IKT vil også bli omtalt.

Noen teorier er benyttet for å underbygge enkelte påstander fra respondentene. Disse blir ikke videre drøftet i denne oppgaven da disse i all hovedsak er benyttet for å forklare hvordan dette henger sammen med de aktuelle faktorene.
Til slutt i kapittelet er det skrevet litt om de ulike aktørene som har deltatt i studien. Dette er overordnet informasjon der elementer blir benyttet i drøftingen.

3.1 Overordnede førende dokumenter

Lover

Grunnloven

I denne oppgaven er det referert til Norges Grunnlov §101 (tidligere §99). Denne paragrafen omhandler bruk av militære styrker mot innbyggere i Norge. Hvordan dette kan påvirke et samarbeid mellom etatene er beskrevet i drøftingene.

Sikkerhetsloven

«Formålet med denne loven er å legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, ivareta den enkeltes rettssikkerhet, og trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjenester» (Forsvarsdepartementet, 2017, s. §1). Denne loven trådde i kraft 1. juli 2001, og det har kun blitt utført mindre endringer i loven siden det. I proposisjon til Stortinget, Prop.153 L(2016-2017), er det sendt frem forslag til lovendring. Dette lovforslaget bygger på NOU 2016: 19 «Samhandling for sikkerhet». Denne kommer jeg tilbake til senere. «Forslaget vil styrke samhandlingen mellom myndigheter og virksomheter slik at det forebyggende sikkerhetsarbeidet mot terror, sabotasje og spionasje kan gjennomføres på en mer effektiv og forsvarlig måte» (Forsvarsdepartementet, 2016, s. 7). Proposisjonen legger anbefalingen fra NOU 2016:19 til grunn og anbefaler at loven skal gjelde på tvers av alle sektorer, og at loven skal gjelde alle grunnleggende nasjonale funksjoner. «En funksjon er å anse som grunnleggende for Norge dersom bortfall av denne får konsekvenser som truer Norges suverenitet, territorielle integritet og demokratiske styreform» (Forsvarsdepartementet, 2016, s. 26). Som respondentene fra politiet uttalte i intervjuene, kan

dette få konsekvenser for deres IKT-systemer, da disse ikke er graderte etter sikkerhetsloven i dag.

Anskaffelsesloven

Lov om offentlige anskaffelser eller (anskaffelsesloven) sier noe om hvordan det offentlige skal forholde seg til leverandører. I dette tilfellet leverandører av IKT. Videre har Forsvarsdepartementet en egen forskrift om forsvar og sikkerhetsanskaffelser. Denne forskriften går i all hovedsak på regelverk for anskaffelser av forsvarsmateriell, gradert materiell eller deler som understøtter dette. Denne loven gjelder også politiet ved anskaffelser av slikt utstyr. Ingen av disse lovene omhandler samarbeid mellom etater, men er førende for begge parter ved anskaffelser.

Personopplysningsloven

«Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger» (Justis- og beredskapsdepartementet, 2015). Dette legger føringer for hvordan politiet og Forsvaret behandler personopplysninger, og vil derfor stille krav til etatenes IKT-systemer som håndterer dette. For ytterligere presisering knyttet til politiets og påtalemyndigheters behandling av personopplysninger finnes politiregisterloven som legger føringer for politiets IKT-systemer. Ingen av disse omhandler samarbeid mellom sektorer eller etater.

Politiloven

Politiloven regulerer politiets arbeid. I §27A regulerer Forsvarets bistand til politiet. Dette knyttet opp mot bistandsinstruksen. Denne omhandler kun Forsvarets operative bistand til politiet, og ikke noe om et eventuelt samarbeid om drift og forvaltning av IKT.

Bistandsinstruksen

Denne instruksen er å gir retningslinjer for Forsvarets bistand til politiet. Det vil si bruk av militært personell og materiell til støtte for politiet. I rapporten «Forsvarets Bistand til Politiet» som skulle komme med forslag for utarbeiding av ny bistandsinstruks, er det lite som omhandler IKT. Det som er nevnt her angående IKT er i første rekke knyttet til Cybertrussler,

og begge etaters begrensede kapasitet til å håndtere dette. «Forsvaret vil i mange tilfeller måtte prioritere drift og sikring av egne militære nettverk og sambandssystemer» (Justis- og beredskapsdepartementet, 2016, s. 26). I tillegg skrives det at det er et signifikant skille mellom militære og sivile IKT-systemer. Det er med andre ord ingenting i dette som omhandler et eventuelt samarbeid innenfor drift og forvaltning av IKT-systemer.

Stortingsmeldinger og rapporter

Det finnes en rekke dokumenter utgitt av forskjellige departementer som går på IKT-sikkerhet, eller der deler av dokumentet omhandler dette. De omhandler sårbarhetene ved økt bruk av IKT, og har gjerne en teoretisk tilnærming til utfordringene. I tillegg er det beskrevet lover og regelverk som gjelder på tvers av sektorer. Ofte er det også beskrevet knytninger til sivile sektorer. Flere av disse har utgangspunkt i sårbarhetsutvalget (Justis- og politi departementet, 2000). Det er svært lite i disse som omhandler er et eventuelt samarbeid mellom Forsvaret og politiet innenfor drift og forvaltning av IKT-systemer. Under er de mest sentrale beskrevet.

«Meld. St. 21 (2012-2013) Terrorberedskap» er en oppfølging av «NOU 2012: 14 Rapport fra 22.juli-kommisjonen». «I denne meldingen legger regjeringen fram en overordnet strategi for forebygging og håndtere terror i Norge og mot norske interesser og nordmenn i utlandet» (Justis- og beredskapsdepartementet, 2013, s. 8). I denne står det at politiet og andre aktører innenfor totalforsvaret skal ha tilgang til graderte informasjonssystemer.

I «NOU 2015:13 Digitale sårbarhet – sikkert samfunn» er det et fokus på de digitale sårbarhetene i samfunnet og hvilke grep det norske samfunnet bør ta for å bedre dette. Her adresseres blant annet utfordringen ved at Telenor er eneste landsdekkende leverandør av kommunikasjonsinfrastruktur. Og at IKT-sikkerhetskompetanse må styrkes i flere sektorer. Den presiserer også viktigheten av informasjonsutveksling innenfor IKT-sikkerhet.

«NOU 2016:19 Samhandling for sikkerhet» omhandler temaer som informasjonssikkerhet, objektsikkerhet, personellsikkerhet og forhold knyttet til dette. Den gir et bilde av risiko for at tilsiktede uønskede hendelser skal ramme verdiene vi ønsker å beskytte, og hvordan vi skal

beskytte oss mot dette. Den omhandler ikke praktisk samarbeid innenfor IKT mellom de to etatene.

«Meld. St. 38 (2016-2017) IKT-sikkerhet – Et felles ansvar» omhandler IKT-sikkerhet i de ulike sektorene. Den er også inne på utfordringer knyttet til at digitaliseringen de siste årene har bidratt til langt flere tverrsektorielle utfordringer (Justis- og beredskapsdepartementet, 2016, s. 22).

I «Meld. St. 10 (2016-2017) Risiko i et trygt samfunn» er utfordringen med moderne IKT-systemer, og hvor sårbart samfunnet er knyttet til dette beskrevet. Det er kartlagt en rekke områder som bør forbedres. Denne har et fokus opp mot IKT-sikkerhet. Sikkerhetskompetanse, nasjonal tilgang til kryptografi, robusthet i IKT-systemer, samt internasjonalt samarbeid innenfor IKT er temaer i denne. Melding presiserer at «Forsvarsdepartementet har ansvaret for IKT-sikkerhet i forsvarssektoren. Justis- og beredskapsdepartementet skal involvere Forsvarsdepartementet i saker innenfor sivil IKT-sikkerhet som berører IKT-sikkerhet i forsvarssektoren, og sammen med Forsvarsdepartementet bidra til at sivil-militære utfordringer og behov sees i sammenheng. (Justis- og beredskapsdepartementet, 2016, s. 62)». Igjen er vi inne på IKT-sikkerhet, men den omhandler ikke samarbeid ut over dette.

I «Meld. St. 27 (2015-2016) Digital agenda for Norge» presenteres regjeringens overordnede politikk for hvordan vi kan utnytte IKT til samfunnets beste. Denne har i tillegg til fokus på sikkerhet, føringer for hvordan regjeringen ønsker økt digitalisering av offentlig sektor i Norge. Denne har fokus på andre etater enn Forsvaret og politiet.

«Difi-rapport 2014:07 Mot alle odds - veien til samhandling i norsk forvaltning» har som formål å belyse samordning i norsk forvaltning og å peke på mulige veier til å forbedre dette. Har fokus på sektorinndelingen i statsforvaltningen, og omhandler ikke generelt IKT samarbeid.

Proposisjoner til Stortinget

«Prop. 73 S (2011 – 2012) Et forsvar i vår tid» ønsker Forsvaret å ta ut gevinster ved å samarbeide med andre offentlige virksomheter. «Samtidig vil noen gevinster hentes ut ved å inngå samarbeidsløsninger med andre aktører, som for eksempel andre offentlige virksomheter, næringsliv og industri, og andre lands myndigheter. Samarbeid med andre kan gi positive effekter for Forsvaret, og bidra til en bedre utnyttelse av samfunnets samlede ressurser og kompetanse» (Forsvartsdepartementet, 2012, s. 138). Dette legger føringer for økt samarbeid innen IKT, men også kompetanse som er en av faktorene som blir drøftet senere i oppgaven.

I «Prop. 151 S (2015-2016) Kampkraft og bærekraft» er det flere elementer som omhandler og påvirker et eventuelt økt samarbeid mellom Forsvaret og politiet. «Regjeringen vil videreutvikle samarbeidet mellom Forsvaret og politiet innenfor IKT-området for å understøtte samhandlingen innenfor totalforsvaret, og bidra til effektiv utnyttelse av de samlede IKT-ressursene» (Forsvarsdepartementet, 2016, s. 104). Her påpekes det tydelig at det er ønskelig med et økt samarbeid mellom politiet og Forsvaret. I tillegg står det: «Ved større investeringer i Forsvaret som kan ha nytteverdi for sivile myndigheter, skal det avklares om det finnes bistands- og støttebehov og muligheter for flerbruk» (Forsvarsdepartementet, 2016, s. 7). Dette gir altså Forsvaret pålegg om at ved større investeringer skal det gjøres vurderinger på om andre myndigheter, f.eks. politiet, kan ha nytte av disse investeringene.

«Prop. 1 S (2017-2018)» er regjeringens forslag til Forsvarsbudsjett for 2018. Her kommer det blant annet frem føringer for hvilke områder innen IKT som Forsvaret skal inngå strategisk samarbeid om.

3.2 Aktører og organisering

Politiet

«Politiet skal gjennom forebyggende, håndhevende og hjelpende virksomhet være et ledd i samfunnets samlede innsats for å fremme og befeste borgernes rettssikkerhet, trygghet og alminnelige velferd for øvrig» (Justis- og beredskapsdepartementet, 2017).
Politiet skal beskytte person, eiendom og fellesgoder, og forebygge kriminalitet. De skal yte borgere hjelp og tjenester i faresituasjoner. Videre skal politiet samarbeide med andre myndigheter, og på anmodning kunne verne og yte bistand for disse. Politiet har i henhold til disponeringsskriv til politi og lensmannsetaten 2018 et budsjett i underkant av 17 milliarder kroner. Her har PIT ett budsjett i underkant av 1 milliard kroner (Politidirektoratet, 2018).

Politiets IKT-tjeneste

Politiets IKT-tjeneste (PIT) ivaretar drift, utvikling og forvaltning av IKT til politiet, tollvesenet, kriminalomsorgen og den høyere påtalemyndighet. PIT er ansvarlig for drift av all infrastruktur i hele politinettet, med i alt 17000 brukere og i overkant av 150 ulike systemer. (Politiet.no, 2018). «PIT er ganske tradisjonelt organisert med en planleggingsavdeling, en utviklingsavdeling, en driftsavdeling og en brukersupportavdeling» (R3, 2018).
Hovedtyngden av virksomheten er lokalisert i Oslo med sirka 400 ansatte. Videre er 100 ansatte fordelt på ulike lokale politi driftsenheter. De er lokale brukerstøtte representanter som ivaretar lokale driftsoppgaver. «Det viktigste systemet for PIT er Basis Løsningen (BL) som støtter hele straffesakshåndteringen helt til dom eller frifinnelse foreligger» (R3, 2018). Dette er et komplekst system med flere tilknyttede systemer. Andre viktige systemer for PIT er etterretningssystemer og politi-operative systemer. Mange av systemene som PIT leverer, er også koblet sammen med andre systemer fra andre offentlige etater som Vegvesenet, Folkerigsiterert med flere. Men PIT drifter alle sentrale systemer selv. Det er kun publikumsnære web-baserte tjenester som blir håndtert av andre aktører.

Politidirektoratet

Politidirektoratet er det øverste ledelsesnivået i politiet, og er et forvaltningsorgan underlagt Justis- og beredskapsdepartementet. «Politidirektoratets rolle og hovedoppgave er faglig ledelse, styring, oppfølging og utvikling av politidistriktene og politiets særorganer» (Justis- og beredskapsdepartementet, 2018). Direktoratet består av fem avdelinger som er avdeling for strategi, økonomi og virksomhetsstyring, politifagavdelingen, avdeling for politiberedskap og krisehåndtering, HR og HMS avdeling og en IKT-avdeling. Denne IKT-avdelingen er premissgiver for utvikling og styring av IKT-området og sikrer sammenheng mellom virksomhetens behov, prioritering og ressursbruk innen IKT (Politidirektoratet, 2018).

Forsvaret

Forsvarets samfunnsoppdrag er å forsvare Norge, sikre selvstendighet og politisk handlefrihet. Dette skal gjøres gjennom ni ulike oppgaver som er definert av Stortinget. Oppgavene er definert i blant annet Forsvarets årsrapport 2017 (Forsvaret, 2017). Forsvaret skal sikre troverdig avskrekking og forsvare Norge og allierte innenfor rammen av NATOs kollektive forsvar. Videre skal Forsvaret håndtere sikkerhetspolitiske kriser, hevde norsk suverenitet og sikre et nasjonalt beslutningsgrunnlag. De skal bidra i internasjonalt samarbeid innenfor sikkerhets -og forsvarspolitikk og dela i flernasjonal krisehåndtering. Forsvaret skal også bidra til ivaretakelse av samfunnssikkerhet og andre sentrale samfunnsoppgaver.

Forsvaret brukte ca. 34 milliarder kroner for å ivareta disse oppgavene hvorav ca. 1,8 milliarder gikk til Cyberforsvaret hvor hoveddelen av kostnadene gikk til de 1230 årsverk, som har en ca. 50/50 fordeling mellom sivile og militært ansatt personell. I tillegg til denne summen er det en betydelig investeringsportefølje for nye IKT-prosjekter. Denne er fordelt til Forsvarets Materielletat (FMA) og er i størrelsesorden 800 Millioner for 2018 (Forsvarsdepartementet, 2018). FMA er en egen etat som er underlagt Forsvarsdepartementet, men er ikke en del av Forsvaret.

Cyberforsvaret

Cyberforsvaret (CYFOR) er under omstilling og endring, men per 1. mai 2018 består Cyberforsvaret av fem underavdelinger. Det er Cyberforsvarets CIS-regiment som leder Cyberforsvarets regionale driftsorganisasjon. Cyberforsvarets IKT- tjenester er ansvarlig for sentral IKT-drift og for drift og utvikling av Forsvarets forvaltningssystemer. Cybersikkerhetssenteret skal beskytte Forsvarets operasjoner mot trusler fra det digitale rom. I tillegg har vi Cyberforsvarets våpenskole og Cyberforsvarets base -og alarmtjenester. «Cyberforsvaret er hovedaktøren innenfor utvikling og drift innenfor IKT-området i Forsvaret» (R2, 2018). «De viktigste systemene CYFOR leverer til Forsvaret, er de systemene som understøtter Forsvarets operative enheter. De er høygraderte systemer som Meldingstjenesten og FisBasis H/NS» (R2, 2018). «Administrative systemer som FisBasis B/U med over 20.000 brukere er også blitt mer og mer integrert i den operative driften, så disse er også blitt mer viktig» (R1, 2018).
Cyberforsvaret er en del av IKT-virksomheten i Forsvaret. Den viktigste aktøren i IKT-virksomheten i Forsvaret ut over Cyberforsvaret er Forsvarets Materiell etat IKT-kapasiteter (FMA IKT-kap). Denne avdelingen er blant annet ansvarlig for forvaltning av systemer, prosjektgjennomføring og innkjøp. Det finnes også egne IKT-elementer hos de ulike forsvarsgrenene, men de blir ikke omtalt i denne oppgaven.

Forsvarsstaben

Forsvarsstabens (FST) oppgave er å støtte Forsvarsjefen (FSJ) som etatsjef for Forsvaret. FST skal ivareta ansvaret for å gjennomføre oppdrag, påse at beslutninger følges opp, og være utøvende myndighet for ledelsen av Forsvaret. FST er organisert med en økonomiavdeling, plan avdeling, HR avdeling og operasjonsavdeling. I planavdelingen er det en egen IKT-seksjon som har sin hovedoppgave med å følge opp tiltak for effektiv drift og utvikling av Forsvaret ved hjelp av IKT. Denne seksjonen skal ivareta og videreutvikle Forsvarets IKT strategi og planer, samt optimaliserer IKT systemporteføljen etter Forsvarets behov. Forsvarsstaben er også sterkt involvert i nye materiell prosjekter innenfor IKT.

4 Faktorer og samarbeidsområder

I dette kapittelet vil empirien som kom frem gjennom intervjuene drøftes opp mot relevante teorier og styrende dokumenter. Ved første gjennomgang av de transkriberte intervjuene ble de ulike utsagnene og forklaringene kategorisert i henhold til tema, og dessuten hvordan dette påvirker et eventuelt samarbeid. Dette ble videre systematisert til åtte faktorer. Flere av temaene som kom frem under intervjuene var relevante for flere enn en faktor. En vesentlig del av analysearbeidet var å plassere utsagnene og temaene innenfor den faktoren der den hadde størst betydning for et eventuelt samarbeid.

Drøftingene av faktorene har til hensikt å avgjøre om disse faktorene fremmer eller hemmer et samarbeid mellom Forsvaret og politiet innenfor IKT. Et av funnene er at de fleste faktorene inneholder elementer som både fremmer og hemmer et eventuelt samarbeid, men jeg vil i del-konklusjonen under hver faktor beskrive om faktoren totalt sett vil fremme eller hemme et samarbeid mellom etatene.
Til slutt i kapittelet vil jeg komme inn på områder som respondentene mente var hensiktsmessig å samarbeide om i fremtiden, og hvilke samarbeid som pågår i dag.

4.1 Faktor økonomi

Tre av fire respondenter hevdet at økonomien var en av de viktigste faktorene som fremmet et samarbeid mellom Forsvaret og politiet. «Et samarbeid kan gi mer ut av de investerte kronene» (R3, 2018), «og sørge for at vi utnytter de offentlige midlene på en best mulig måte» (R4, 2018). Et samarbeid vil kunne ta ut økonomiske effekter på flere områder, ikke kun i form av rene investeringskostnader og kontrakter med private aktører. Momenter som ble omtalt er benyttelse av felles eiendom-bygg og anlegg (EBA), gjenbruk av eksisterende løsninger, bruk av kompetanse på tvers av etatene, og økt operativ evne med felles løsninger. Dette blir omhandlet i egne punkt eller andre steder i oppgaven.
Hvilke type økonomisk gevinst som er mulig å få ut av økt samarbeid er derfor vanskelig å anslå før dette samarbeidet konkretiseres. Dette kan gjøres i flere ulike former, det er derfor vanskelig å forutse hvilke økonomiske gevinster det er mulig å få ut av et slikt samarbeid.

Men alle aktørene nevner fremtidige prosjekter knyttet opp mot digitalisering av virksomheten. Dette vil kunne kreve store investeringer og teknologiske løft for å kunne ta ut effekter av. Jeg skal derfor komme litt inn på et tenkt scenario knyttet til dette under.

Digitalisering

Både Forsvaret og politiet har et uttrykt behov for, og tanker om ytterligere digitalisering. For å forstå hvordan digitaliseringen skal kunne gi økt produktivitet for etatene må en kjenne til begrepet, og hvordan dette bør implementeres. Digitalisering er å ta i bruk teknologi for å fornye, forenkle og forbedre (Kommunal- og moderniseringsdepartementet, 2017). Ved å innføre ny teknologi skal en effektivisere og forenkle arbeidsprosessene, både for eventuelle brukere og ansatte. Denne implementeringen kalles ofte IKT- prosjekter.
IKT- prosjekter i offentlig sektor skiller seg litt fra privat sektor. Eierskapet er muligvis den mest fremtredende forskjellen, der offentlig sektor bygger på demokratiske verdier, og eies av alle (Rainy, 1976). Dette fører til at offentlige etater ikke er ute etter å ta ut økonomiske gevinster, men effektiv ressursutnyttelse, og å kunne tilby tjenester til befolkningen. I tillegg ser man at offentlig sektor i stor grad er bundet av juridiske føringer for hvordan prosesser og prosjekter gjennomføres (Rainy, 1976). Dette er en utfordring for både politi og Forsvaret. Respondent 3 har tidligere erfaringer fra det sivile næringsliv, og ser at det er utfordringer i statlig sektor med å få midler til å gjennomføre de store løftene for å modernisere porteføljen. Dette på tross av at Respondent 3 mener at både politiet og Forsvaret er av mange ansett for å være budsjettvinnere i de siste års statsbudsjetter. Det at etatene kunne gått sammen for å ta noen av disse store løftene ville vært positivt, men det at Forsvaret og politiet har ulike behov og ønsker vil kunne gjøre et slikt prosjekt vanskelig å gjennomføre.

Dersom Forsvaret og politiet skulle inngå et tettere samarbeid for å kunne digitalisere raskere, og kraftsamle ressurser og eventuelt kjøre et prosjekt sammen, vil det oppstå utfordringer siden Forsvaret og politiet her forskjellig prosjektmodeller. Konklusjonen i rapporten «Prosjektmodeller og proskjekteierstyring i statlige virksomheter» står det at Forsvaret som eneste departement har en egen prosjektmodell, PRINSIX. Denne definerer når og hvordan Forsvarsdepartementet i de ulike fasene skal inkluderes. (Andersen, 2016). Årsaken til at Forsvarsdepartementet skiller seg ut ved å ha et tydelig eierforhold til prosjektene kan være at prosjektene samspiller med budsjettsystemet. I Forsvaret finansieres prosjekter ved at FD tildeler midler dirkete til prosjektene i FMA. Politiet har en modell der mesteparten av

prosjekter og utvikling finansieres direkte gjennom PIT. Det vil derfor være utfordringer knyttet til prosjektgjennomføring og finansiering av eventuelle felles prosjekter.

Et annet element som påvirker faktoren økonomi som ble hevdet av respondent 3 og 4 var størrelsesforholdet. Forsvarets IKT-organisasjon er betydelig større enn PIT, både med tanke på personell og økonomi. Om en ser på antall årsverk og økonomi er den nesten dobbelt så stor. I tillegg skal investeringsporteføljen innenfor IKT i Forsvaret bli betydelig større de neste årene. «Forsvaret har en annen økonomisk kraft enn det politiet har gjennom investeringsplanen på IKT området for Forsvaret. Så det er klart hvis det er mulig å utnytte det til felleskapets beste, så tror jeg de fleste vil synes det er en god ide» (R4, 2018). Dette kan gi politiet mulighet til å dra nytte av de investeringer og utvikling Forvaret gjennomfører, men dette kan også føre til at politiet ikke vil bli hørt, og dermed ikke får løsninger som er tilpasset deres behov. Det kan derfor være utfordrende. Dette vil også bli omtalt under faktoren ledelse og styring.

Delkonklusjon økonomi

Økonomi er uttalt av respondentene til å være en av de viktigste faktorene for økt samarbeid. Et hvert samarbeid bør i en eller annen form kunne gi økonomiske effekter. Dette kan være i form av bedre kontrakter med industrien, felles investeringer, reduserte lønnsutgifter med mer. Siden samarbeidet er så lite som det er i dag er det vanskelig å forutse hvilke økonomiske gevinster det er mulig å få ut av samarbeidet, men det er viktig for begge etatene «å sørge for at de utnytter de offentlige midlene på en best mulig måte» (R4, 2018). Økonomi er derfor en faktor som fremmer samarbeid.

4.2 Faktor lover og regelverk

Det er en rekke lover og regler som vil kunne påvirke et eventuelt samarbeid mellom Forsvaret og politiet. I dette avsnittet skal jeg komme inn på de lover som ble nevnt i intervjuene. Denne listen er nødvendigvis ikke utfyllende, men gir en indikasjon på de viktigste forutsetningene for et samarbeid. Det må påpekes at ingen av respondentene var jurister eller hadde inngående kjennskap til dagens lovverk, men de har bedre overordnet kjennskap til praksis enn andre utenfor fagfeltet.

Grunnloven

I en demokratisk rettstat vil bruk av militære styrker mot landets egen befolkning være høyst problematisk (Dyndal, 2010, s. 277). Norge er ikke noe unntak her. Frem til Stortingsvedtak av 13 mai 2014 om endringer i grunnloven, var det paragraf 99 som la begrensninger for bruk av militære styrker mot egen befolkning. Etter 2014 er det paragraf 101som lyder: «Regjeringen har ikke rett til å bruke militær makt mot innbyggere uten etter lov, med mindre en forsamling forstyrrer den offentlige ro, og ikke oppløses etter at de lovbestemmelser som angår opprør, tre ganger høyt og tydelig er opplest for forsamlingen av den sivile øvrighet» (Justis- og beredskapsdepartementet, 2014, s. §101). Det er kun språket som ble endre fra tidligere paragraf 99, rettstilstanden er ikke endret. Høyesterettsjustitiarius Carsten Smith uttalte til Politiforum i 2004: «at militært utstyr eller personell overhodet ikke kan brukes mot norske borgere» (Dyndal, 2010, s. 103). Om en skal legge tolkning fra Smith i 2004 til grunn vil bruk av militære IKT-ressurser kunne bli problematisk. Årsaken til dette kommer fra Alta-aksjonen i 1979 der politiet ønsket å benytte militært materiell får å få kontroll på demonstrantene. Her var det snakk om at dette materiellet som, biler og helikoptre, skulle settes inn mot de sivile demonstrantene. Denne restriktive tolkningen er blitt noe oppmyket etter 22. juli terroren. Det er innført en ny paragraf i politiloven som omhandler bruk av militære kapasiteter der det blant annet står: «Utenfor tilfeller som nevnt i første ledd kan Forsvaret etter anmodning bistå politiet med materiell, spesialkyndig operatørpersonell og annet» (Justis- og beredskapsdepartementet, 2017, s. §27A). Dette vil da kunne gjelde for IKT-materiell. Det er derfor etablert et skille ved at militær maktbruk i indre politiske uenigheter er noe helt annet enn at Forsvaret bistår politiet med å beskytte befolkningen mot terrorister (Håkenstad, 2016).

IKT ligger tradisjonelt litt utenfor det man kan kalle en tradisjonell militær kapasitet, som kan benyttes mot egen befolkning. Men i dag er tilgang til internett blitt allemannseie, og demonstrasjoner i dag har ofte større effekt ved å benytte internettkampanjer enn fysiske demonstrasjoner. I denne oppgaven ser jeg på et teknisk og administrativt samarbeid mellom etatene, men om Forsvarets personell og materiell skulle bli satt inn for å bekjempe en kampanje eller trussel på internett fra egen befolkning, vil dette kunne bli problematisk. En annen utfordring med dette er at cybertrussel ofte er internasjonal, da internett ikke

nødvendigvis forholder seg til landegrenser. Det er nok en av årsakene til at respondent 4 var klar på at det måtte være en skillelinje mellom Forsvarts og politiets ansvarsområder. Deling av informasjon mellom etatene kunne være problematisk. Dette vil kunne påvirke et eventuelt samarbeid mellom Politiets sikkerhetstjeneste (PST) og Forsvarets etterretningstjeneste. Ettertingstjenesten kan ikke «på norsk territorium overvåke eller på annen fordekt måte innhente informasjon om norske fysiske eller juridiske personer» (Forsvarsdepartementet, 1998). Dette blir ikke omtalt i denne oppgaven.

Sentrale prinsipper for samfunnssikkerhet

Et element som respondent 1 nevner, kan ha innflytelse på et samarbeid mellom Forsvaret og politiet, er sektorprinsippet. Sektorprinsippet foreskriver at hver statsråd styrer sin sektor, og har et konstitusjonelt ansvar og kompetanse innenfor sitt myndighetsområde (Forsvarsdepartementet, 2016). Dette prinsippet står sterkt i forvaltningen, og flere av informantene i rapporten «Mot alle odds-veien til samordning i norsk forvaltning» utgitt av Direktoratet for forvaltning og IKT, peker på dette ministeransvaret som en reell hindring for tverrsektoriell oppgaveløsning. Andre uttrykker bekymring for at ministeransvaret tolkes for strengt, og de tror det er et uutnyttet handlingsrom for samordning. (Direktotorat for forvaltning og IKT, 2014, s. 28). Professor Eivind Smith skriver i artikkelen «Ministerstyre-et hinder for samordning?» at sviktende samordning aldri kan unnskyldes med bakgrunn i sektorprinsippet og fagstatsrådens individuelle ansvar. «Når de ulike sektorene i sentralforvaltningen, til skade for landets ve og vel ikke virker sammen, er det regjeringens plikt å gripe inn (Smith, 2015).

Av de 4 prinsipper for beredskap og krisehåndtering, henger dette sammen med ansvarsprinsippet. «Ansvarsprinsippet innebærer at alle organisasjoner som til daglig har ansvaret for et fagområde, også har ansvaret for samfunnssikkerheten på området uavhengig av type hendelse» (Justis- og beredskapsdepartementet, 2016, s. 20). Dette innebærer at politiet og Forsvaret selv er ansvarlige for å opprettholde viktige funksjoner og oppgaver innenfor egen organisasjon. Dette kan gi utfordringer også knyttet til IKT. Dersom f.eks. forsvaret leverte et kritisk IKT-system til politiet, ville ikke politiet eller Justisdepartementet selv sitte på ansvaret. Det er nok en av årsakene til at to av respondentene er kritisk om et samarbeid om IKT-systemer som understøtter kjernevirksomheten. For politiet var dette den

polisiære virksomheten, og for Forsvaret var dette utstyr som militære radioer og Link systemer som er viktige for den operative delen av virksomheten.

«Likhetsprinsippet innebærer at organisasjonen under en krise skal være mest mulig lik den daglige organisasjonen» (Justis- og beredskapsdepartementet, 2016, s. 20). Dette er nært knyttet til ansvarsprinsippet da dette skal påse at erfaringer, roller og ressurser som er opparbeidet gjennom det daglige arbeidet blir effektivt benyttet under kriser eller større hendelser. Kriser kan treffe forskjellige, og en krise som f.eks. treffer justissektoren trenger ikke nødvendigvis treffe Forsvaret. Vil da Forsvarets ressurser som eventuelt understøtter politiets IKT-systemer være tilgjengelige? Bruk av Forsvarets ressurser for støtte til politiet er ytterligere beskrevet i avsnittet om bistandsinstruksen, men denne er ikke tiltenkt å dekke daglige hendelser. Dette bringer oss over på nærhetsprinsippet. «Nærhetsprinsippet innebærer at kriser skal håndteres på lavest mulig nivå» (Justis- og beredskapsdepartementet, 2016, s. 21). Det vil si at en krise innenfor en virksomhets ansvarsområde er det virksomheten selv som har ansvar for å håndtere.

«Samvirkeprinsippet presiserer at ansvarlige myndigheter, virksomheter og etater skal sikre best mulig samvirke og samarbeid med alle relevante aktører i arbeidet med forebygging, beredskap og krisehåndtering» (Justis- og beredskapsdepartementet, 2016, s. 21). Et økt samarbeid mellom etatene innenfor IKT vil derfor kunne bedre operativ evne og beredskap. Dette kommer jeg nærmere inn på i et eget punkt i studien.

Bistandsinstruksen

Bistandsinstruksen legger også føringer for hvordan et samarbeid mellom politi og Forsvaret skal være. «Formålet med denne instruksen er å gi retningslinjer for Forsvarets bistand til politiet, slik at samfunnets samlede ressurser utnyttes best mulig innenfor de rammer som følger av lov og Grunnlov» (Regjeringen, 2017, s. §1). Denne instruksen går på hvilken bistand Forsvaret kan gi politiet dersom politiets egne ressurser antas å ikke være tilstrekkelig eller tilgjengelige. Denne gjelder altså kun støtte til politiet fra Forsvaret og ikke motsatt. Instruksen er rettet mot operative forhold, men den presiserer at Forsvaret kan etter anmodning bistå politiet med materiell og spesialkyndig operatørpersonell. I et IKT perspektiv vil dette si at politiet kan be Forsvaret om bistand i form av IKT-materiell, eller

støtte ved alvorlige hendelser i cyberdomene. Alle respondentene nevner denne instruksen som grunnleggende for samarbeid, men ingen mener denne er begrensende for samarbeid. Dette henger i stor grad sammen med at denne instruksen ikke inneholder noen form for føringer på samarbeid ut over politiets behov for støtte og bruk av Forsvarets allerede eksisterende kapasiteter. Denne instruksen gir derfor ingen begrensninger eller føringer for et økt teknisk og administrativt samarbeid innenfor IKT.

Sikkerhetsloven

Den loven som oftest ble nevnt av respondentene både fra politiet og Forsvaret som kunne påvirke og legger føringer for et eventuelt samarbeid mellom etatene, var lov om forebyggende sikkerhetstjeneste, ofte kalt sikkerhetsloven. «Formålet med denne loven er å: a) legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet, og andre vitale nasjonale sikkerhetsinteresser b) ivareta den enkeltes rettssikkerhet, og c) trygge tilliten til, og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjenester» (Forsvarsdepartementet, 2017, s. §1). Denne loven med tilhørende forskrifter har vært førende for store deler av Forsvarets sin virksomhet, og spesielt innenfor IKT. Gjennom forskrifter blir det blant annet satt tekniske krav til IKT-systemene og krav til behandling av data.

Denne loven er under revidering, og proposisjon til Stortinget 153 L (2016- 2017) er under behandling. Dette lovforslaget er en modernisering av tidligere lov, og har som mål å sette myndigheter og virksomheter i bedre stand til å sikre de nasjonale interessene mot et trusselbilde- og risikobilde i stadig endring. «Forslaget vil styrke samhandlingen mellom myndigheter og virksomheter slik at forebyggende sikkerhetsarbeid mot terror, sabotasje og spionasje kan gjennomføres på en mer effektiv og forsvarlig måte, på tvers av alle samfunnssektorene» (Forsvarsdepartementet, 2016, s. 7). I denne lovendringen kommer det frem at det er et ønske om en bedre samhandling mellom flere offentlige og private aktører innenfor sikkerhet.

Implementering av denne loven vil kunne endre kravene til IKT. Dette vil spesielt kunne ramme politiet da de i dag har få informasjonssystemer som er tilpasset behovet for gradert informasjon. «Vi i politiet selv har lite graderte systemer. Det er egentlig en del av

utfordringen vår, at vi har lite informasjonssystemer som er tilpasset behovet for gradert informasjon og håndtering av dette. Vi har kartlagt behovet, og alle virksomhetsområdene har behov for det, men vi har det ikke selv» (R4, 2018). I dag benytter politiet Politiets Sikkerhetstjenestes (PST) graderte nett, og i en liten utstrekning Forsvarets graderte systemer. Revidering av Sikkerhetsloven vil kunne gjøre denne utfordringen større. Begge respondentene fra politiet fremhevet derfor ønske om samarbeid innen graderte systemer og kryptografi. Dette var et område som Forsvaret har mye kompetanse og erfaringer på, og som politiet gjerne ønsket å dra nytte av i et samarbeid.

Et annet moment som kom opp fra respondentene i intervjuene som har knytninger til Sikkerhetsloven var leverandørsikkerhet. Ved sikkerhetsgraderte anskaffelser og anskaffelser av kritisk infrastruktur stilles det krav til leverandøren. «Leverandøren skal uten ugrunnet opphold orientere Nasjonal Sikkerhetsmyndighet om endringer i styre eller ledelse, forandring i eierstrukturen, flytting av lokaliteter og utstyr, åpning av gjeldsforhandlinger eller begjæring om konkurs og andre forhold som kan ha betydning for leverandørens sikkerhetsmessig sikkerhet» (Forsvarsdepartementet, 2017, s. §28). Dette blir fremhevet som en utfordring av respondentene med dagens leverandører og sivile samarbeidspartnere. IKT-systemer består i dag av utstyr og programvare fra en rekke forskjellige leverandører. Disse leverandørene benytter igjen mange forskjellige underleverandører. Leverandører og underleverandører har i tillegg ofte komplekse eierforhold som gjør det vanskelig å vite hvilken nasjon og eier som står bak leveransene. Eksempler på dette er da en indisk IT arbeider stanset produksjon på Mongstad grunnet en tastefeil (Remen A. T., 2016), og utenlandske IT-arbeidere fikk tilgang til sensitive pasientdata fra Helse Sør-Øst (Remen A. T., 2016). «Politiet har derfor fått føringer for Justis -og Beredskapsdepartementet der hensyn til informasjonssikkerhet og tilgjengelighet i politiets tjenester, gjør at vi må ha gode vurderinger knyttet til bruk av markedet» (R4, 2018). Politiet er derfor blitt mer opptatt av leverandørsikkerhet, og mener at dette styrker muligheten for fremtidig samarbeid med Forsvaret. «Begge organisasjonene har en forståelse av viktigheten av å beskytte systemene og dataene man sitter på» (R3, 2018). Men her kan det virke som Forsvaret og politiet har ulike føringer fra departementene på hvordan etatene skal forholde seg til outsourcing av tjenester. Det kan virke som om Forsvaret har tydeligere føringer for outsourcing enn det politiet har fått. Respondent uttalte: «Og nå ser vi jo at Forsvaret, slik jeg har oppfattet det i alle fall, har lagt seg på en strategi som er litt annerledes enn den politiet har gjort. Nemlig sagt at man skal kjøpe så mye som overhodet

mulig» (R4, 2018). Det vil si at Forsvaret ønsker å benytte private leverandører så mye som mulig. Dette blir også nevnt av Respondent 1 fra FST som refererer til proposisjon til Stortinget 1 S (2017-2018). Her står det: «Øvrige leveranser og oppgaver vil i økende grad bli ivaretatt gjennom et utvidet strategisk samarbeid med NATO, allierte, næringslivet og andre virksomheter. Strategisk samarbeid planlegges etablert innenfor IKT tjenesteområdene operativ beslutningsstøtte, forvaltning, stasjonære og mobil kommunikasjonsinfrastruktur samt innenfor IKT-plattform og datasenterløsninger». (Forsvarsdepartementet, 2017, s. 21). Videre står det: «Harmonisering av IKT-porteføljen i forsvarssektoren, standardisering, og økt bruk av IKT utviklet til sivile formål, også for militære formål, skal være bidrag i finansieringen av satsningen på IKT» (Forsvarsdepartementet, 2017, s. 21). Det er derfor grunn til å anta at Forsvaret ønsker mer bruk av sivile leverandører for sine IKT-leveranser, som er i motsetning til det politiet ønsker, å ta mer ansvar selv for sine leveranser. Konsekvensen av dette er at det kan bli en utfordring i forhold til samarbeid med tanke på ulikt syn på sivile leverandører, samtidig som det fremmer et mulig strategisk samarbeid mellom etatene.

Personopplysningsloven

Personopplysningsloven er en av de lovene som påvirker kravene til politiets IKT-løsninger. Mye av informasjonen som politiet besitter om personer i Norge skal behandles etter denne. «Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger» (Justis- og beredskapsdepartementet, 2015, s. §1). Denne loven gjelder også for Forsvaret, men om en ser bort i fra Etterretningstjenesten og vernepliktsforvaltning, så behandler Forsvaret i liten grad personopplysninger som ikke omhandler eget personell. Forsvaret er i større grad påvirket av sikkerhetsloven. Dette er beskrevet under punktet for sikkerhetsloven. Det er derfor naturlig at denne loven påvirker politiets løsninger mer enn Forsvaret, selv om begge må forholde seg til denne.
Derfor har politiet også en egen lov om behandling av personopplysninger i politiet og påtalemyndigheten. «Formålet med loven er å bidra til effektiv løsning av politiets og påtalemyndighetens oppgaver, beskyttelse av personvernet og forutberegnlighet for den enkelte ved behandlingen av opplysninger» (Justis- og beredskapsdepartementet, 2016). Denne loven gir føringer for mange av politiets IKT-systemer, deriblant et av de viktigste systemene til politiet som heter Basis Løsningen (BL), som respondent 3 fremhevet som et av

de viktigste systemene. Denne loven gir ingen føringer for at systemet skal være gradert begrenset etter sikkerhetsloven.

Andre lover og regelverk

«Lov om offentlige anskaffelser» er også en lov som blir nevnt av respondentene som kan legge føringer for samarbeidet. «Loven med tilhørende forskrifter skal bidra til økt verdiskapning i samfunnet ved å sikre mest mulig effektiv ressursbruk ved offentlige anskaffelser basert på forretningsmessighet og likebehandling» (Nærings og fiskeridepartementet, 2017, s. §1). Denne går i første rekke på hvordan det offentlige skal forholde seg til private aktører, og dette vil være likt både for politiet og Forsvaret. I tillegg til denne er det en forskrift om Forsvar og sikkerhetsanskaffelser: Denne presiserer i tillegg til anskaffelsesloven at formålet også er å ivareta behovet for å utvikle og opprettholde en europeisk forsvar- og sikkerhets teknologisk og industriell base (Forsvarsdepartementet, 2018, s. §1). I §4-1 i denne loven står det at denne gjelder for offentlige myndigheter, statlige, fylkeskommunale eller kommunale myndigheter og sammenslutninger dannet av en eller flere av disse. Denne loven er derfor ingen hindring for et eventuelt samarbeid mellom Forsvaret og politiet innenfor IKT.

Et annet regelverk som blitt tatt opp av respondent 1, er Meld.St.9 (2015-2016) som omhandler forholdet mellom forsvarsektoren og forsvarsindustrien. Regjeringens hovedmål med meldingen er å ivareta nasjonale sikkerhetsinteresser gjennom å opprettholde og videreutvikle en internasjonalt konkurransedyktig norsk forsvarsindustri. (Forsvarsdepartementet, 2015). «Denne meldingen gir et signal fra regjeringen om at man ønsker at Forsvaret i større grad skal samarbeide med næringsliv og industri, og for så vidt andre aktører» (R1, 2018). Denne meldingen omhandler ikke samarbeid med andre offentlige etater, men den viser at Forsvaret ønsker å samarbeide med flere ulike aktører for å ivareta nasjonale sikkerhetsinteresser, gjennom å opprettholde og videreutvikle en internasjonal konkurransedyktig norsk forsvarsindustri.

Delkonklusjon lover og regelverk

Respondentene hadde ikke inngående kjennskap til hvilke lover og regelverk som vil være førende for et eventuelt samarbeid. Tolkningen av tidligere grunnlovsparagraf 99, nå §101 angående bruk av militært materiell, kan være problematisk dersom IKT-materiellet ble benyttet mot innbyggere i Norge. Sektorprinsippet kan være en utfordring for samhandling på departementsnivået, men dette er ikke i fokus i denne oppgaven. Bistandsinstruksen gjør det mulig for politiet å benytte allerede eksisterende kapasiteter ved behov. Det kan virke som for politiet er personopplysningsloven det mest førende for politiets IKT-systemer, mens det fra Forsvarets side er mer knyttet opp mot Sikkerhetsloven. Lovene gjelder for begge, og med forslaget til ny sikkerhetslov Prop.153 L vil denne i større grad enn tidligere treffe politiet og IKT-virksomheten der. Denne har også som et uttalt mål å fremme samarbeid for å bedre sikkerheten. Selv om lovverket stiller litt forskjellige krav til IKT-systemene er det ingenting som tyder på at dette legger hindringer for et økt samarbeid innenfor IKT. Som R2 uttalte i intervjuet, har de så langt ikke funnet noen lover eller regelverk som hindrer et økt samarbeid mellom Forsvaret og politiet.

4.3 Faktor ledelse og styring

Det at Forsvaret og politiet er underlagt to forskjellige departementer kan gjøre samhandling og samarbeid mer utfordrende. «Den formelle beslutningsmyndighet er etter norsk forfatning tillagt det enkelte fagdepartement, eller Kongen i statsråd. Hver enkel statsråd er konstitusjonelt og parlamentarisk ansvarlig for det saksområdet vedkommende er satt til å styre» (Justis- og beredskapsdepartementet, 2012). Dette er beskrevet tidligere under sektorprinsippet. Oppdraget til politiet og Forsvaret er forskjellig, og dette vil føre til at departementet som det står over, er ansvarlige for underliggende etater. Det kan med andre ord oppstå interessekonflikter på overordnet nivå for hvordan IKT skal utvikle seg innenfor de forskjellige etatene. Dette henger sammen med de ulike oppdragene departementene har. I tillegg har Justis- og Beredskapsdepartementet (JBD) og Forsvarsdepartementet (FD) en forskjellig tilnærming til hvordan prosjekter i etaten skal styres. Nå har ikke denne oppgaven hatt til hensikt å se på hvordan departementene ser på et eventuelt samarbeid innenfor IKT,

men både politiet og Forsvaret har fått føringer fra overordnet departement om at en skal vurdere et ytterligere samarbeid.

Justis- og Beredskapsdepartementet og Forsvarsdepartementet samarbeider allerede om en rekke forhold. Kystvakten er en del av Forsvaret, men driver polisiære oppgaver på vegne av Norge i norske farvann. Redningstjenesten er også et samarbeid mellom departementene. I tillegg her vi Nasjonal sikkerhetsmyndighet (NSM) som ligger under FD, men har viktige oppgaver som ligger under Justis- og beredskapsdepartementet. Nasjonal Sikkerhetsmyndighet er Norges ekspertorgan for informasjon – og objektsikring, og det nasjonale fagmiljøet for IKT-sikkerhet. (Nasjonal sikkerehtesmyndighet, 2014). NSM støtter både Forsvaret og politiet ved ekspertise innen disse fagfeltene. Og her er IKT-sikkerhet en viktig del av samarbeidet. Så selv om det i Sikkerhetsfag råd fra NSM til FD står at det er for dårlig utviklede samvirkemekanismer mellom de ulike aktørene (Najonal Sikkerhetsmyndighet, 2015, s. 23), så er disse to departementene godt kjent med samarbeid.

Et tema som blir presentert fra Forsvarets aktører under intervjuene er momentet knyttet til organisering, ansvar og myndighet innenfor IKT i Forsvaret. I dag er dette ansvaret fragmentert. «Det er ikke en tydelig aktør som kan ta initiativ til å sitte med makt og ressurser til å gjennomføre dette» (R1, 2018). Det er flere aktører i Forsvaret som har ulikt ansvar og myndighet innenfor IKT i Forsvaret. FSTs planavdeling har en seksjon som har en koordinerende rolle innenfor IKT-område. Cyberforsvaret er hovedaktøren på alle felles IKT systemer og er ansvarlig for drift av disse. FMA IKT-kap er den aktøren som har ansvar for forvaltning av systemene, og gjennomføring av nye IKT-prosjekter. FD har en rolle knyttet til nye investeringer. I tillegg har de ulike forsvarsgrenene systemer som de selv er ansvarlig for. Tidligere sjef for Cyberforsvaret, Odd Egil Pedersen, uttalte under et foredrag på Oslo militære samfunn at: «utfordringen for meg er at det er flere sjefer med delansvar for IKT i Forsvaret, som opererer med dels ulike mål og prioriteringer» (Pedersen, 2015). Denne utfordringen ble adressert i Stortingsproposisjon 151 S, der det blir definert at Cyberforsvaret skal utvikles videre til en helhetlig organisasjon for IKT-virksomheten i Forsvaret. Ansvarsdelingen internt i forsvarsektoren og grensesnitt mot andre aktører skal gjennomgås videre (Forsvarsdepartementet, 2016, s. 72).

I tråd med dette har arbeidet med en gjennomgang av omstrukturering og modernisering av cyber- og IKT-virksomheten i Forsvaret begynt. Det ble skrevet et mandat for utredning. En av disse delutredningene skulle omhandle Forsvarsektorens bistand og støtte til aktører utenfor forsvarsektoren innenfor cyber- og IKT-området. Denne utredningen skulle etter planen ha vært ferdig innen 31/12 2017, men av ukjente årsaker er den blitt forsinket. Det er derfor per tid ikke kjent hvor dette arbeidet står. Det at denne utredningen er forsinket, og at Forsvaret de seneste årene har vært under omstilling, har ført til konkrete vanskeligheter med samarbeid.

Et eksempel som kom frem under intervjuet med respondent nummer 4, var ønske om et samarbeid innenfor EBA. Politiets inntrykk var at Forsvaret hadde vanskelig for å kunne planlegge langt frem i tid: «Dersom politiet skal realisere noe, hvordan vet vi at det ikke to år senere havner på en liste som skal avhendes, og så har man investert tungt» (R4, 2018). Dersom politiet skal investere sammen med Forsvaret er de avhengige av forutsigbarhet. Det kan for politiet virke som Forsvaret stadig endrer planer og lokasjoner. Omstillingsaktivteten i IKT-virksomheten i Forsvaret med stadige endringer, og det at IKT-utredingen ikke er ferdigstilt kan derfor hindre et samarbeid med politiet.

En annen utfordring knyttet til ledelse og styring som flere av respondentene mener hemmer et økt samarbeid, er prioritering og prioriteringsmekanismer. Dette er i dag utfordrende å bli enige om internt i etatene om hvilke prioriteringer som skal gjelde innenfor IKT-området. Hvilke prosjekter skal prioriteres, og hvilke type løsninger og teknologi skal vi satse på? Denne jobben blir enda vanskeligere når to etater må bli enige. Men om Forsvaret og politiet skal samarbeide er det straks andre som også ønsker å være med, og en må da i tillegg vurdere å koordinere med PST, NSM, FMA og andre etater som ligger under samme sektor. Som Respondent 4 uttaler: «Plutselig er det to sektorer, og ikke bare to organisasjoner (R4, 2018). Respondent 3 uttaler videre: «Jeg tror det er lurt at bare politiet og Forsvaret samarbeider. Jeg tror det er mer enn nok krevende i forhold til prioritering og størrelse. For det er veldig fort gjort fra politikerhold å se at da bare slår man sammen alt mulig» (R3, 2018).

Styringen av eventuelle felles prosjekter vil derfor være veldig krevende. «Og viljen må være tilstede hos begge parter. Hvis den ikke eksisterer så vil ikke dette fungere» (R1, 2018). Men alle respondentene var klar på at viljen til samarbeid var tilstede, og respondent 4 kom også

med konkrete eksempler der Forsvaret, med støtte fra andre aktører under FD, hadde fått ting til. Eksiterende samarbeid kommer jeg inn på senere i oppgaven.

Delkonklusjon ledelse og styring

Det at Forsvaret og politiet er plassert i to forskjellig sektorer, vil føre til utfordringer ved ledelse og styring. Prioriteringer innenfor prosjekter og hvilke løsninger og krav som gjelder, er en utfordring for begge etater i dag. Når to etater har forskjellig oppdrag og forskjellig økonomi blir dette enda vanskeligere. I tillegg er det interne utfordringer knyttet til ledelse og styring av IKT-virksomheten i Forsvaret. Faktoren ledelse og styring vil derfor kunne hemme et økt samarbeid mellom etatene

4.4 Faktor kulturforskjeller

Alle respondentene nevner at ulike kulturer i Forsvaret og politiet kan påvirke et samarbeid mellom de to etatene. Men ingen hevder at dette er av en avgjørende karakter. Litteraturen gir mange ulike definisjoner av hva kultur er i ulike organisasjoner, og hvordan dette påvirker organisasjonen og menneskene som jobber der. Den definisjonen jeg forholder meg til i denne oppgaven er: «Organisasjonskultur forbindes med de uformelle normene og verdiene som vokser frem, og har betydning for livet i og virksomheten til formelle organisasjoner» (Christensen, 2015, s. 52). Både politiet og Forsvaret har sine egne organisasjonskulturer som påvirker både det indre livet i organisasjonen, og eventuelt samhandling med andre aktører. Begge disse kulturene er påvirket av at de begge er uniformerte avdelinger, og som har et samfunnsoppdrag om å forvalte statens voldsmonopol i Norge. Politiet i fredstid og for innbyggerne i landet, Forsvaret i krigstid og for en ekstern trussel.
Begge etater bruker begrepet sivile om andre og militær/uniformert om seg selv.

Det som kommer frem i intervjuene er i stort de kulturforskjellene som påvirker de forskjellige IKT-miljøene fra operativ side. I politiet har de en kultur som fremhever raske løsninger. «Politiets IKT-tjenester og personell må være på, og virke til enhver tid. Det er ikke akseptabelt at politiet ikke er tilstede og virker hele tiden, samtidig som de har daglig kontakt med publikum. Politiet kan ikke låse seg inn i en bunkers, slik det til en viss grad er akseptert at Forsvaret gjør» (R3, 2018). Denne kulturforskjellen fører til litt ulike krav til IKT-systemene som også fører til litt forskjellig bruk av sikkerhetsloven. Men både politiet og

Forsvaret er opptatt av å ha en god sikkerhetskultur, både med tanke på eget personell og ikke minst beskyttelse av informasjonen på systemene. I tillegg vil denne kulturforskjellen påvirke prosessene rundt IKT forskjellig. En kan anta at Forsvaret vil ønske å gjennomføre lengre og grundigere planprosesser, og ha et ønske om å ikke vise løsningene frem for det offentlige. Politiet vil på den andre siden ha et fokus på raskere saksbehandling og løsninger som vil støtte opp om deres behov for kontakt med publikum. Samtidig fremhever alle respondentene at kulturen ikke burde være noen hindring for samarbeid innenfor IKT. Hovedårsaken til dette er at begge organisasjonene understøtter uniformert personell, med mange fellestrekk både i organisering, og prioriteringer opp mot samfunnsoppdraget etatene har. I tillegg består PIT og IKT-organisasjonen i Forsvaret både av personell med fagutdanning innen politi eller forsvar, og en stor andel av sivile fagspesialister. PIT består stort sett av personell med sivil bakgrunn, mens det i Forsvaret er en andel 50/50 mellom sivile og militært utdannede. Disse sivile har ikke den samme kulturen som uniformert personell. Disse besitter i tillegg til den interne kulturen en mer IKT relatert kultur som er formet fra sivile skoler og miljøer.

Det er i dag også stadig flere personer som har arbeidserfaringer fra begge etater, enten som ansatt eller som leverandør, og dermed besitter kompetanse og kulturforståelse fra begge etater. Ett eksempel kan være respondent 4 i POD som har utdanning fra Forsvaret, og har tidligere jobbet i informatikkstaben i Forsvarets overkommando. Etter 22. juli terrorangrepet har det også vært et økt fokus på samhandling mellom etatene, som blant annet har ført til at det i dag sitter liaisoner fra Forsvaret i politiet, og fra politiet i Forsvaret. Denne funksjonen er knyttet opp mot det operative, men det viser at det er vilje fra begge parter at det er et ønske om å bedre samarbeidet.

Når respondentene fra både forsvaret og politiet ble spurt om hvilke offentlige etater de anser for å være mest hensiktsmessige å samarbeide med innenfor IKT fremhevet de begge hverandre. Et av argumentene de benyttet er kultur. De fremhevet den uniformerte kulturen, sikkerhetskultur og det at det er en kultur for samarbeid på andre arenaer enn IKT mellom disse etatene. Politi og Forsvar har mer felles kultur enn med andre offentlige aktører, som det kunne være muligheter for et samarbeid med. Kulturen vil derfor kunne påvirke hvordan samarbeidet blir, samtidig som den fremhever samarbeid mellom akkurat disse to aktørene.

Delkonklusjon kulturforskjeller

Det er kulturforskjeller mellom Forsvaret og politiet, og dette vil påvirke et samarbeid innenfor IKT. Samtidig er kulturene i Forsvaret og politiet mer lik hverandre enn andre offentlige etaters kulturer. I tillegg består IKT-miljøene i etatene av store deler sivile fagspesialister som ikke er i like stor grad påvirket av den militære eller politi kulturen som de operative er. Kulturfaktoren kan derfor være hemmende for at samarbeid mellom politiet og Forsvaret, samtidig som den fremmer et samarbeid mellom dem fordi de har flere likhetstrekk i kulturen sett opp mot andre offentlige etater og samarbeidspartnere.

4.5 Faktor media

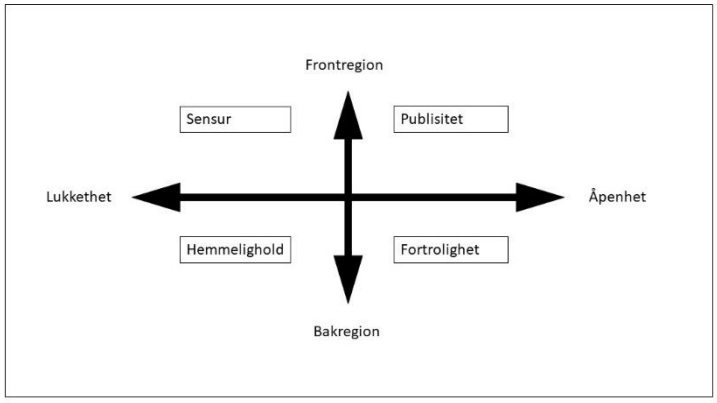
Respondent 3 mente at det var viktig å ikke undervurdere medias oppmerksomhet knyttet til et økt samarbeid mellom etatene. «Det går sikkert an å vinkle dette negativt på en eller annen måte» (R3, 2018). Eksemplet som ble tatt opp under intervjuet, var den da aktuelle saken som ble publisert av NRK angående Etterretningstjenesten som samlet data om nordmenn fra lyttestasjon på Eggemoen (Skille, 2018). Skal ikke diskutere innholdet i denne saken i detalj, men den omhandler etableringen av en avansert lyttestasjon til mange hundre millioner kroner, som er betalt av Norge, med støtte fra den amerikanske etterretningsorganisasjonen NSA. Dette var en del av amerikanske dokumenter lekket av varsleren Edward Snowden. Det er blitt stilt spørsmålstegn med lovligheten av at norsk etterretning samler inn metadatasøk som kan inneholde informasjon om nordmenn i Norge. Ett lignende scenario kan oppstå dersom politiet og Forsvaret samarbeider om IKT-systemer. Politiet, og kanskje spesielt PST, har som oppdrag å innhente informasjon om nordmenn dersom de har en rettslig kjennelse på dette. Forsvaret har ikke denne rettigheten. Selv om et samarbeid ikke nødvendigvis inneholder samarbeid om informasjon som ligger på datasystemene, og det finnes sikkerhetsgodkjente løsninger for dette, vil det være vanskelig å argumentere for at det ikke finnes muligheter for at informasjon utilsiktet kan gå på tvers av etatene. Dette vil gjerne være komplekse systemer som ikke nødvendigvis journalister eller samfunnet har nødvendig kunnskap om til å kunne forstå.

Nå skal ikke denne oppgaven handle om medienes makt, men enkelte teorier kan klargjøre noen av utfordringen med media ved et samarbeid. Mediene er ute etter overskrifter, og ikke

informasjon om hvordan dette løses teknisk. De ser på seg selv som den 4.statsmakt, og har et oppdrag om å etterspørre informasjon og være kritiske på samfunnets vegne.
I følge Eide og Hernes «triangelhypotese» har mediene makt til å påvirke hvordan aktør A forholder seg til aktør B (Eide, 1987, s. 30). I tillegg er konflikt ofte et hovedelement i mediesaker, og media har en tendens til å ha en regisserende rolle over nyheten de dekker. «Poenget er at media i sin dramatisering ikke overlater til partene selv «å komme ut på banen» de tar kontakt for å få dem til å ta stilling. Media gjør dermed aktørene til sine medspillere ved å gjøre dem til motspillere i en konflikt» (Eide, 1987, s. 133). En vil derfor kunne oppleve at Forsvaret og politiet blir spilt opp mot hverandre.

Både politiet og Forsvaret er interessert i å ha et godt forhold til media og journalister. Begge etater har presseavdelinger som i tillegg til å svare på henvendelser fra journalister, også ønsker å spre sitt budskap til opinionen. En nyhet som virker å ha blitt skrevet av en journalist, vil være mye større fordel for kilden enn en reklamesnutt eller annonse (Allern, 1997, ss. 72-74). Dette er derfor likt for begge, men på den andre siden har vi informasjonshindre. I boken: «Negotiating control. A study of News Sources» (Ericson, 1989), blir det presentert en modell om hva pressen kan forvente å møte i relasjon med kilder.

Figur 1 Relasjon med kilde



Frontregionen sier noe om hva kilden presenterer i det offentlige rom, og det som er tilgjengelig for offentligheten. Bakregionen er det som holdes internt i virksomheten. I begge regioner kan virksomheten være åpen eller lukket. I den åpne delen av frontregionen vil informasjon bli presentert, og i den lukkede delen vil informasjonen som blir presentert bli

sensurert. I den åpne delen av bakregionen vil informasjon bli spredt i fortrolighet, og i den lukkede vil den holdes hemmelig. Jeg skal ikke komme inn på detaljer om hvordan Forsvaret eller politiet forholder seg til mediene, og journalister vil møte alle de fire forskjellige hindringene hos begge etater, men det er verdt å legge merke til at politiet og Forsvaret opp gjennom historien har hatt litt forskjellig forhold til mediene. Frem til innføringen av Nødnett, som ble etablert mellom 2007- 2015, var store deler av politiets operative samband åpen og tilgjengelig for journalister. Det er faktisk kommet klager fra media at de ikke får den informasjonen de trenger fra politiet (Mossin, 2015). Flere kilder i media hevder at dagens løsning med at politiet benytter tjenesten Twitter for å informere media, ikke er tilstrekkelig for at journalister kan kontrollere at politiet gjør den jobben de skal. Forsvaret derimot, har en annen historikk. Militærmakten har hatt en ryggmargsrefleks om å skjerme seg mot mediene (Bøe-Hansen, 2011, s. 215). På grunn av samfunnsoppdragets natur og sikkerhetsloven, har Forsvaret ofte holdt informasjonen hemmelig og lukket. Om dette har stor betydning for et samarbeid innenfor IKT er lite trolig, men forskjellige erfaringer og kultur for håndtering av media kan gi media større muligheter for å dramatisere og sette partene opp mot hverandre.

Delkonklusjon media

Politi- og forsvarssaker vil alltid være interessant stoff for mediene. Et eventuelt samarbeid mellom politiet og Forsvaret innenfor IKT vil også være det, og media kommer til å benytte de metodene de har for å dekke dette. Det er selvfølgelig en mulighet for at mediene kommer til å prøve å sette etatene opp mot hverandre, og skape overskrifter knyttet til et slikt samarbeid. Men samtidig burde dette ikke være en stor utfordring dersom samarbeidet foregår i ordnede former. Faktoren media kan dermed sies å være svakt hemmende for et samarbeid.

4.6 Faktor kompetanse

Respondent 3 fremhever kompetanse som en av de viktigste faktorene som fremmer et samarbeid mellom etatene. Kompetansebegrepet er sammensatt og flerdimensjonalt og kan defineres på en rekke forskjellige måter. En definisjon på kompetanse er: «Kompetanse er de samlede kunnskaper, ferdigheter, evner og holdninger som gjør det mulig å utføre aktuelle oppgaver i tråd med definerte krav og mål» (Lai, 2013, s. 46). I dette tilfellet vil det gjelde kunnskaper, ferdigheter, evner og holdninger som gjør det det mulig å utføre ulike oppgaver

innenfor fagfeltet IKT. Dette kan være ingeniører, programmerere, prosjektledere med flere som har kompetanse innen IKT.

En rapport utgitt av IKT Norge fra 2015 har kartlagt hvor mange IKT-arbeidsplasser som mangler i den norske IKT-næringen. I henhold til undersøkelsen mangler norsk IKT-næring i 2015 6300 IKT-arbeidere. Tar vi med store brukere av IKT (dvs. virksomheter som ikke er regnet som IKT-bedrifter, men som har store IKT-avdelinger) er mangelen over 8600 (IKT Norge, 2015). I samme undersøkelse står det at det er størst mangel på kompetanse på mobile plattformer, IT-sikkerhet og skytjenester. Mobile plattformer og skytjenester som nevnt senere i oppgaven, er områder som politiet og Forsvaret allerede er i samtaler om et fremtidig samarbeid. Det kan ikke utelukkes at kompetanse er en av de viktigste faktoren for dette. Tilgang til kompetanse, som utviklere og prosjektledere med tung IKT-kompetanse, er viktig for å løse alle de store digitaliseringsbehov som er i både politiet og Forsvaret.

Når det i tillegg finnes undersøkelser som viser av ingeniører tjener bedre i privat sektor fremfor i det offentlige blir rekrutering enda vanskeligere. En undersøkelse i regi av fagforeningen Forskerforbundet viser det seg at en overingeniør i privat sektor tjener i gjennomsnitt i underkant av 40.000 NOK mer enn i statlig sektor (Forskerforbundet, 2017). Dersom en legger til grunn tall fra fagforeningen Tekna, som er den største fagforeningen for teknologer med mastergrad, er forskjellen enda større. Nå er ikke lønn det eneste parameter for valg av karrierer, men dette viser at offentlig sektor har betydelig utfordringer med å få inn nødvendig kompetanse. Et samarbeid vil ikke løse lønnsforskjellene mellom stat og privat sektor, men det vil kunne være mulig å utnytte spesial og kritisk kompetanse på tvers av sektorene.

Begge etatene har også IKT-systemer som er særegne for den virksomheten de bedriver. Både med tanke på operative krav og sikkerhet, men også med tanke på at de er helt eller delvis utviklet av politiet eller Forsvaret selv for å dekke et konkret behov. Et eksempel på dette er kommando og kontroll (K2) systemer. Dette er systemer som det ikke finnes stor sivil kompetanse på utenfor egen etat. Det kan også være relativt små fagmiljøer, og et samarbeid rundt dette vil kunne bidra med erfaringsutveksling og styrking av fagmiljøet totalt sett.

Forsvaret ved Forsvarets ingeniørskole utdanner også egne ingeniører innen IKT. Dette er i all hovedsak ingeniører som skal bidra i alle deler av IKT-virksomheten i Forsvaret og får jobb i Forsvaret etter endt utdanning. Det finnes eksempler på at personer som har gjennomført denne utdanningen slutter, og begynner hos andre aktører som politiet, men denne utdanningen er først og fremst rettet mot å dekke Forsvarets behov. Hele utdanningssystemet i Forsvaret er under omstrukturering, så det vil bli endringer på denne utdannelsen i fremtiden.

Et annet element under faktoren kompetanse kommer også frem under intervjuene. Dette gjelder kunnskap om hverandres systemer, organisering eller kapasiteter. Det var kun en av respondentene, R4, som hadde vesentlige kunnskap om den andre etaten. Dette skyldes at denne personen hadde utdanning og erfaring fra Forsvaret, og hadde tidligere jobbet i privat sektor opp mot Forsvaret. Alle respondentene hadde vært i møter der representanter for etatene var tilstede, så de hadde en overordnet kunnskap om hvordan den andre etaten var organisert. Det som hadde vært i fokus på disse møtene hadde vært fremtidige digitaliseringsstrategier og fremtidige løsninger. Dette ble diskutert på et overordnet strategisk nivå. Respondentene hadde liten eller ingen kjennskap til tekniske løsninger eller systemer som var viktige for motparten. Dette kan nok ha sammenheng med at alle respondentene er på et strategisk nivå. Det finnes sikkert personer i de to etatene som har bedre kjennskap til tekniske systemer og løsninger, men siden dagens samarbeid er så lite som det er i dag er det nok grunn til å anta at dette ikke er mange. Dette vil kunne påvirke et eventuelt samarbeid om eksisterende løsninger, men samtidig er store deler av IKT-kompetansen så generell at den kan benyttes på tvers av sektorene.

Delkonklusjon kompetanse

Allerede i 2000 i forbindelse med sårbarhetsutvalget så man utfordringer knyttet til kompetanse. «Digitalisering av den kritiske infrastrukturen har økt systemenes kompleksitet, og man trenger ofte spesialkompetanse for å rette opp tekniske feil» (Justis- og politi departementet, 2000, s. 68). I tillegg har Forsvaret og politiet en rekke spesial løsninger som det kan være enda vanskeligere å få tak i kompetanse på. Det vil derfor være gunstig for begge parter at det var mulig å dele erfaringer og kompetanse. Det store behovet for IKT-kompetanse i begge etater fremmer derfor et samarbeid.

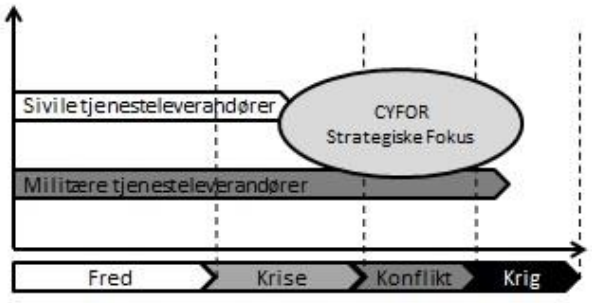
4.7 Faktor operativ- og beredskapsevne

Alle respondentene var inne på at et økt samarbeid kunne gi både Forsvaret og politiet effekter på etatenes operative evne, eller momenter som underbygger operativ evne. Dette kan være økt redundans, større tillitt mellom etatene som igjen kan føre til bedre samhandling og informasjonsdeling. Tidligere drøftede faktorer som for eksempel økonomi og kompetanse, vil også kunne øke den operative evnen, men de har også påvirkning ut over den operative evnen. Disse effektene eller under-faktorene er tett knyttet sammen, og noen kunne sikkert vært en egen faktor, men jeg har valgt å samle disse under en faktor som skal underbygge den operative evnen. Disse under-faktorene vil også kunne gi positiv innvirkning på andre faktorer. Bedre samhandling og informasjonsdeling vil for eksempel kunne gi positive effekter på faktoren ledelse og styring, kompetanse med flere.

Operative krav

Det å skrive om operative krav i detalj er vanskelig, da dette er gradert informasjon for både Forsvaret og politiet. Ingen av respondentene ønsket derfor å snakke om hvilke krav de hadde til virksomheten og IKT-systemene. Denne studien vil derfor kun omtale dette i generelle former. I henhold til alle respondentene, utleder begge etatene sine operative krav ut i fra oppdraget de har fått fra sine respektive departementeter. Dette inkluderer også operative krav til IKT-virksomheten og tjenestene. Siden samfunnsoppdraget er ganske forskjellig har dette medført at de har ulike operative krav. Forsvaret er en organisasjon som forbereder seg på krise og krig. Dette gjelder også Cyberforsvaret, og en del av de siste års omstillinger har gått ut på å endre organisasjonen fra å være en tilbyder av IKT-tjenester til Forsvarets avdelinger, til å bli mer militært rettet med fokus på å understøtte militære operasjoner. CYFOR skal levere IKT-tjenester til Forsvaret og andre kritiske samfunnsfunksjoner når ingen andre kan levere.

Figur 2 CYFORs strategiske fokus



Figur 2 er hentet fra en av flere presentasjoner som ble holdt i CYFOR i forbindelse med omstillingsaktiviteten, og er utarbeidet av daværende nestkommanderende for CTK, Stian Norløff. Den beskriver et av elementene som skiller Cyberforsvaret med øvrige sivile leverandører av IT-tjenester. Sivile IT-leverandører skal levere tjenester så lenge det er forsvarlig. I all hovedsak vil dette være i fredstid og under kriser. Dersom det er alvorlige kriser i samfunnet, eller Norge er i en konflikt med et annet land, eller i ytterste konsekvens krig, er det ikke forventet at disse skal kunne levere IT tjenester til Forsvaret. Derfor er Cyberforsvarets strategiske fokus rettet mot det området der ikke sivile leverandører kan levere. Dette fører til at mange av Forsvarets systemer har særegne krav. Dette kan være krav til sikkerhet, redundans, robusthet og mobilitet. Slike løsninger er ofte mer komplekse, kostbare å anskaffe og vedlikeholde enn standard materiell.

Politiet er naturligvis også interessert i robuste systemer da de også har behov for systemer som virker, da politiets oppgaver er de samme i fred, krise og krig. «Politiet er jo en av de samfunnsvirksomhetene som er forventet å fungere når mye annet ikke fungerer» (R4, 2018). Dersom en ser på tabellen over kan en derfor anta at politiets krav til IKT-tjenenester er en plass mellom det sivile leverandører tradisjonelt leverer og de kravene Forsvaret har. Kravene som Forsvaret setter på noen av sine mest kritiske systemer vil kunne være veldig fordyrende for politiet. Med de kravene som politiet opererer etter vil det ikke alltid være hensiktsmessig å benytte seg av samme løsning som Forsvaret. Dette blir ytterligere forsterket når enn ser dette sammen med den totale økonomien i etatene. PIT har totalt ca. 1 milliard kroner i 2018,

mens CYFOR og FMA til sammen har et budsjett på over 2,6 milliarder kroner. Politiet vil i mange tilfeller ikke ha råd til å benytte kostbare og spesifikke systemer som Forsvaret. Det at Forsvaret og politiet har operative krav som er høyere enn det sivile leverandører normalt leverer, vil både være fordyrende og kompliserende for begge etatene. Når en i tillegg legger til grunn at Forsvaret har fått føringer om å etablere en strategisk samarbeidspartner i Prop 1 S 2017, er det derfor ikke unaturlig at begge respondentene fra Forsvaret peker på politiet som en åpenbar kandidat for samarbeid.

Operativ evne

Begge respondentene fra Forsvaret uttalte i intervjuene at et økt samarbeid kunne gi økt operativ evne. Operativ evne er i Forsvarets fellesoperative doktrine definert som: «Evnen til å løse sine oppgaver, herunder planforberedelser og beredskap. En funksjon av styrkenes evner og kapasiteter, tilgjengelighet, deployerbarhet og utholdenhet» (Forsvarets høgskole, 2014, s. 227). Operativ evne i Forsvaret er nært knyttet til kampkraft, altså hvilke evner de operative avdelinger har til å utføre sine oppgaver. Det er tilsvarende hos politiet. Den operative evnen er knyttet opp til hvilken evne politiet har til å utføre sine oppgaver. Nå har cyber i Forsvaret blitt et egen krigføringsdomene på like linje men land, sjø og luft. Politiet har også etablert avdelinger som jobber aktivt med kriminalbekjempelse på nett. Men i denne oppgaven er det fokus på de mer tradisjonelle IKT-tjenestene. Det er de tjenestene som støtter det operative miljøene med ulike typer IKT. Det kan være alt fra operative IKT-systemer som kommando- og kontrollsystemer, til administrative systemer for saksbehandling og lønn. IKT understøttelse har blitt viktigere for de operative avdelingene, og de blir stadig mer avhengig av at IKT-systemene fungerer for å kunne utføre sitt arbeid. Dette fører til at det stilles strengere krav til de IKT-systemene som understøtter denne virksomheten. Hvordan vil et samarbeid mellom Forsvaret og politiet innen IKT kunne gi økt operativ evne for begge etater? Dersom en legger definisjonen til grunn skal altså evner, kapasiteter, tilgjengelighet, deployerbarhet og utholdenhet bli bedre for begge etater. Siden det er et svært begrenset samarbeid innenfor IKT i dag, er det vanskelig å vite hvilke konkrete forbedringer etatene vil få på den operative evnen dersom en etablerer et mer omfattende samarbeid, men det er noen generelle effekter som man kan anta vil bedre den operative evnen. De er beskrevet under.

Tillit og informasjonsdeling

Det finnes mange ulike tolkninger av begrepet tillit, og teorier om hvordan dette påvirker relasjoner. I denne oppgaven benytter jeg definisjonene som er benyttet i studien: «En god dag på jobben – evaluering av prosjektet trygghet og tillitt» utgitt av Politihøgskolen. Den baserer seg på Giddens tre hovedinndelinger: relasjonstillit, systemtillit og implisitt tillit (Giddens, 1997). De to første tillitsformene kan vi knytte til ulike møter. Relasjonstilliten er knyttet til møtene ansikt til ansikt, og systemtilliten møte og opplevelse av institusjonene. Den implisitte tilliten er mer å forstå som en «miljøfaktor» og finnes innenfor konstellasjoner som jobbfellesskap, foreninger, familie eller vennskapsgrupper (Egge, 2010).

Ved at personer som jobber innenfor IKT i de to etatene møtes og jobber sammen, vil det kunne bedre tillitten mellom dem personlig, noe som igjen vil gjøre samarbeid lettere. Dersom personer jobber tettere opp mot en annen etat, vil systemtilliten, altså opplevelsen av den andre etaten, kunne bli bedre. Når det gjelder implisitt tillit så vil dette også påvirke samarbeidet. Men selv om personer i Forsvaret og politiet har ulik bakgrunn, er det mange fellestrekk både med tanke på kultur og seleksjon. Et økt samarbeid kan derfor gi implisitt tillitt med at det etableres nye jobbfelleskap og vennskap. Respondenten fra POD som hadde bakgrunn fra Forsvaret, uttalte at en av grunnen til at Forsvaret var en hensiktsmessig samarbeidspartner var at det var sett på «som et kvalitetsstempel å si at man samarbeider med Forsvaret» (R4, 2018) . Dette er nok også knyttet til andre faktorer enn tillit, men uten noen form for tillit til den andre etaten ville ikke dette blitt sagt.

Økt samarbeid mellom etatene vil derfor kunne gi økt tillit mellom organisasjonene, som igjen vil føre til bedre informasjonsdeling. Som respondent 2 uttaler: «Hvis vi skulle komme i den situasjonen at vi skulle sy sammen vår IKT og infrastruktur, ville det gjøre det langt enklere å utveksle informasjon sammen. Og det er da åpenbart at det i en del sammenhenger er viktig at Forsvaret og politiet har en god kommunikasjon, og har en evne til å kunne utveksle informasjon direkte med hverandre» (R2, 2018). Nå er det ikke problemfritt at Forsvaret og politiet utveksler all informasjon med hverandre. Dette var jeg inne på under lover og regelverk. Men dersom dette gjøres innenfor gjeldende regelverk vil informasjon kunne flyte raskere mellom etatene. Dette vil gi operative

effekter knyttet til den operative samhandlingen mellom etatene ut over et rent IKT-samarbeid.

Redundans og robusthet

I Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarsektoren er det beskrevet at: «Forsvarsektoren skal etablere kostnadseffektive systemer med en robusthet og redundans som er i henhold til gjeldene krav» (Forsvarsdepartementet, 2014, s. 9). Robusthet går på systemenes evne til å tåle forstyrrelser som kan påvirke systemets funksjoner. Dette er grunnen til at mange av forsvarets IKT-installasjoner er fortifisert og beskyttet mot elektromagnetisk puls (EMP). Dette er kostnadskrevende, og gjøres normalt ikke av sivile leverandører. Redundans innenfor IKT vil si at det finnes alternativt utstyr og kommunikasjonslinjer som automatisk overtar dersom det er feil på utstyret eller kommunikasjonslinjene. Dette benyttes ikke kun av Forsvaret, men de store kommersielle teleoperatørene har også gjerne redundante løsninger på de mest kritiske systemene og kommunikasjonslinjene. Både politiet og Forsvaret har høye krav til sine IKT-systemer, både med tanke på redundans og robusthet som nevnt over. Dette fører til at det tilstrebes å ha flere kommunikasjonsveier inn til de ulike lokasjonene.

Forsvaret har som skrevet i innledningen et egen kommunikasjonsinfrastruktur. Det vil si et eget nettverk av fiber og radiolinjer for kommunikasjon som ivaretar dette i henhold til kravene for robusthet og redundans. Dette nettverket er ikke en del av det kommersielle nettverket som leverandører som for eksempel Telenor er ansvarlige for. Politiet har ikke en egen nettverksinfrastruktur og benytter derfor sivile leverandører for dette. Respondent 3 fra PIT var klar over risikoen knyttet til at Telenor var så sentral, og til dels enerådende i å tilby infrastruktur nasjonalt. Både respondenter fra Forsvaret og politiet var derfor inne på at det burde være mulig å benytte hverandres kommunikasjonsløsning som redundans for egen, eller leid infrastruktur. «Forsvaret er jo opptatt av at man har sin egen infrastruktur på grunn av robusthetskrav med mer. Men det går jo an å tenke seg at det går an å få enda mer robusthet ved å samarbeide med andre» (R1, 2018). Respondent 4 fra POD er også positiv til dette. «Vi kunne ha levert infrastruktur. Ikke nødvendigvis som sin eneste plattform, men kanskje som et bein i en løsning, for å skape større seighet. Det kunne vært gjensidig, for å skape større redundans» (R4, 2018). I dette tilfellet benytter Respondent 4 seighet som et annet ord for

både redundans og robusthet. I dette punktet har fokuset blitt redundans og robusthet innenfor kommunikasjonsinfrastruktur. Men dette kunne også gjelde andre områder for eksempel plattformtjenester eller EBA, som kan gjøre IKT-systemene totalt sett får mer redundans og økt robusthet. Et økt samarbeid vil derfor kunne gi operativ effekt ved at IKT-systemene blir mer redundante og får økt robusthet.

Delkonklusjon operativ- og beredskaps evne

Begge etatene har høye operative krav, men Forsvaret har krav til sine systemer som vil kunne være fordyrende for politiet i forhold til de kravene de har til sine systemer. Men et økt samarbeid vil kunne gi nye muligheter for å øke redundansen og robustheten i begges IKT-systemer. Økt samarbeid i seg selv vil også kunne gi økt tillit, som vil bedre informasjonsdelingen. Økt informasjonsdeling vil kunne gi bedre samhandling og bedre operativ evne. Faktorer som ikke er under dette punktet vil også kunne øke den operative evnen. Bedre økonomi vil kunne gi bedre og mer utstyr. Økt kompetanse vil kunne bedre systemer osv. Faktoren operativ evne fremmer et økt samarbeid.

4.8 Faktor organisatoriske implikasjoner

I intervjurunden ble det stilt spørsmål om hvordan et eventuelt økt samarbeid vil bli mottatt i etatene. Alle respondentene jobbet på et strategisk nivå i organisasjonene, noe som vil kunne prege svarene da de sitter på et overordnet nivå. Alle var sikre på at egen avdeling ville være positive til et økt samarbeid. Samtidig var alle klare på at de overordnede har et sterkt ønske om å få til et samarbeid. Som respondent 1 sa om FD: «Både i Stortingspropen (Forsvarsdepartementet, 2017) og også med oppdrag de har sendt ut til både Forsvaret og FMA i de siste, så er de veldig positive til samarbeid mellom ulike offentlige etater innenfor IKT-område» (R1, 2018). Men det ble presisert at samarbeid måtte gi en eller annen form for gevinst for etaten. Det vil si økonomisk eller operativ gevinst. Politiet var også fra ledelsesnivå veldig positive til et samarbeid med andre offentlige og private aktører.

Det var først under spørsmålet knyttet til hvordan underordnede avdelinger ville se på at slikt samarbeid at det kom opp noen interessante observasjoner. Respondent 3 uttalte: «Jeg er ikke veldig pessimistisk i forhold til det. Men det er klart at alltid når man skal inngå et strategisk

samarbeid, uansett om det er privat eller offentlig aktør, så vil alltid medarbeidere tenke hva skjer med meg oppi dette her. Mister jeg jobben?» (R3, 2018) Respondent 2 fra Forsvaret utalte: «Hvis dette samarbeidet utvikler seg i en retning om at andre utenom Cyberforsvaret kommer til å gjøre en del av de jobbene som Cyberforsvaret gjør i dag, tror jeg holdningen vil være negativ» (R2, 2018). Det kan derfor virke som om at dersom et samarbeid fører til organisatoriske endringer eller nedbemanning, vil dette møte motstand i organisasjonene. Dette er ikke en unaturlig reaksjon for personer som står i fare for å miste jobben, eller få nye oppgaver i forbindelse med en omstilling. Samtidig sa respondent 3: «Det er mer enn nok å gjøre for alle så tror ikke det er noen som føler seg truet i forhold til det» (R3, 2018). Dette henger sammen med punktet kompetanse der jeg beskriver mangelen på IKT-kompetanse i Norge.

Delkonklusjon organisatoriske implikasjoner

Det kan virke som om at de organisatoriske implikasjonene ikke er en faktor som påvirker et økt samarbeid i vesentlig grad på nåværende tidspunkt. Dette vil først bli en faktor den dagen et eventuelt samarbeid blir av en slik art at det gjøres organisatorisk tilpasning i form av redusering eller omstilling av personell. Som Respondent 1 sa: «Potensielt kan jo konsekvensene være relativt store og medføre nedbemanning og organisatoriske endringer» (R1, 2018). Fra ledelse hold i begge etater er det ikke utrykt bekymring for at dette vil hindre et eventuelt samarbeid mellom etatene.

4.9 Eksisterende og anbefalte samarbeidsområder

Det er noe eksisterende samarbeid mellom etatene i dag, men mye av dette samarbeidet er enten gradert etter sikkerhetsloven eller unntatt offentligheten. Dette vil derfor ikke bli omtalt i denne oppgaven. I intervjuene ble respondentene spurt om hvilke områder de ser for seg et samarbeid mellom politiet og Forsvaret. Jeg vil derfor drøfte og forklare de ulike samarbeidsområdene som ble foreslått i intervjuene. På noen av disse områdene finnes det allerede pågående samtaler om videre samarbeid, uten at dette samarbeidet er formalisert. Flere av disse samarbeidsområdene er også nevnt i Prop 1 S(2017-2018) der det står: «Strategisk samarbeid planlegges etablert innenfor IKT –tjenesteområdene operativ

beslutningsstøtte, forvaltning, stasjonær og mobil kommunikasjons infrastruktur løsninger for IKT-plattformer og datasenterløsninger» (Forsvarsdepartementet, 2017, s. 21).

Datasenter

Som det står i Prop 1 S (2017-2018) er datasenterløsninger et område hvor Forsvaret ønsker å inngå et strategisk samarbeid med andre. Det finnes en rekke forskjellige definisjoner på hva et datasenter egentlig er, og forskjellen på et datasenter, serverrom eller datarom, er ikke helt klar. En definisjon kan være: «En miljø-kontrollert, sentralisert fasilitet som tilbyr forretningstjenester ved å levere applikasjoner og data til et nettverk av fjerne og nære brukere på en sikker måte» (Steen-Olsen, 2006). Et datasenter er derfor ofte en egen lokasjon som har nødvendig kraft og kjøling(miljø-kontrollert) som leverer ulike IKT-tjenester (applikasjoner og data) til et nettverk som brukere er tilkoblet, på en sikker måte. Både Forsvaret og politiet har i senere tid etablert, eller har i nær fremtid planer om å etablere slike datasentre. Her har Forsvaret og politiet allerede inngått et samarbeid om eiendom, bygg og anlegg (EBA). Dette kunne vært utvidet til også å omhandle IKT-tjenester, men som respondent 4 sa: «Nå var det tydelig at det skulle være et EBA samarbeid, nettopp fordi å ha et IKT-samarbeid er mer krevende» (R4, 2018). Årsaken til dette kan knyttes til faktoren lovverk som setter begrensninger knyttet til håndtering av data, og media som kan misforstå hvordan elektronisk informasjon blir behandlet i IKT-infrastrukturen dersom dette i større grad er felles. Som respondent 1 uttalte: «Ikke felles lagring av data. Det er behov for å holde ting adskilt her, med tanke på sikkerhetsloven» (R1, 2018). Faktorene ledelse og styring vil også være gjeldene da et slikt samarbeid blir mer komplekst.

Skytjenester

Et annet moment for samarbeid som kom frem gjennom intervjuene var såkalte skytjenester. Skytjenester (cloud computing) er en samlebetegnelse på alt fra dataprosessering og datalagring, til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett (Datatilsynet, 2014). Dette gir mye av den samme funksjonaliteten som et datasenter, forskjellen er at disse systemene ikke nødvendigvis ligger på etatens egne eller leide dataservere, men på store eksterne servere. I mange tilfeller vil disse kunne ligge i utlandet. Ved dette er det helt åpenbare sikkerhetsutfordringer som gjør at dette kan bli problematisk

både for politiet og Forsvaret. Derfor vil muligens en datasenterløsning, ofte omtalt som privat sky, være en bedre løsning. Alternativt en løsning som respondent 3 nevner: «Også skytjenester. Hvis man ser at det er utfordrende å bruke det kommersielle markedet, kanskje man skulle ha gjort noe rundt sikker offentlig sky som løsninger som man kan samarbeide på» (R3, 2018). Dersom det ble etablert en sikker skyløsning, det vil si en løsning der en kan være sikker på at dataene blir håndtert i Norge, og etter gjeldene regelverk, kunne denne vært benyttet av flere instanser i det offentlige Norge. En slik løsning vil ikke komme av et samarbeid mellom kun Forsvaret og politiet, men gjennom flere departementer og etater. Dette er også respondent 3 inne på: «Det er et stort initiativ offentlig rundt platform as a service. Der er veldig mange IT folk fra offentlige etater, Forsvaret også, som jobber sammen om å bygge og lære av hverandre, knyttet til det å bygge platform as a service» (R4, 2018). Platform as a service er en form for skytjeneste hvor kunden har kontroll på egne applikasjoner, men ikke kontroll over nettverk, servere, operativsystem eller lagringsmuligheter (Datatilsynet, 2014). Om dette ville være tilfredsstillende for politiet og Forsvaret er usikkert, først og fremst med tanke på sikkerhet. Så en privat skytjeneste i offentlig regi (datasenter) er nok en mer hensiktsmessig modell.

Sikre plattformer

I Forsvaret har vi mange ulike sikre plattformer. Det vil si IKT-systemer med maskinvare og kommunikasjonsteknologi (Hardware) og programvare (Software) som er sikkerhetsgodkjente for ulike sikkerhetsgraderinger. De mest kjente er Fisbasis B som er et begrenset system, og FisBasis H/NS som er et system godkjent for den høyere graderingen Hemmelig/NATO Secret. Politiet derimot har lite graderte systemer som respondent 4 uttaler: «Men vi har jo ingen plattform for hverken begrenset, konfidensielt eller hemmelig i politiet» (R4, 2018). Dette er et behov for Politiet, spesielt dersom det blir endringer i gjeldene sikkerhetslov. Men som han uttaler videre: «Men å ta i bruk FisBasis noe mer enn det vi har gjort er neppe hensiktsmessig i og med at Forsvaret selv ser hva de skal gjøre med FisBasis» (R4, 2018). Dagens sikre plattform-løsning i Forsvaret er under videreutvikling, og politiet er meget interessert i dette arbeidet og eventuelt hvilke valg Forsvaret kommer til å gjøre. Forsvaret er kjent med dette. «Det er en dialog med Justisdepartementet på dette med sikre plattformer og skytjenester. For rett og slett diskutere om det kan være noen felles interesser der. Det er en

interessant sak» (R1, 2018). Hva som kommer ut av dette arbeidet er for tidlig å uttale seg om, men dette er et område som både Forsvaret og politiet er interessert i et samarbeid om.

Kommando og kontroll informasjonssystemer (K2IS)

Begge representantene fra politiet ønsket også et samarbeid innenfor kommando og kontroll informasjonssystem. I militæret er dette programmer og systemer som skal gi ledelsen oversikt over egne styrker, og gjerne motstanderens styrker, for å kunne utøve militær kommando og disponering av styrker. Dette har ofte integrerte kartsystemer og kommunikasjonsløsninger for å kunne lede egne styrker. Politiet benytter også systemer som dette for å lede sine egne styrker og patruljer. Respondent 3 uttalte: «Jeg tror Forsvaret har mye erfaringer fra kommando og kontroll. Vi har mye erfaring på det vi også, og dere har masse erfaringer på i en litt annen setting. Tror vi kunne blitt bedre sammen» (R3, 2018). Det er igjen rettet inn mot kompetanse. Dette er et område som det er lite ekspertise å hente i privat sektor. Det var ingen fra Forsvaret som nevnte dette som et fremtidig samarbeidsområde. En av årsakene til det kan være at dette er høygraderte systemer i Forsvaret. Respondent 1 fra FST uttalte at samarbeid om høygraderte systemer ville gjøre ting vanskeligere.

Kommunikasjons infrastruktur

Kommunikasjonsinfrastruktur var jeg litt inne på i punktet redundans og robusthet. Forsvaret har sin egen landsdekkende kommunikasjonsinfrastruktur. Denne består av både radiolinje og fiber, men stadig mer kapasitet blir lagt over på fiber. Ved å gjøre dette vil man få større kapasitet og blir mer lik den teknologien som benyttes av kommersielle aktører. Etableringen av dette fibernettverket gjøres ofte i samarbeid med kommersielle aktører, ved at en til en viss grad benytter samme felles kabeltraseer eller koblingspunkter. Forsvarets infrastruktur vil i større grad enn i dag fremstå som en integrert del av samfunnets øvrige infrastruktur. Respondent 4 var interessert i dette: «Forsvaret bytter jo ut gamle radiolinjenettet med fiber. Politiet leier kommersielt nett hos Telenor, så det kunne jo vært interessant å samarbeide med» (R4, 2018). Respondenten fra PIT nevnte også dette som et mulig samarbeidsområde, da Forsvaret eventuelt kunne bruke deres leide infrastruktur som redundans for egen infrastruktur. Respondentene fra Forsvaret var også positive til å se på et samarbeid innenfor

dette. Dersom det er mulig å benytte hverandres infrastruktur som redundans vil dette kunne øke den operative evnen, samt kunne redusere eventuelle kostnader knyttet til investeringer og leie av kapasitet.

Mobile virtual network operator (MVNO)

En MVNO kjøper trådløs kapasitet fra en teleleverandør (mobile network operator). I Norge er det kun to MNO'er som tilbyr landsdekkende mobildekning. Dette er Telenor og Telia. Ved å etablere en egen MVNO kan Forsvaret og eventuelt politiet ha sitt eget mobilselskap som kjøper kapasitet fra en av leverandørene i markedet. Fordelen med dette vil være at de selv kan administrere abonnementer, og redusere kostnader da en ikke trenger et fordyrende mellomledd som mobiloperatører som f.eks. Ventelo. I tillegg vil en kunne øke sikkerheten knyttet til mobilbruk, da en selv sitter med abonnementsdatabasen. «Det pågår arbeid i Forsvaret på blant annet MVNO, og at Forsvaret skal bli sin egen MVNO. Dette tror jeg vil være veldig interessant for politiet» (R1, 2018). Dette er også representanten fra PIT inne på: «Det å ha mobiltelefoni og ikke minst kundebaser, og ha kontroll på det» (R3, 2018). Dette arbeidet er i en startfase, men det kommer helt klart frem av dokumenter og uttalelser fra Forsvaret at de ønsker at politiet skal være med på dette. Politiet er også positive til samarbeid knyttet til dette. Samarbeid om dette vil kunne gi positiv effekt på faktorene økonomi og sikkerhet, som er beskrevet under sikkerhetsloven i oppgaven.

Driftstjenester

Representanten fra PIT var også inne på mulighetene ved at begge etater hadde en stor driftsorganisasjon som kunne støtte hverandre. Dette var i hovedsak hengt opp i muligheten for å utveksle kompetanse, men det er også andre likheter ved denne organisasjonen. Både PIT og CYFOR har driftspersonell på flere steder i landet. Som respondent fra CYFOR sa: «En av de tingene som vi har felles er jo at vi opererer i hele landet» (R2, 2018). Hvilke muligheter som finnes for felles bruk av disse ressursene ble ikke videre omtalt av noen av respondentene i intervjuene, men det er mulig å anta at et mulig samarbeid innenfor lokal drift av systemer kan være mulig. Dette blir sannsynligvis ikke aktuelt å ta videre før en eventuelt har noen felles løsninger å drifte. Dersom dette samarbeidet blir betydelig, vil dette kunne få organisatoriske implikasjoner på de to etatene.

Krypto og sikkerhet

Flere av utredingene og rapportene som er nevnt i litteraturkapittelet omhandler utfordringer knyttet til sikkerhet innenfor IKT, og sårbarheten med at stadig flere systemer blir tilkoblet internett. Det er derfor et stort fokus på dette arbeidet. Justis og beredskapsdepartementet har ansvar for sikkerhet i det sivile samfunn, mens Forsvarsdepartementet har overordnet ansvar for dette i Forsvaret. Det pågår et utstrakt samarbeid innenfor dette feltet. Dette samarbeidet går i hovedsak på hvordan man håndterer uønskede hendelser i cyberdomenet, og hvordan en kan beskytte seg mot dette. Det er planer om å etablere et felles senter for dette. Men det skal sies at mange av IKT-løsningene som benyttes for å overvåke og detektere cybertrusler er felles. Dette har jeg definert bort i oppgaven da dette er av mer operativ karakter, men samarbeid om dette vil kunne gi behov eller ønske om felles systemer for håndtering av dette. Det er i tillegg flere sikkerhetssystemer som skal beskytte egne data. Et eksempel på dette er krypto. Kryptoteknologi er blitt stadig mer vanlig i sivil nettverkteknologi, og flere leverer en eller annen form for krypto på sine systemer. Forsvaret har tradisjonelt vært veldig opptatt av dette og har derfor mange erfaringer knyttet til bruk av krypterte systemer. Det er nok en av grunnene til at respondent 4 uttalte at et samarbeid om dette var ønskelig. Dette er i første rekke for å få tilgang til kompetanse da det er en nasjonal målsetting å ha kryptokompetanse i Norge, for å unngå utenlandske aktører. Det vil være uheldig sett fra et nasjonalt sikkerhetsperspektiv (Justis- og beredskapsdepartementet, 2016).

Oppsummering fremtidig samarbeid

Som en ser av områdene som er diskutert her gjelder mange av dem fremtidige tekniske løsninger eller systemer. Det kan derfor virke som om at det er mye lettere å se for seg et samarbeid innen utvikling, eller nye systemer fremfor å samarbeide om allerede eksisterende løsninger. Økt digitalisering og og bruk av skytjenester vil kreve store økonomiske løft og endringer inne hvordan IKT-systemer tradisjonelt er blitt driftet. Områder som kommunikasjonsinfrastruktur og krypto, er også områder en ser for seg et økt samarbeid for å bedre operativ evne og utnytte kompetansen best mulig.

5 Konklusjon

Hensikten med denne oppgaven har vært å finne ut hvordan Forsvaret og politiet ser på muligheten for et økt samarbeid innenfor IKT. Dette er gjort ved å finne de faktorene som påvirker et eventuelt økt samarbeid innenfor IKT. I tillegg er de områdene som etatene ser for seg vil være hensiktsmessig å samarbeide om i fremtiden analysert.
Dette er et tema som det i svært liten grad har blitt forsket på tidligere, og det er lite litteratur som omhandler samarbeid mellom etatene ut over operativt samarbeid. Formålet er derfor å bidra til økt forståelse, og etablere empiri for samarbeid mellom Forsvaret og politiet innenfor IKT. Gjennom i hovedsak induktivt forskningsdesign, med ekspertintervjuer, har oppgaven avdekket hvordan Forsvaret og politiet ser på et økt samarbeid innen IKT.
I denne oppgaven intervjues eksperter fra fire forskjellige vinkler. To fra politiet (PIT og POD) og to fra Forsvaret (CYFOR og FST) på ulikt nivå i etatene.

Oppgaven søker å klargjøre hvilke faktorer som hovedsakelig fremmer eller hemmer et økt samarbeid mellom Forsvaret og politiet innen IKT. Det ble i oppgaven drøftet åtte ulike faktorer. Et av hovedfunnene er at en rekke av faktorene bærer med seg elementer som både fremmer og hemmer et samarbeid. Samtidig som en ser at flere av faktorene vil påvirke hverandre. Av de åtte faktorene er det tre som fremmer et økt samarbeid (økonomi, kompetanse og operativ- og beredskapsevne), og det er to faktorer som hemmer et økt samarbeid (Ledelse- og styring og media). Faktorene kultur kan være hemmende for samarbeid mellom politiet og Forsvaret, samtidig som den fremmer et samarbeid mellom dem fordi de har flere likhetstrekk i kulturen sett opp mot andre offentlige etater og samarbeidspartnere. Lover og regelverk kan være en kompliserende faktor for samarbeid, samtidig som offentlige myndigheter ønsker et økt samarbeid. Men det er ingenting som er avdekket i denne studien som tyder på at lover og regelverk begrenser et økt samarbeid. Organisatoriske implikasjoner var en faktor som respondentene ikke mente var en faktor av avgjørende betydning på nåværende tidspunkt. Denne ville først bli en faktor dersom økt samarbeid ville påvirke organisasjonene.

De faktorene som påvirker samarbeidet mest er svært sammenfallene fra respondentene i begge etater. Både respondentene fra Forsvaret og politiet mener at økonomi og operativ evne er de viktigste faktorene som fremmer samarbeid, samtidig som ledelse og styring er den

faktoren som hemmer mest. Respondent 1 uttalte at: «at det viktigste som fremmer et økt samarbeid er at begge parter har noe å tjene på det. Og da tjene i utvidet forstand» (R1, 2018). I dette ligger både økonomiske gevinster, og effekter innen operativ evne. Felles investeringer vil kunne gi økonomiske gevinster, i form av bedre kontrakter med industrien, mindre kostnader til prosjektgjennomføring, og mer effektiv drift av systemene. Felles løsninger vil også kunne bidra til at bedre operativ evne gjennom økt tillitt og informasjonsdeling. Samtidig vil ledelse og styring av felles løsninger bli en utfordring. Ledelse og styring av IKT-virksomheten i Forsvaret er allerede en utfordring, og skal en inkluderer politiet i dette blir det enda vanskeligere da de har ulike krav og behov til tjenestene enn det Forsvaret har.

Begge etaters behov for og ønske om digitalisering og økt bruk av en eller annen form for sky-tjenester gir muligheter for økt samarbeid. På strategisk nivå foregår det dialog om dette mellom etatene, men det er foreløpig lite konkrete samarbeid om IKT som kjent. Dersom det skal bli et mer konkret samarbeid om slike fremtidige løsninger, må prosjektene som tar dette fram samkjøres. Det kan for meg virke som om at en slik samkjøring av prosjekter er vanskelig. Dette er knyttet opp til ulike bevilgningssystemer for økonomi, og forskjellig prosjekt -og styringsmodeller. I tillegg virker hensynet til etatenes egne behov og krav viktigere enn å kunne se synergier på tvers av sektorer. Nå er ikke etaten FMA som står for prosjektgjennomføringen i Forsvaret en del av denne studien, og det ville vært interessant å se videre på hvordan de ser på muligheten for å kjøre et prosjekt sammen med en annen offentlig etat.

De andre områdene som er avdekket som mulig samarbeidsområder ble i mindre grad omtalt i intervjuene. Årsaken til det kan nok være at alle respondenter har i senere tid, i en eller annen form, vært involvert i strategisk arbeid knyttet til digitalisering av sine respektive etater. Det kan også virke som at det er lite kunnskap om hverandres systemer og løsninger. Om studien hadde hatt respondenter fra lengre ned i driftsorganisasjonene ville muligens samarbeid om flere andre eksisterende løsninger blitt kartlagt, men det er lite som tyder på at kunnskapen om hverandres systemer er bedre på et lavere nivå. For at et økt samarbeid omkring eksisterende løsninger vil det derfor være behov for at begge parter må øke kunnskapsnivået om hverandres løsninger, behov og krav.

Et annet funn i undersøkelsen er at Forsvaret og politiet her ulike føringer for outsourcing. Forsvaret ønsker å sette mer av sine systemer ut til private leverandører. Hovedårsaken til dette er knyttet til økonomi. Samtidig ønsker politiet det motsatte. De vil ta mer av driften selv for å kunne bedre sikkerheten på sine systemer. Forsvaret har tradisjonelt driftet flere av sine systemer selv, sett opp mot det politiet har, så det er ikke nødvendigvis problematisk for et samarbeid om Forsvaret går «et steg» mot outsourcing av tjenester, og politiet beveger seg den andre veien. Det kan argumenteres for at de i så fall vil møtes i synet på outsourcing, men fokuset på videre utvikling av IKT innad i etatene vil være forskjellig.

Kompetanse er den siste faktoren som helt klart fremmer et samarbeid. Begge etater har utfordringer knyttet til små fagmiljøer og rekrutering av kompetent IKT-personell. Et økt samarbeid vil kunne gjøre fagmiljøene større, og en mer effektiv utnyttelse av kompetansen. Politiet fremhevet behovet for kompetanse innenfor krypto som en utfordring, spesielt dersom den nye sikkerhetsloven vil legge føringer for politiets løsninger. Her sitter Forsvaret på en god del kompetanse og erfaringer som vil være gunstig for politiet å få tilgang til.

Media er den siste faktoren er som er svakt hemmede for samarbeid. Det er forskjell i lovverket knytte til hva de forskjellige etatene kan gjøre og hvilket samfunnsoppdrag etatene har. Det kan være problematisk å forklare skille mellom Forsvaret og politiet til media dersom mange av IKT-løsningen er felles. Men samtidig har Forsvaret og politiet allerede et operativt samarbeid, så om dette samarbeidet foregår i ordnede former bør ikke dette bli problematisk.

Det er mange offentlige dokumenter som omhandler samarbeid mellom Forsvaret og politiet. Flere av disse omhandler også IKT-samarbeid, Men det er lite som omhandler samarbeid ut over operative leveranser og sikkerhet. Det finnes operativ samarbeid i dag, men begge etater har et ønske om et økt samarbeid også innenfor andre områder innen IKT, og spesielt Forsvaret har fått klare føringer for å se på andre samarbeidspartnere innenfor IKT. Begge respondentene fra Forsvaret mente derfor at politiet var en nærliggende aktør å samarbeide med. Respondentene fra politiet mente også at Forsvaret var en foretrukken samarbeidspartner innen IKT.

I denne studien har det vært begrenset til å omhandle etatene Forsvaret og politiet, og med kun 4 respondenter som empirigrunnlag. Det ville vært fornuftig å søke å undersøke IKT samarbeid mellom politiet og Forsvaret i et større perspektiv, og med flere respondenter, fra flere nivåer i begge etater. Det ville også vært interessent å se hvilke implikasjoner et økt samarbeid mellom etatene politiet og Forsvart innenfor IKT ville fått dersom en inkluderte det politiske nivå. Det vil være utfordringer på departementsnivå mellom Forsvarsdepartementet og Justis –og beredskapsdepartementet. Ett naturlig sted å begynne kan være å spørre om dagen tolkning av sektorprinsippet vil ville fått påvirkning på et slikt samarbeid.

6 Forkortelser

CTK	Cyberforsvarets taktiske kommando
CYFOR	Cyberforsvaret
EBA	Eiendom, bygg og anlegg
EMP	Elektromagnetisk puls
FD	Forsvarsdepartementet
FMA	Forsvarets Mattereille etat
FMA IKT-kap.	Forsvaret mattereille etat IKT-kapasiteter
FST	Forsvarsstaben
IKT	Informasjon og kommunikasjonsteknologi
IT	Informasjonsteknologi
JBD	Justis- og beredskapsdepartementet
Meld.St.	Stortingsmelding
MVNO	Mobile virtual network operator
MNO	Mobile network operator
NorCERT	Norwegian computer emergency response team
NOU	Norges offentlige utredinger
NSA	National Security Agency
NSF	Norsk senter for Forskningsdata AS
NSM	Nasjonal sikkerhetsmyndighet
PIT	Politiets IKT-tjenester
POD	Politidirektoratet
PRINSIX	Forsvarets prosjektstyringssystem
Prop.	Stortingsproposisjon
PST	Politiets Sikkerhetstjeneste

Litteraturliste

Allern, S. (1997). *Når kildenbyr opp til dans*. Oslo: Pax Forlag.

Andersen, B. K. (2016). *Prosjketmodeller og prosjketsstyring i statlige virksomheter*. Trondheim: Ex ante akademiske forlag.

Bogen, O. H. (2015). *Balansegang*. Oslo: Dreyers Forlag.

Bøe-Hansen, O. (2011). Nytt Landskap - Nytt forsvar. I T. Heier, *Nytt Landskap - Nytt forsvar*. Oslo: Abstrakt Forlag AS.

Christensen, E. L. (2015). *Organisasjonsteori for offentlig sektor*. Oslo: Universitetsforlaget.

Datatilsynet. (2014, 8 26). *Hva er skytjenester*. Hentet fra www.datatilsynet.no: www.datatilsynet:no/regelverk-og-skjema/veileder/skytjenester---cload computing/hva-er-nettskytjenester/

Departementenes sikkerhets- og serviceorganisasjon Informasjonsforvaltning. (2015). *NOU 2015:13 Digital sårbarhet-sikkert sanfunn*. Oslo: Norges Offenlige Utredninger.

Direktotorat for forvaltning og IKT. (2014). *Mot alle odds - veien til samhandling i norsk forvalning 2014:07*. Oslo.

Dyndal, G. L. (2010). *Strategisk ledelse i krise og krig*. Oslo: Fagbokforlaget.

Egge, M. B. (2010). *En god dag på jobben - evalueringav prosjektet "trygghet og tillitt"*. Oslo: Politihøgskolen.

Eide, M. ,. (1987). *Død og pine! Om massemediaog helsepolitikk*. Oslo: FAFO.

Ericson, R. V. (1989). *Negotiating control. A study of News Sourses*. Milton Keyes: Open University Press.

Forskerforbundet. (2017, 12 31). *Vår lønsstatestikk*. Hentet fra www.forskerforbundet.no/lonnstatestikk

Forsvaret. (2017). *Forsvarets årsrapport* . Forsvaret.

forsvaret.no. (u.d.). Cyberforsvaret. s. www.forsvaret.no/organisasjon/cyberforsvaret.

Forsvarets høgskole. (2014). *Forsvarets Fellesoparative doktrine*. Oslo: Forsvarsstaben.

Forsvarsdepartementet. (1998). *Lov om Etteretingstjenesten*.

Forsvarsdepartementet. (2014). *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberopperasjoner i forsvarssektoren*. Oslo: Forsvarsdepertementet.

Forsvarsdepartementet. (2015). *Nasjonal forsvarsindustriell strategi (Meld.St.9)*.

Forsvarsdepartementet. (2015). *Prop. 151 S Kampkraft og Børekraft*.

Forsvarsdepartementet. (2016). *NOU 2016:19 Samhandlig for sikkerhet*.

Forsvarsdepartementet. (2016). *Prop 151S Kampkraft og bærekraft*. Oslo.

Forsvarsdepartementet. (2016). Prop 153 L Lov om nasjonal sikkerhet.

Forsvarsdepartementet. (2017, 1 1). *Lov om forebyggende sikkehetstjeneste (sikkerhetsloven)*.

Forsvarsdepartementet. (2017). *Prop. 1 S* . Oslo.

Forsvarsdepartementet. (2018). *Forskrift om forsvar og sikkerhetsanskaffelser*.

Forsvarsdepartementet. (2018). *Fremtidige anskaffelser til forsvarssektoren 2018-2025*. Oslo: Forsvarsdepartementet.

Forsvartsdepartementet. (2012). *Prop. 73 (2011-2012) Et forsvar i vår tid*.

Giddens, A. (1997). *Modernitetens Konsekvenser*. Oslo: Pax Folag AS.

Heier, T. K. (2013). *Mellom Fred og Krig*. Oslo: Universitetsforlaget.

Håkenstad, M. (2016, 8 15). *Farvel til Menstadslaget*. Hentet fra www.vg.no: https://www.vg.no/nyheter/meninger/i/nzEJQ/farvel-til-menstadslaget

IKT Norge. (2015). *Kritisk Mangel på IKT kompetanse*. Hentet fra www.ikt-norge.no/nyheter/kritisk-mangel-pa-ikt-kompetanse
Jackobsen, D. (2005). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskaaplig metode*. Kristiansand: Høyskoleforlaget.
Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser? : innføring i sammfunnsvitenskaplig metode*. Kristiansand: Cappelen Damm akademisk.
Justis- og beredskapsdepartementet. (2012). *Meld.St.29 (2011-2012) Samfunnssikkerhet*.
Justis- og beredskapsdepartementet. (2013). *Meld:St.21 (2012-2013) Terrorberedskap*. Oslo.
Justis- og beredskapsdepartementet. (2014). *Norges Grunnlov*.
Justis- og beredskapsdepartementet. (2015). *Lov om behandling av peronopplysninger (personopplysningsloven)*.
Justis- og beredskapsdepartementet. (2015). *NOU 2015:13 Digital sårbarhet - sikkert samfunn*. Oslo.
Justis- og beredskapsdepartementet. (2016). *Forsvarets bistand til politiet*. Oslo: Arbeidsgruppen for utarbeiding av ny instruks for Forsvarets bisatand til politiet.
Justis- og beredskapsdepartementet. (2016). *Lov om behandling av personopplysninger i politiet og påtalemyndighet (politiregisterloven)*.
Justis- og beredskapsdepartementet. (2016). *Meld.St 38 (2016-2017) IKT sikkerhet*. Justis. og Beredskapsdepartementet.
Justis- og beredskapsdepartementet. (2016). *Meld.St.10 Risiko i et trygt samfunn*.
Justis- og beredskapsdepartementet. (2017). *Politiloven*. Oslo.
Justis- og beredskapsdepartementet. (2018). *www.regjeringen.no*. Hentet fra Politidirektoratet: www.regjeringen.no/no/dep/jd/org/underliggende-etater/politdirektoratet/id426315
Justis- og politi departementet. (2000). *NOU 2000:24 - Et sårbart samfunn*. Oslo.
Kommunal- og moderniseringsdepartementet. (2017, 09 08). *Digitaliseringsrundskrivet*. Hentet fra www.regjereingen.no.
Lai, L. (2013). *Strategisk kompetanseledelese*. Bergen: Fagbokforlaget Vigmostad & Bjørke AS.
Mossin, Å. (2015, 6 5). *Dette forteller ikke politiet om*. Hentet fra www.journalisten.no: https://journalisten.no/2015/07/Dette-forteller-ikke-politiet-om
Najonal Sikkerhetsmyndighet. (2015). *Sikkerhetsfaglig råd*.
Nasjonal sikkerehtesmyndighet. (2014, 02 21). *www.nsm.stat.no*. Hentet fra Om NSM.
Nærings og fiskeridepartementet. (2017). *Lov om offentlige anskaffelser (anskaffelsesloven)*.
Pedersen, O. E. (2015, 2 2). *Gir IKT satsing til Forsvaret en forsvarbar informasjonsinfrastruktur og et fundament for moderne militære oparasjoner*. Hentet fra www.oslomilsamfunn.no.
Politidirektoratet. (2018). *Disponeringsskriv for politi og lensmannsetaten*.
Politidirektoratet. (2018). *Organisering av politidirektoratet*. Hentet fra www.politiet.no: https://www.politiet.no/om/organisasjonen/andre/politidirektoratet/om-pod/avdelinger-pod/
Politiet.no. (2018, 02 02). *Om PIT og produkter*. Hentet fra www.politet.no: https://www.politiet.no/om/organisasjonen/andre/pit/om-pit/om-pit-og-produkter/
R1. (2018). Intervju FST.
R2. (2018). Intervju CYFOR.
R3. (2018). Intervju PIT.
R4. (2018). Intervju POD.
Rainy, H. B. (1976). Comparing Public and Private Organizations. *Public Administration Review 36(2)*, ss. 233-244.

Regjeringen. (2017). *Forsvarets bistand til politiet. (Bistandsinstruksen).*
Remen, A. T. (2016, 5 3). *Helse Sør-Øst: Innrømmer at utelandske IT arbeidere fikk tilgang til sensitive pasiantdata*. Hentet fra www.nrk.no: www.nrk.no/norge/helse-sor-ost_-innrommer at-utenlandske-it-arbeidere-har-hatt-tilgang-til pasiaentjournaler-1.13478443
Remen, A. T. (2016, 10 28). *Tastefeilen som stoppet Statoil*. Hentet fra www.nrk.no: www.nrk.no/norge/xl/tastefeil-som-stoppet-statoil-1.13174013
Ringdal, K. (2013). *Enhet og mangfold : samfunnsvitenskaplig forskning og kvantitativ metode.* Bergen: Fegbokforlaget.
Skille, Ø. H. (2018, 3 1). *Antennene som samler inn data om norske borgere*. Hentet fra www.nrk.no: https://www.nrk.no/dokumentar/xl/antennene-som-samler-inn-data-om-norske-borgere-1.13881286
Smith, E. (2015, 09 17). "Ministersyre" - et hinder for samordning. *Nytt Norsk Tidskrift*.
Statsministerens kontor. (2009). *Beskyttelsesinstruksen.*
Steen-Olsen, G. (2006, 6 4). *Datarom, serverrom, datasenter*. Hentet fra www.cw.no: www.cw.no/artikkel/komponenter/datarao-serverrom-datasenter
Store Norske Leksikon. (2018, 01 29). *informasjons- og kommunikasjonsteknologi*. Hentet fra www.snl.n: https://snl.no/informasjons-_og_kommunikasjonsteknologi
Yin, R. (2014). *Case study research: design and methods.* SAGE.

Vedlegg A Respondentoversikt

Respondent	Grad/ tittel	Tjenestested	Funksjon	Tid og sted for intervju	Ident. i studien
Truls Petter Bjerkestuen	Oblt	FST PLAN-AVD IKT-SEKSJONEN	Seksjonssjef	Intervjuet 6. mars 2018 Akershus Festning	R1
Jo Austberg	Oblt	CYFOR CST STATEGI, PLAN Og INVESTERINGSSTYRING	Senior stabsoffiser	Intervjuet 9. mars 2018 Jørstadmoen	R2
Tormod Stien	Ass. Direktør	Politiets IKT-Tjeneste	Assisterende direktør	Intervjuet 13. mars 2018 Majorstuen	R3
Wilfred Østgulen		POD IKT-avdeling	Seksjonsleder IKT	Intervjuet 4. april 2018 på Majorstuen	R4

Vedlegg B Intervjuguide

Innledning

Informasjon om meg og FHS/studie
Informasjon om selve oppgaven, og når denne skal være ferdig
Formalia:

- Samtykkeerklæring
- Kan trekke seg når som helst
- Eventuell Anonymisering
- Bruk av diktafon

Kort om intervjuet

- Varighet 1-1.5 time
- Ugradert
- Vil bli transkribert, dersom kapasitet
- Mulighet for gjennomlesing og kommentarer dersom respondenten ønsker dette

Spørsmål

Bakgrunn og erfaringer:

1. Hva er din nåværende stilling og funksjon?

2. Hvilken rolle og erfaringer har du innenfor IKT i politiet/Forsvaret?

3. Hvordan er politiets/Forvarets IKT organisert?
   Eventuelle oppfølgingsspørsmål
   - Hvordan gjennomføres anskaffelser av nytt materiell/tjenester?
   - Drift?
   - Viktige systemer/tjenester?

Lover og regelverk:

4. Hvilke generelle lover og regelverk legges til grunn for et eventuelt samarbeid med andre etater for politiet/Forsvaret?

5. Hvilke lover og regelverk er førende innenfor IKT for politiet/Forsvaret innen:
    - Organisering/Bemanning?
    - Krav til IKT-systemene?
    - Økonomi?
    - Sikkerhet og redundans?
    - Samhandling med andre?

Føringer:

6. Hva har Forsvaret/politiet av føringer fra overordnede/departementet for samarbeid med andre etater?

7. Hvilke føringer har dere for å konkurranse utsette innkjøp og drift av IKT-systemer?

8. Hvilke føringer gjelder for bruk av private aktører. (Drift og anskaffelse)

9. Hvilke andre offentlige etater ser dere at det kan være hensiktsmessig å etablere et samarbeid innenfor IKT?

10. Hvorfor akkurat denne aktøren?

Kunnskap om samarbeidspartner

11. Hvilken kjennskap har du til politi/Forsvarets IKT-systemer eller organisering? (Den andre aktøren)

12. Har du kjennskap om systemene, drift og anskaffelser hos som politiet/Forsvaret?

13. Har du kjennskap til eksiterende samarbeid mellom politi og Forsvaret i dag?
    - Om ikke ta opp Meldingstjenesten og Nødnett
    - Noen erfaringer knyttet til dette?

14. Er det noen av systemene/tjenestene hos den andre aktøren som dere har behov for? (Operative, administrative, teknisk)

Interne forhold:

15. Hva er de generelle holdningen til samarbeid med andre etater for politiet/Forsvaret ved avdelingen?

16. Hvordan vil et samarbeid med politi/Forsvart innenfor IKT bli mottatt i din avdeling?

17. Hvordan tror du en slikt samarbeid med vil bli mottatt av overordnede/underordnede avdelinger?

18. Er det noe med politiet/Forsvaret som gjør et slikt samarbeid mer problematisk enn andre statlige aktører?

19. Dersom Politiet/Forsvaret leverte deler av IKT løsning/tjenesten hvordan vil dette bli sett på internt?

20. Vil dette sees på som noe positivt, eller vil dette kunne skape uro i organisasjonen?

21. Hvilke endringer vil et økt samarbeid innenfor IKT kunne få for politiet/Forsvaret innen:
    - Organisering/Bemanning?
    - Krav til IKT-systemene med kontroll over drift og anskaffelser?
    - Økonomi?
    - Kvalitet, sikkerhet og redundans?
    - Samhandling og prioritering?

Samarbeid:

22. Hvilke type tjenester ser du for deg politiet/Forsvaret kan gi til Forsvaret/politiet?

23. Hvilke type tjenester ser du for deg politiet/Forsvaret kan gi Forsvaret/politiet?

24. Hvilke områder innenfor IKT tror du det vil være mest hensiktsmessig å inngå et samarbeid? Hvorfor?

25. Hvilke områder vil det ikke være aktuelt med et samarbeid innenfor IKT? Hvorfor?

26. Hvilke operative fordeler eller ulemper ser du med et slikt samarbeid?

27. Hvilke fordeler, ut over tidligere nevnt, ser du med tanke på et samarbeid mellom politi og Forsvar?

28. Hvilke utfordringer, ut over tidligere nevnt, ser du med tanke på et samarbeid mellom politi og Forsvar?

Oppsummering:

29. Hva mener du er det viktigste momentet som fremmer et økt samarbeid mellom politiet og Forsvaret innenfor IKT.

30. Hva mener du er det viktigste momentet som hemmer et økt samarbeid mellom politiet og Forsvaret.

Avslutning:

Takker for intervjuet
Spørre om det er noe som ikke er som ikke er tatt opp som burde vært belyst i forbindelse med oppgaven.
Avslutte lydopptaket.

Etter intervjuet:

Forslag til andre personer som burde intervjues
Forslag til skrevne kilder

Fortelle om videre prosess med oppgaven og om muligheten til å eventuelt lese transkripsjon og oppgaven dersom det er ønskelig.

Vedlegg A Samtykkeerklæring

Informasjonsskjema

Forespørsel om deltagelse i forskningsprosjekt

Kan Forsvaret og politiet samarbeid innenfor IKT?

Bakgrunn og formål

Jeg skriver masteroppgave ved Forsvarets Høgskole/Stabsskolen. Hensikten med masteroppgaven vil være å undersøke mulighetsrommet for samarbeid mellom politi og Forsvaret om IKT-tjenester. Hvilke muligheter og begrensinger finnes for økt samarbeid innenfor IKT mellom politi og Forsvaret. Oppgaven skal leveres våren 2018. Masteroppgaven bli lagt ut på internett

Hva innebærer deltagelse i studien?

Du vil som intervjuobjekt være førstehåndskilde som kan bidra til å besvare deler av studien. Du er anbefalt og utvalgt som intervjuobjekt med bakgrunn i din kunnskap, kompetanse og nåværende eller tidligere tjenestefunksjoner. Jeg har som utgangspunkt ikke tenkt å anonymisere informasjon fra intervjuet, men jeg vil anonymisere dersom dette er ønskelig.

Oppgaven vil i utgangspunktet være ugradert slik at den kan være tilgjengelig for flest mulig lesere. Dersom respondenten har behov for benytte gradert informasjon for å få frem viktige poeng, vil dette måtte håndteres i henhold til sikkerhetsloven.

Intervjuet vil vare ca. 1-1.5 time. Du vil i forkant av intervjuet motta mer informasjon på epost slik at du kan ha mulighet til å forberede deg. Jeg ønsker å ta opp intervjuet på lydfil og

ta notater underveis, men dersom det ikke er ønskelig med lydfil vil jeg kun benytte notater underveis i intervjuet.

Hva skjer med informasjonen om deg?

Alle personopplysninger vil bli behandlet konfidensielt. Lydfilen og notater vil bli lagret på min PC, og vil kun være tilgjengelig for meg og mine veiledere. Sitater og utsagn vil bli anonymisert i oppgaven dersom dette er et ønske. Prosjektet skal etter planen avsluttes i juli 2018. All informasjon innhentet i forbindelse med intervju vil bli slettet når sensur på oppgaven faller i juli 2018.

Frivillig deltakelse

Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi noen grunn. Studien er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste AS. All informasjon vil bli behandlet i tråd med Personvernforbundets retningslinjer og i henhold til generelle forskningsetiske retningslinjer.

Dersom du har spørsmål til studien ta kontakt med Arve Christensen, tlf. 40448376 eller mail: arvech@gmail.com
Veileder er:
Ingerid M. Opdal, ingerid.opdahl@ifs.mil.no
Magnus Håkenstad, mhakenstad@ifs.mil.no

Samtykke til deltagelse i studien

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

☐ ***Jeg samtykker til bruk av lydopptaker***

☐ ***Jeg ønsker at mine sitater og utsagn anonymiseres i studien.***

Dato:

(Signert av prosjektdeltager)