FORSVARET
Forsvarets høgskole

Logistikk i en Cyberkontekst

Hvordan påvirker økt bruk av sivile aktører i forsyningskjeden informasjonsdelingen mellom Forsvaret og sivile leverandører?

John Anders Bestum

Forord

Denne masterstudien markerer avslutningen på to år med studier ved Forsvarets Høgskole. Det har vært en spennende tid med både opp- og nedturer. For det første har det vært et privilegium å kunne sette seg inn i interessant tematikk og fordype seg på heltid. På den annen side har det tidvis vært frustrerende å få omgjort tanker og ideer til skriftlig vitenskapelig arbeid. Jeg har lært mye gjennom arbeidet med denne oppgaven, men å omsette læringsutbyttet til en samfunnsvitenskapelig tekst har vært svært krevende.

Først og fremst vil jeg takke min kone Sylvi, som har støttet og holdt ut med meg gjennom hele perioden. Jeg vil også rette en takk til min veileder Per Skoglund for metodisk veiledning og faglig støtte.

En stor takk rettes også til mine respondenter og kolleger som velvillig har stilt opp til intervju og samtaler, og således bidratt til at jeg har kunnet gjennomføre studien.

Alle vurderinger i denne oppgaven står for min regning.

Lillehammer 2016-05-20

John Anders Bestum

Sammendrag

Denne mastergradsstudien i regi av Forsvarets høgskole (FHS) ser på hvordan økt bruk av sivile aktører i forsyningskjeden påvirker informasjonsdelingen mellom Forsvaret og sivile aktører. Studien har en kvalitativ tilnærming og fokuserer på digital informasjonsutveksling og konsekvensene ved økt utveksling sett i lys av informasjonssikkerhet og forvaltning av understøttelsessystemene.

Studien tar utgangspunkt i teoriene om Supply chain management (SCM), Prestasjonsbasert logistikk (PBL), forsyningskjeder og Enterprise resource planning (ERP) som alle har informasjonsdeling som viktig premiss for at de skal fungere. Deretter er det med bakgrunn i gjennomførte intervjuer med respondenter fra avdelinger med forskjellige roller sett på hvordan disse påvirkes av utviklingen. Dette er avdelinger innenfor systemstyring, drift og videreutvikling (DVU), DVU logistikk, prosjekt- kampvogn og kampfly integrasjon verksted for landmateriell og innkjøp ved Forsvarsmateriell (FMA). Hensikten har vært å få analysert utfordringene fra flere sider fremfor å gå i dybden for på den måten å få belyst flere aspekter ved informasjonsdelingen.

Funn i studien peker på at en utvikling med økt behov for informasjonsutveksling vil fordre en styrket merkantil kapasitet. Videre må det på plass en enhetlig arkitektur og konsolidering av understøttelsessystemene på driftssiden. Manglende MLS løsning og krav til sikkerhet trekkes frem som årsak til mye ekstraarbeid og som et hinder for Forsvaret i å realisere gevinstpotensialet.

Ut fra hovedfunn er det rimelig å anta at en økt bruk av sivile aktører i forsyningskjeden vil, all den tid en ikke har på plass en løsning for effektiv informasjonsutveksling, medføre vesentlig økt ressursbruk. En kan derav konkludere med at det teoretiske rammeverket ikke passer overens med funn i analysen. All den tid premisset for effektiv informasjonsutveksling ikke er tilstede. Derav er kanskje ikke økt sivilisering av forsyningskjeden vegen å gå ut fra et økonomisk perspektiv, men på den annen side, hva er alternativet?

> *Det er uunngåelig i fremtiden at vi ikke skal dele informasjon. Det blir mer og mer av det, så vi må bare bli bedre til å håndtere det, og vite hvordan vi skal tilnærme oss det!* (R6).

Summary

This thesis is written under auspices of the Norwegian Defence University College (NDUC) and looks at how increased use of civilian actors in the supply chain affects information sharing between defence and civilian actors. The study has a qualitative approach and focuses on digital information and the consequences of increased exchanges in light of information security and management of support systems.

This study is based on theories of supply chain management (SCM), supply chain, performance based logistics (PBL), and enterprise resource planning (ERP) all of which have information sharing as important premise for them to function. Several respondents from different departments were interviewed to look at how they were affected by current developments. All respondents work in the field of management; Norwegian Cyber Defence Cyber Services and Operations (NOR CYDEF) project Fighting Vehicle and aircraft integration, workshop for land supplies and procurement by Norwegian Defence Material Agency (NDMA). The intention has been to shed light on the challenges from several angles rather than going in depth so as to reveal several aspects of information sharing.

Findings of the study point out that increased demand for information will require a strengthened contract capacity. Moreover there must be established a unified architecture and consolidation of the support systems on the operational side. Missing Multi Level Security (MLS) solutions and security requirements seem to be drivers for considerable increases in work and maintenance and consequently a hindrance for defence in realizing potential gains.
Based on the main findings, it is reasonable to assume that a greater use of civilian actors in the supply chain will, as long as one does not have a solution for effective information sharing in place, involve substantially increased resource use.

One can therefore conclude that the theoretical framework does not match with the results of the analysis. All the time the premise for effective exchange of information is not present.
Thereof increased civilization of supply chain may not bee the future in an economic perspective, but on the other hand, what is the alternative?

It is inevitable in the future that we will not share information with our suppliers. It becomes more and more common, so we just have to be better to deal with it, and know how we should approach it!

Innholdsfortegnelse

Figuroversikt

Tabelloversikt

1 Innledning

Denne delen av studien gir først en introduksjon av bakgrunnen for oppgaven og en beskrivelse av problemet, forskningsspørsmål og oppgavens hensikt. Deretter følger en avgrensing av oppgavens omfang. Kapittelet avsluttes med noen nøkkelbegreper og en oversikt over studiens struktur.

1.1 Bakgrunn

Opp gjennom historien, fra Alexander Den Store til dagens konflikter, har en fått erfare at logistikken er en vesentlig og uatskillelig del av det militære virke. Logistikk kan på mange måter sies å være hygienefaktoren[1] ved en militær operasjon så vel som i daglig drift. Innføringen av New Public management (NPM) fra 1980 tallet (Heier, 2011, s. 50), og ett stadig fokus på effektivisering av Forsvarssektoren (Forsvaret, 2015a, s. 4), sammen med et endret trusselbilde (Meld. St. 37 (2014-2015), 2015, s. 9), har medført store endringer i hvordan en organiserer og utfører understøttelsen i Forsvaret. Trange forsvarsbudsjetter tvinger frem behovet for å tenke smartere og mer kosteffektivt, samtidig som forsvarsevnen og kampkraft skal ivaretas. Markedsøkonomisk teori sier at bedrifter i et konkurranseutsatt marked tvinges til å produsere billigere eller bedre for å overleve, da de ikke har den økonomiske beskyttelsen det offentlige, herunder Forsvaret, opererer under (Pindyck, Rubinfeld, & Synnestvedt, 2013, s. 205; Østre, 2014, s. 2). For å få mest mulig ”*Bang for the buck”* har en derfor sett på nye måter å utøve understøttelsen (Borgen, 2013, s. 42). I det senere har Supply Chain Management (SCM) vært ett av satsningsområdene. SCM ser på logistikken i et helhetsperspektiv fra produsent til sluttbruker. Det være seg horisontal samhandel internt i Forsvaret, sivilt militært samarbeid eller outsourcing av virksomhet som ikke er kjernevirksomhet. SCM søker optimalisering av ressursbruken gjennom forsyningskjeden ved eventuelt å relokalisere og effektivisere de enkelte elementer i et helhetsperspektiv. Denne form for relokalisering og justering av hvem som gjør hva styres gjennom gjensidige avtaler aktørene i mellom, og omtales som prestasjons basert logistikk (PBL). PBL har sitt utspring fra det sivile næringsliv på lik linje som SCM, og kan sees på som et virkemiddel for å få en effektiv forsyningskjede. Forsvarets logistikk har mange likhetstrekk med sivil logistikk, men det er også en del områder som er særegne for Forsvaret.

[1] Fredrick Herzberg (f.1923) utviklet en tofaktor teori der den ene ”hygienefaktoren” må være tilstede for å skape grunnlag for trivsel/produktivitet (les kampkraft). Trivsel i seg selv gir ikke økt produktivitet, men er ett premiss som må være tilstede for å få det.

Eksempler på forskjeller er krav til at logistikken skal virke i fred så vel som i krise og krig. Videre har Forsvaret skjermingsverdig informasjon som i ytterste konsekvens kan berøre rikets sikkerhet. En annen trend i samfunnet har vært innføringen av Enterprise Resource Planning (ERP) systemer. For Forsvarets del kom dette med innføringen av Felles Integrert Forvaltningssystem (FIF) der SAP er motoren som ligger i bunn. Kongstanken ved innføringen av ERP er at den interne informasjonsflyten skal bli bedre ved at "all" informasjon samles på ett sted. Dette gjøres ved at informasjonen samles i SAP basen, for Forsvarets del, og at den enkelte saksbehandler kan hente ut og legge inn data som så umiddelbart blir tilgjengelig for øvrige interne instanser som har bruk for dem (Melbo, 2006, s. 10-11).

Forsvarssjefen anbefaler i forsvarssjefens fagmilitære råd (FMR) en økt sivilisering av logistikken (Forsvaret, 2015a, s. 58). Informasjonsdeling er ansett for å spille en avgjørende rolle for å oppnå en positiv effekt på SCM, PBL-avtaler, forsyningskjeden eller ERP systemet (Kulp, Lee, & Ofek, 2004, s. 431; Mentzer et al., 2001, s. 8; Vitasek & Geary, 2008; Aar, 2015, s. 32). Deling av informasjon til sivile kan for Forsvaret ofte være problematisk av sikkerhetsmessige årsaker, da Forsvarets informasjon befinner seg på en gradert plattform (Skoglund, 2012, s. 70). Hvordan treffer dette Cyberforsvaret? Er det samsvar mellom teori og praksis i utførelsen, eller er det uheldige konsekvenser ved økt behov for informasjonsdeling med sivile aktører? Det antas at et økt behov for informasjonsdeling med sivile leverandører har konsekvenser i en cyberkontekst. Med cyberkontekst menes i denne sammenheng de som har i oppdrag å tilrettelegge for god informasjonsflyt og samtidig ivareta informasjonssikkerheten i det digitale domenet. Det er lite studier på informasjonsutveksling mellom Forsvaret og sivile aktører, og av de få som er skrevet det er ikke funnet noen som ikke er gradert eller unntatt offentlighet.

1.2 Utvikling av problemstilling

Direktør i Forsvarsmateriell (FMA) er gjennom retningslinjer for logistikkvirksomheten i forsvarssektoren, gitt ansvar for fremskaffelse av materiellsystemer, forsyninger og tjenester i Forsvaret. Hun skal blant annet ivareta eierskapsforvaltningen i hele materiellets levetid med hensyn til ytelse, teknisk tilgjengelighet og materiellsikkerhet. Hun skal også i samråd med bruker definere vedlikeholds og forsyningskonsept for nye systemer til Forsvaret (Forsvarsdepartementet, 2016a, s. 8-9). Sjef FLO har videre bestemt at "*Forvaltning av forsvarets materiellsystemer skal skje ved hjelp av Forsvarets Felles Integrerte*

Forvaltningssystem (FIF)." (Forsvarets Logistikk Organisasjon, 2010, s. 9). Denne ligger på Forsvarets plattform FISBasis som er gradert BEGRENSET[2]. For å få til en god og sømløs informasjonsutveksling vil en enten måtte autorisere leverandør for tilgang til FISBasis, eller etablere metoder for utveksling av informasjon mellom graderingsnivåer. Sistnevnte fordrer også at informasjonen leverandør trenger er UGRADERT. Etablering av FISBasis utenfor Forsvarets kontrollerte område er en omfattende prosess, der det stilles strenge krav til utforming av bygg, prosedyrer, tilgangskontroll, kryptoforvaltning, sikkerhetsorganisasjon med mer. Det er derfor meget kostnadskrevende og utfordrende å få til. Etablering av metoder for utveksling av informasjons mellom graderingsnivåer er også en omfattende sak. Dette er blant annet regulert i Forskrift om informasjonssikkerhet som gir føringer for hva som er mulig og ikke. Her ligger blant annet krav om at "*Det skal etableres en helhetlig og enhetlig IKT-infrastruktur med nødvendige sikkerhetsfunksjoner, -strukturer og tillitsnivå"* (FOR-2001-07-01-744: Forskrift om informasjonssikkerhet, §5-2). Det er videre gitt føringer som avgrenser mulighetene for sammenkobling av informasjonssystemer ved at de skal ha samme graderingsnivå (FOR-2001-07-01-744: Forskrift om informasjonssikkerhet, §5-8).

Ut fra et driftsteknisk og sikkerhetsmessig perspektiv er det ønskelig med størst mulig grad av variantbegrensing på informasjons- og kommunikasjonsteknologi (IKT)-systemer og plattformer (Forsvarssjefen, 2013, s. 6). Dette for lettere å sikre dem mot uønskede hendelser. En god variantbegrensing letter også konfigurasjonskontrollen, noe som igjen bidrar til mer robuste og sikre systemer. En stor utfordring er at en ønsker økt bruk av sivile aktører i forsyningskjeden, deriblant gjennom PBL kontrakter. En av forutsetningene som fremmer denne typen kontrakter er høy grad av informasjonsdeling og integrasjon. Innen forvaltning av informasjonsstyring er det også en rekke rammebetingelser å forholde seg til. Dette er lover og regler fra det sivile samfunn, føringer og pålegg fra FMA, Cyberforsvaret, Nasjonal sikkerhetsmyndighet (NSM), forsvarssjefen med flere, som legger restriksjoner som tilsynelatende vanskeligjør en slik informasjonsdeling. Innen forskermiljøet pågår det også en diskusjon på linken mellom intern informasjonsdeling og dennes knytning til interne IKT systemer. Det hevdes at det er lite trolig at et firma kan dele informasjon og data med eksterne partnere dersom det ikke har et velfungerende ERP-system som integrerer data og deler informasjon mellom interne enheter (Zhao, Huo, Selen, & Yeung, 2011, s. 19). Ut i fra et cyberperspektiv er det derfor av interesse å

[2] *"BEGRENSET nyttes dersom det i noen grad kan medføre skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende." (Sikkerhetsloven, 1998§11)*

få analysert hvilke implikasjoner en dreining mot økt sivilisering av logistikken og derigjennom økt informasjonsdeling vil ha. Denne studien bygger videre på deler av tidligere studier innen PBL, SCM, ERP og forsyningskjeder. Der det er elementene som berører informasjonsdeling som danner grunnlaget for denne studien. Redegjørelse for de mest aktuelle studiene kommer i kapittel 3.

1.2.1 Problemstilling

Ut fra beskrivelsen av situasjonen har jeg kommet fram til en problemstilling som søkes forsket på i denne studien. Problemstillingen ble:

Hvordan påvirker økt bruk av sivile aktører i forsyningskjeden informasjonsdelingen mellom Forsvaret og sivile leverandører?

1.3 Oppgavens hensikt

Cyberforsvaret har i oppdrag å understøtte Forsvarets virksomhet med styringssystemer og IKT-infrastruktur. Oppgaven har til hensikt å analysere noen av de konsekvensene en økt sivilisering av logistikken vil kunne medføre sett i et cyberperspektiv[3]. Hva betyr det for Forsvaret at det er et økende behov for informasjonsdeling mellom gradert plattform (FISBasis B) og ut til sivile leverandører og visa versa. Er det mulig å understøtte Forsvarets virksomhet på en god måte? Studien er vitenskapelig og praktisk relevant da det ikke er nyere studier på hvilke konsekvenser et slikt økt informasjonsdelingsbehov vil ha. Derimot er det mye litteratur som peker på at informasjonsdeling og integrasjon mellom kunde (Forsvaret) og leverandør er en forutsetning for en velfungerende forsyningskjede.

For å besvare problemstillingen vil studien ta for seg to forskningsspørsmål, henholdsvis F1 og F2, for å belyse problemstillingen. Forskningsspørsmålene er henholdsvis:

F1: *Hvilke konsekvenser får økt sivilisering av forsyningskjeden for informasjonssikkerheten?*

[3] Cyberperspektiv går på at det sees i lys av Cyberdomenet. I denne studien defineres Cyberdomenet som " *Fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data. Synonym: Det digitale rom*" (Forsvarsdepartementet, 2014, s. 5).

Forskningsspørsmålet ser på det sikkerhetsmessige aspektet ved å utveksle datainformasjon mot sivile leverandører og hvilke konsekvenser dette vil kunne få.

> F2: *Hvilke konsekvenser får økt sivilisering med hensyn til forvaltning av understøttelsessystemet?*

Forskningsspørsmålet ser på hvilke forvaltningsmessige konsekvenser en økt bruk av sivile aktører vil kunne få.

1.4 Avgrensning

Det er i litteraturen for PBL flere faktorer som fremmer (enablers) eller hemmer (barriers). Håbjørg (2015) har i sin masteroppgave sett på forhold som fremmer (påvirker positivt) og hemmer (påvirker negativt) i en norsk forsvarskontekst. Hun har sett på PBL-avtaler knyttet til drift og vedlikehold av motor F100 til F-16 kampfly og vedlikehold på C-130J Hercules transportfly, og kommet frem til at det er tre forhold som fremmer. Dette er *"Forbedret leveranse, informasjonsdeling og tillitsrelasjoner" (Håbjørg, 2015, s. 70)*. Tilsvarende trekkes informasjonsdeling frem som et premiss for at et ERP system skal fungere (Somers & Nelson, 2001, s. 5). Innen SCM og forsyningskjeder trekkes integrasjon og informasjonsdeling frem som et suksesskriterium (Kulp et al., 2004, s. 431; Mentzer et al., 2001, s. 8; Mohr & Spekman, 1994, s. 139; Porterfield, 2008, s. 42).

Jeg vil i denne studien avgrense meg til å fokusere på de implikasjoner som oppstår med hensyn til informasjonsdeling i det digitale domenet eller cyberdomenet. Hva som legges i cyberdomenet i denne studien er beskrevet under nøkkelbegreper i kapittel 1.5. Videre avgrenses studien til å omhandle informasjonsdeling og integrasjon mellom Forsvarets FIF løsning og sivile aktører. Det vil med andre ord ikke ta for seg utveksling eller integrasjon mellom de ulike graderingsnivåene innad i Forsvaret. Studien vil heller ikke ta for seg løsningene til Fregatt eller NH90 helikopter, men konsentrere seg om konsekvensene ved utvalgte enheter redegjort for under kapittel 2.5 *utvalg av enheter.*

1.5 Nøkkelbegreper

I det følgende vil det forklares noen sentrale begreper og hva som legges i disse i denne studien.

1.5.1 Multilevel security (MLS)

Med Multilevel security menes et system som samtidig kan håndtere (f.eks. dele og bearbeide) flere nivåer av data eller informasjon. Dette gjør at brukerne på ulike sikkerhetsnivåer (f.eks. UGRADERT og BEGRENSET) kan få tilgang på systemet samtidig. Systemet som sådan sikrer at den enkelte bruker bare får tilgang til informasjon den enkelte er akkreditert for. (Information Assurance Directorate, 2008, s. 23)

1.5.2 Informasjonsdeling

Det er mange former for informasjonsdeling. Det være seg ved utveksling av informasjon mellom ulike organisasjoner, mennesker og teknologi i ulike former. Videre er det mange former for informasjon. Den kan være i papirformat, et bilde, tale eller en digital fil. Med informasjonsdeling menes i denne studien deling eller utveksling av digitale data mellom Forsvaret og sivile aktører ved anvendelse av FIF.

1.5.3 Informasjonssikkerhet

I denne studien legges FDs cyberretningslinjers definisjon av informasjonssikkerhet til grunn. Den sier informasjonssikkerhet er:

> *Sikkerhetstiltak for i nødvendig grad å oppnå konfidensialitet, integritet, tilgjengelighet og autentisitet ved behandling av informasjon i alle situasjoner, uavhengig av verktøy og metoder.* (FDs cyberretningslinjer, 2014).

Konfidensialitet: innebærer beskyttelse mot at informasjon blir kjent for uvedkommende, og dermed at bare de vi gir lov til å se informasjonen, faktisk får se den. Det er verdt å merke seg at konfidensialitetsbrudd i praksis er uopprettelige i det digitale domenet (NOU 2015:13, 2015, s. 34). En undersøkelse vil mest sannsynlig fortelle deg at det er dette de fleste betrakter som informasjonssikkerhet. Her inngår typisk ting som skallsikring, adgangskort, koder/passord, kryptering, nøkler til arkivskuffen, brannmur med mer.

Tilgjengelighet: innebærer at informasjonen er tilgjengelig for brukere når de har behov for denne. Dette innebærer at en sørger for at informasjonen er tilgjengelig for de som har et legitimt behov til den, når behovet er der (NOU 2015:13, 2015, s. 34). I tilgjengelighet ligger alt av ulike

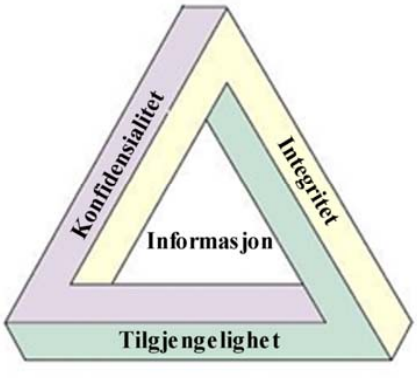
datasenterløsninger som RAID[4], Cluster[5] og et fokus på tilgjengelighet og kapasitetsplanlegging. Dette kan for eksempel være å skaler systemene slik at de takler for ressurspeaks for å sikre at systemet ikke går ned. Et typisk eksempel på det er når ligningene legges ut og "alle" skal inn og se samtidig. En får da et veldig press på systemene som en må ha et bevist forhold til om en skal skalere for eller ikke. Det blir en kost nytte vurdering mellom konsekvens ved ikke å få tilgang versus kostnadene ved å øke kapasiteten på systemet.

Integritet: innebærer at informasjon er til å stole på, og at systemer og tjenester fungerer slik det er tenkt. Informasjonen skal være korrekt og gyldig. Bare de som har lov til å endre informasjonen, får endret den. Nært beslektet er *Autentisitet* som handler om å sikre opphavet til informasjonen, for eksempel bekrefte identiteten til en sendt melding (NOU 2015:13, 2015, s. 35). Hvert år leser en om saker der en person har mottatt brev om noe som angikk en avdød ektefelle eller en eiendom som er revet for flere år siden fra kommunen. Dette er typiske eksempler på dårlig datakvalitet. Ofte som følge av at noen har glemt å slette/oppdatere et system, eller så er det en "datavask" jobb som ikke er kjørt hyppig nok.

Sporbarhet: Sporbarhet handler om å kunne finne ut hva som har skjedd, i etterkant, for eksempel hvem som har håndtert informasjonen, og hvor den har vært kommunisert. Typiske eksempler er tilgangslogger, endringslogger og andre typer hendelseslogger. Kompromittering av sporbarheten innebærer at det blir vanskelig eller umulig å etterforske i ettertid (NOU 2015:13, 2015, s. 35).

Figur 1 viser en modell av de mest brukte begrepene innen informasjonssikkerhet, og hvordan det er gjensidig avhengighet mellom dem. I dette legges at det holder ikke å fokusere på integritet og konfidensialitet om en ikke har tilgjengelighet. En må nivellere tiltakene opp mot hverandre for å sikre at alle aspekter ved informasjonssikkerhet blir ivaretatt på en hensiktsmessig måte, da hver enkelt faktor er avhengig av de to andre. Så for å få et velbalansert informasjonssystem må alle tre være tilstede i tilstrekkelig grad ut fra viktigheten av informasjonen i systemet.

[4] RAID er betegnelsen på en teknologi for feiltolerant datalagring. Gjennom fordeling og duplisering av data over flere harddisker. Teknologien gjør at om én disk feiler, vil ingen data gå tapt, og det vil fortsatt være mulig å lese og skrive data til disksystemet.
[5] Cluster er ett sett av løst eller tett koblet datamaskiner som fungerer sammen slik at de på mange måter kan bli sett på som et enkelt system.



Figur 1 KIT-modell (Didriksen, 2008, s. 3)

1.5.4 Risiko

Risiko defineres som summen av sannsynlighet for at en uønsket hendelse skal inntreffe multiplisert med konsekvensen av at den inntreffer (Direktoratet for samfunnssikkerhet og beredskap, 2014). For denne studien eksemplifisert ved sannsynlighet for at noen får tilgang på informasjon vi ikke ønsker å dele, multiplisert med konsekvensen av at den informasjonen er kommet på avveie. For Forsvaret er det essensielt å ha et bevist forhold til risikobegrepet og det er derfor også krav om at det skal gjennomføres risiko og sårbarhetsanalyse for all aktivitet (ROS-analyse). Innen drift av IKT er tiltak som variantbegrensning og konfigurasjonskontroll på systemene tiltak for å redusere risikoen. Ved å ha variantbegrensning vil det bli færre systemer å holde kontroll på med hensyn til sårbarheter. En vil også kunne få bedre ombyttbarhet, eller at en kan gjenbruke komponenter fra ett system i et annet system da konfigurasjonen som sådan er lik. Konfigurasjonskontrollen på sin side søker å sikre at systemene til enhver tid har siste oppdateringer slik at kjente svakheter og hull i systemsikkerheten blir tettet så raskt som mulig.

1.5.5 Cyberdomenet

Cyberdomenet blir ofte grovt delt inn i tre deler fra Open Systems Interconnection Basic modell (OSI-modellen). Det laveste laget er det fysiske laget som består av hardware slik som selve datamaskinene med tilhørende kabler, fiber og rutere. Dette er det fysiske grensesnittet og mekanismer for å plassere en rå strøm av databits i nettverkskablene. Det andre laget som betegnes som det syntaktiske, det er laget som styrer informasjonsflyten mellom de enkelte programmer og ivaretar mekanismer for utveksling mellom de enkelte komponentene. Det tredje laget er det semantiske. Det er her koblingen mellom menneske og maskin foregår. Det brukerne ser og opplever når de knytter seg sammen i nettverk som for eksempel Facebook (Langø &

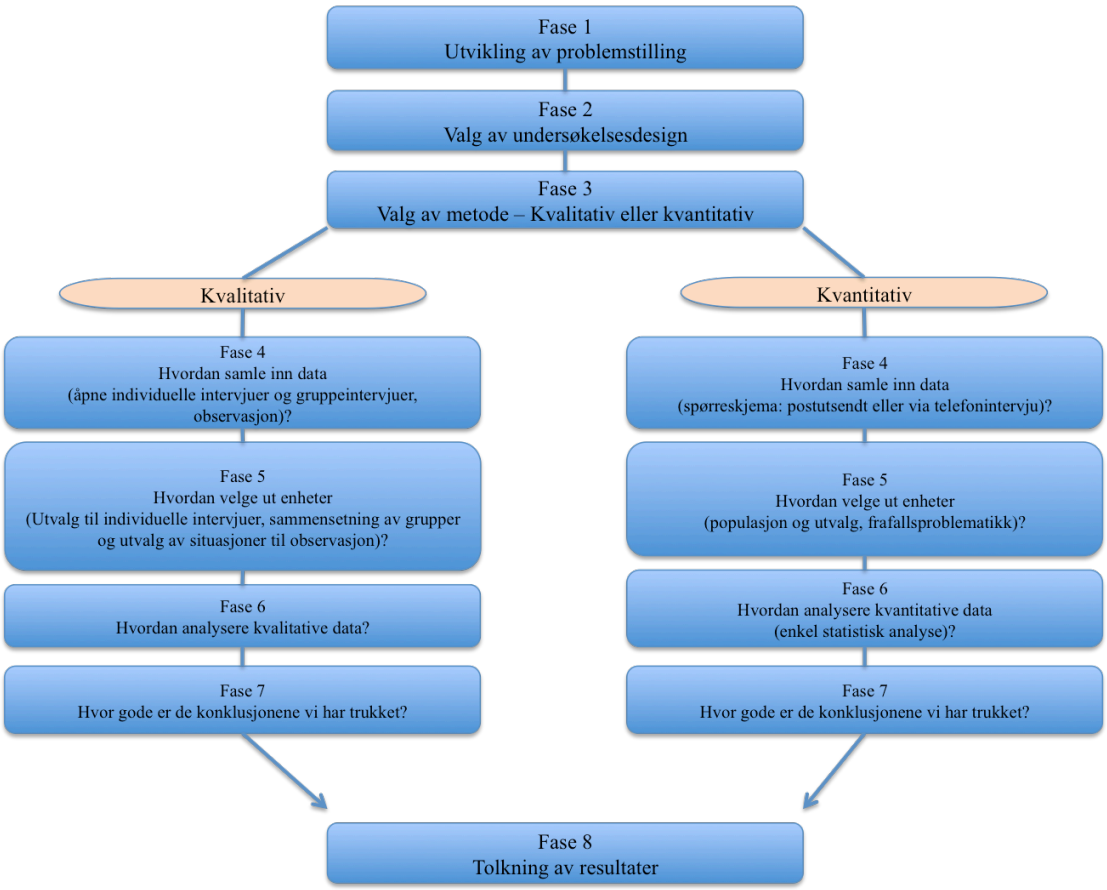
Sandvik, 2013, s. 222). Cyberdomenet er således en samlebetegnelse for disse forskjellige nivåene i utveksling av informasjon. Det finnes flere definisjoner i litteraturen på hva cyberdomenet er. I min studie vil jeg nytte definisjonen ” Fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data. Synonym: Det digitale rom” (Forsvarsdepartementet, 2014, s. 5).

1.6 Studiens struktur

I første kapittel fremlegges bakgrunn og beskrivelse av problemstillingen. Det fremkommer også der hvorfor studien har vitenskapelig og praktisk relevans. I kapittel 2 går en gjennom metoden som er nyttet for gjennomføringen av studien, samt hvilke vurderinger som er lagt til grunn for valgt metodikk. Kapittel 3 omhandler litteraturstudiet og det teoretiske rammeverket for denne studien. Kapittel 4 og 5 tar for seg empiri og rammefaktorer, før det i kapittel 6 oppsummeres hvilke faktorer som skal brukes i analysen. I kapittel 7 kommer først en analyse og drøfting av forskningsspørsmålene opp mot de enkelte faktorer, før en oppsummering av funn per forskningsspørsmål. Kapittel 8 inneholder konklusjon av de viktigste funn fra studien og forslag til videre forskning. Avslutningsvis følger noen refleksjoner rundt denne studiens styrker og svakheter.

2 Metode

For å sikre en god struktur og at alle momenter i fremgangsmåten i studien blir dekket vil studien ta utgangspunkt i modellen til Jacobsen (Jacobsen, 2015, s. 68). Modellen tar for seg de enkelte steg i en vitenskapelig studie og består av 8 faser, der fase fire til syv avhenger av hvorvidt det velges kvalitativ eller kvantitativ tilnærming.



Figur 2 Faser i undersøkelsesprosessen (Jacobsen, 2015, s. 68)

Jacobsen tar i de første kapitlene i boken for seg empiri, litteraturstudie og forskjellige tilnærmingsmetoder til selve metoden. Han går også gjennom etiske og praktiske avveininger som må vurderes opp mot metoden en velger å benytte. Deretter følger de enkelte steg i undersøkelsesprosessen tildelt hvert sitt kapittel i boken.

2.1 Første fase - Utvikling av problemstilling

Enhver undersøkelse starter med at en er nysgjerrig på eller ønsker å finne ut mer om ett eller annet begrenset tema. Dette kan begynne med et enkelt spørsmål eller en antagelse om en

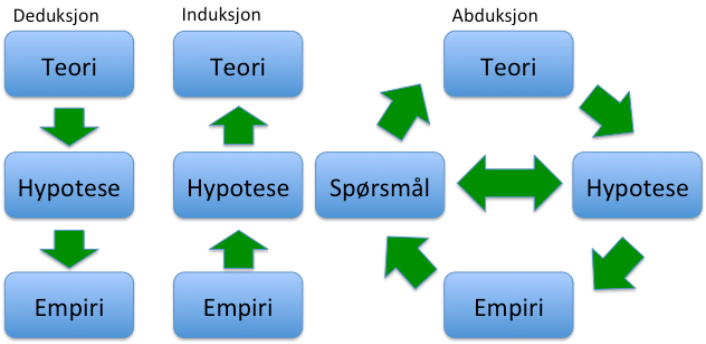
sammenheng eller mangel på sådan (Jacobsen, 2015, s. 71). For min studie startet det med en interesse for sammenhengen mellom informasjonsflyten i logistikken og Cyberforsvarets evne til å understøtte prosessene slik at de enkelte aktører kan få riktig informasjon. Det fremsto som om det var mange aktører som hadde interesse av at informasjonsdeling skulle finne sted, men det fremkom ikke hvordan dette skulle løses i en militær setting. Med militær setting menes her de graderingsmessige og sikkerhetsmessige utfordringer som skiller Forsvaret fra de fleste sivile aktørene. Det var også begrenset med litteratur på hvilke konsekvenser en tilrettelegging og integrering av mekanismer for informasjonsutveksling ville ha ut fra et sårbarhet eller sikkerhetsperspektiv. Ut fra dette ble spørsmålet som ble lagt til grunn for utvikling av problemstillingen: *Hvilke implikasjoner har det økte behovet for informasjonsdeling som følge av større bruk av sivile aktører i forsyningskjeden, og hva betyr det for cyberforsvaret?*

Kravene til en problemstilling er at den skal være spennende, enkel og fruktbar (Jacobsen, 2015, s. 77). For utviklingen av problemstilling i denne studien anses kravene å være fylt, da det er en dagsaktuell problemstilling som vil tilføre Forsvaret ny kunnskap innen et område det er lite tidligere forskning på. Enkelheten er søkt dekket gjennom en avgrensning til å se på to aspekter ved siviliseringen av forsyningskjeden. Dette er henholdsvis informasjonssikkerhet og forvaltningen av understøttelsessystemet.

Det skilles gjerne mellom beskrivende og forklarende problemstillinger, hvor beskrivende søker å kartlegge trekk ved situasjonen, mens den forklarende skal avdekke sammenhenger mellom årsak og virkning (Jacobsen, 2015, s. 82-83). Før en går videre til andre fase i valg av metode må en i følge Jacobsen også stille spørsmålet om studien skal være generaliserbar eller ikke (Jacobsen, 2015, s. 86). Dette har betydning for størrelsen på utvalgte enheter en undersøker. Jo større utvalget er jo mer vil en kunne generalisere resultatene. Ved lite utvalg vil en konsentrere seg om noen få utvalg og heller søke å gå i dybden. Dette vil typisk være undersøkelser der en benytter intervju som en av datainnhentingsmetodene.

Denne studiens problemstilling vil betegnes som beskrivende og eksplorerende da den har til hensikt å finne implikasjoner ved informasjonsdeling. Den vil være eksplorerende fordi den tar for seg noen få faktorer i søken etter å avdekke hvilke konsekvenser disse får ved å gå i dybden (Jacobsen, 2015, s. 64). Studien vil således få frem nyanserte data og være åpen for kontekstuelle forhold.

Tilnærmingen til studien vil være pragmatisk og deduktiv. (Jacobsen, 2015, s. 35). I dette legges at studien vil ta utgangspunkt i gjeldende teori på området, for deretter gjennom forskningsspørsmålene og analysen å bygge empiri innen området for Forsvaret.



Figur 3 Forskjeller mellom en deduktiv, en induktiv og en abduktiv tilnærming (Jacobsen, 2015, s. 35)

2.2 Andre fase - Valg av undersøkelsesdesign

Ved valg av undersøkelsesdesign må en blant annet ta stilling til hva slags problemstilling som skal besvares. Jacobsen peker på skille mellom beskrivende eller korrasjonelt design og kausalt design (årsakssammenheng) (Jacobsen, 2015, s. 64).

I denne studien søker forskeren å gå i dybden på konsekvensene av økt informasjonsdeling for å beskrive situasjonen. For å få identifisert implikasjonene dette gir har forskeren brukt en metodikk som gir nyanserte data gjennom et intensivt design. Intensive design går i dybden på en hendelse eller et fenomen men med få enheter. En slik studie vil gi høy intern gyldighet da en får belyst mange variabler, men i mindre grad være generaliserbar da det er en eller få enheter som undersøkes (Jacobsen, 2015, s. 90-91). Denne Studien vil betegnes som intensive ved at det vil være en lite utvalg.

Ved et studie der en søker å få svar på hva som har skjedd, eller hvorfor noe har skjedd mener Yin at et casestudie er det best egnede (Yin, 2012, s. 5). Videre anbefales en casestudie når en skal undersøke en hendelse av noe i dybden (Oates, 2006, s. 141).

Caset som studeres i denne studien er selve informasjonsflyten mellom Forsvaret som kunde og de som leverer varer og tjenester som leverandører. Ved å benytte en casestudie søker forskeren

å få svar på hva hvilke konsekvenser en økt informasjonsflyt vil ha sett i lys av informasjonssikkerhet og forvaltningen av understøttelsessystemet.

2.3 Tredje fase - Valg av metode – kvalitativ eller kvantitativ

Ved valg mellom kvalitativ og kvantitativ metode tas en vurdering av hvilken datatype forsker er ute etter. *"Kvalitative og kvantitative data er like gode, men egner seg til å belyse ulike spørsmål og problemstillinger"* (Jacobsen, 2015, s. 125). Der kvantitative data primært omhandler tall og størrelser vil kvalitative data i større grad omhandle språk, handlinger og meninger (Dey, 1993, s. 10-11). Jacobsen påpeker at metodene ikke er motsetninger men snarere ytterpunktene på en skala.

Figur 4 Kvalitativ og kvantitativ metode som ytterpunkter (Jacobsen, 2015, s. 127)

Denne studien vil benytte kvalitativ metode da denne gir større fleksibilitet og passer godt til den utledede problemstillingen. Fordelen med en kvalitativ metode er at den i motsetning til kvantitativ metode møter respondentene på deres premisser og ikke forskerens. Dette gir en nærhet til respondenten som åpner for nyanser og oppfatninger som ellers ville blitt borte. Dette gir liten grad av kontroll på de data forsker får samlet inn, da det er respondenten som med egne ord formidler sin forståelse av det det ønskes forsket på. En vil dermed oppnå høy relevans og få frem den "riktige" forståelsen av et fenomen (Jacobsen, 2015, s. 129). En annen fordel med at respondenten gis mulighet til å formidle sin virkelighetsoppfatning er den nyanserikdommen det fører med seg. Respondentens bruk av egne ord og formuleringer gir økt mulighet for variasjon og kompleksitet. Dette medfører at det forsker i utgangspunktet mente var kjernen i problemstillingen kanskje ikke var det allikevel. Ved å bruke kvalitativ metode vil jeg da kunne justere problemstillingen, undersøkelsesopplegget, analyse og datainnsamlingsmetode underveis i studien gjennom en interaktiv prosess.

En av ulempene ved kvalitativ metode er at intervjuer tar lang tid og er meget ressurskrevende. Ved utvalg vil jeg derfor i denne studien prioritere nyanser og dybde fremfor mange enheter (Jacobsen, 2015, s. 131). Få enheter vil gi en fare for at studien ikke gir et representativt bilde,

men snarere et bilde av noen enkeltrespondenters oppfatning. Studien vil også kunne få et generaliseringsproblem og den eksterne gyldigheten vil være fraværende eller svak. Intervjuene vil gi en stor mengde ustrukturerte ord som ofte vil kunne være svært komplekse. Når forsker så skal strukturere informasjonen er det en fare for at oversikten mistes. Min virkelighetsoppfatning vil også kunne være preget av en subjektiv realisme og derigjennom påvirkes av min kunnskap og tidligere erfaringer. Forsker må søke å være objektiv og bevisst at det ikke nødvendigvis er samsvar mellom egen og respondentens virkelighetsoppfatning (Oates, 2006, s. 178).

Problemstillingen søker å gå i dybden på et fenomen ved å være eksplorerende og beskrivende. Det søkes å få frem nyanser ved informasjonsdeling, noe som ikke i samme grad er mulig ved en kvantitativ studie. En kvalitativ studie anbefales der en ikke har tilstrekkelig med kunnskap eller informasjon om det som søkes forsket på (Jacobsen, 2015, s. 133). Denne studien bruker fortolkende forskning da den ikke søker å bevise eller motbevise en hypotese men forsøker heller å identifisere, utforske og forklare hvordan faktorene i en bestemt setting henger sammen (Oates, 2006, s. 143).

2.4 Fjerde fase - Innsamling av kvalitative data

For å kunne formulere en god problemstilling er en solid kjennskap til teori og tidligere forskning helt nødvendig (Ringdal, 2013, s. 63). Ringdal fremhever også viktigheten av at tidligere studier og forskning kommer tydelig frem i skrivefasen. Dette for å kunne avdekke eventuelle svakheter eller mangler i tidligere forskning og derigjennom bygge ytterligere empiri.

Fremgangsmåten som anbefales er å starte med egen samling av bøker, rapporter og tidsskrifter for deretter å benytte bibliotekets databaser. Ringdal har følgende generelle råd til fremgangsmåte:

- Begynn på toppen av informasjonspyramiden.
- Søk etter oversiktsartikler.
- Finn nøkkelbegrepene på fagfeltet og bruk dem til systematiske søk.
- Finn de sentrale forskerne og forskningsmiljøene på feltet og søk etter arbeider fra disse.
- Se gjennom innholdsfortegnelsen for de siste årgangene av de mest relevante tidsskriftene. (Ringdal, 2013, s. 65)

For innhenting av sekundærdata ble biblioteket ved Forsvarets Høgskole (FHS) og Forsvarets arkivbase DocuLive brukt initialt. Søkemotoren i Oria, Nora, Google Scholar og Defence

Technical Information Center (DTIC) ble brukt til å søke på taksonomier innenfor fagområdet. Dette er informasjonsbaser som er anerkjent av forskermiljøer og innehar valid litteratur (Ringdal, 2013, s. 64). Det ble søkt med taksonomier på både norsk og engelsk. Innledningsvis ble det søkt generelt for å finne relevante dokumenter. Deretter ble søkene spisset ved å snevre inn perioden, da utviklingen innen IKT går fort. Det ble etter hvert også søkt direkte på forfatter for å se hvilke andre arbeider de har utgitt. Søkeord som ble brukt var prestasjonsbasert logistikk, supply chain management, ERP, informasjonsutveksling, Forsvaret, multilevel security, management, IT-styring, informasjonssikkerhet, IKT, sikkerhet, FFI og master. Søkeordene ble brukt alene og i kombinasjoner for å spisse treff. Dette som et ledd i å bygge kunnskap på forskningsområdet for å bearbeide forskningsspørsmålene. Ved funn av relevante studier ble litteraturlistene brukt som grunnlag for videre søk. Etter hvert som litteraturomfanget vokste ble en vurdering på hva som måtte forkastes ut fra relevans og tilgjengelig tid gjennomført. Det ble også skilt på empiri ved tidligere studier og litteratur på teori innen fagområdet. Videre ble det gjennomført en vurdering på om hensikten med empirien var i samsvar med det denne studien var på jakt etter, og en vurdering av kvaliteten på arbeidet. Det ble også gjort en vurdering på tidspunkt for gjennom føring av studiene, da IKT området utvikler seg raskt. Studier eldre enn 2010 ble normalt forkastet om de ikke var av generell karakter. Teorien ble blant annet vurdert opp mot i hvilken grad forfatter fremsto som anerkjent gjennom kryssreferanser og andre publikasjoner. En utfordring ved flere av funnene i DocuLive var at empirien var gradert eller unntatt offentlighet. Men referanselistene ble nyttet for finne relevant litteratur. Innsamling av primærdata til en kvalitativ undersøkelse vil ha innvirkning på studiens gyldighet. Det er derfor viktig at innsamlingsmetoden er egnet til å besvare forskningsspørsmålene. Jacobsen deler inn fire hovedkategorier for innsamling (Jacobsen, 2015, s. 145).

- Det individuelle, åpne intervjuet.
- Fokusgruppeintervju
- Observasjon
- Dokumentundersøkelse

Det individuelle åpne intervjuet er det mest vanlige innen kvalitativ metode, og også det som er nyttet i denne studien. Det er best egnet når det er relativt få enheter som skal undersøkes og en er interessert i den enkelte respondents oppfatninger. Ulempen er at selv om en intervjuer flere respondenter separat, vil en ikke kunne generalisere det opp til hva gruppen som sådan mener uten å komme i konflikt med gyldigheten i studien (Jacobsen, 2015, s. 147). Intervjuene ble gjennomført ansikt- til –ansikt da det gir best mulighet for å etablere god flyt i samtalen, samt gir

mulighet for å lese reaksjoner hos respondentene. Dette var reaksjoner som indikerte hva de brenner for, eller er mer usikre på. Enkeltspørsmål fra intervjuguiden er også gjennomført via telefon og mail mot faginstanser for å avklare fakta. Intervjuet kan struktureres med ulike grader av åpenhet fra det helt lukkede til helt åpent.

Figur 5 Grader av strukturering av et intervju (Jacobsen, 2015, s. 150)

Det ble i forkant av intervjuene utarbeidet en semistrukturert intervjuguide der det varierte mellom spørsmål med svaralternativer og helt åpne svar. Intervjuguidene ble kvalitetssikret uformelt mot en kollega som kjenner fagområdet, og deretter justert før selve datainnhentingen. Intervjuene ble gjennomført på respondentens kontor, eller et møterom på dennes arbeidsplass. Intervjuene ble tatt opp ved bruk av mobiltelefon, da det ga bedre gjengivelse enn tilgjengelig diktafon. Selve intervjuene varte i 1-1,5 timer og ble transkribert i etterkant.

2.5 Femte fase - Utvalg av enheter

Kvalitative undersøkelser er tidkrevende og kostbare. Dette medfører at en ikke kan få intervjuet alle de respondenter en måtte ønske, men det må foretas en prioritering og et utvalg (Jacobsen, 2015, s. 177). Det vil derfor alltid være en fare for at de respondentene en velger ut ikke er representative og derigjennom kan få feilaktige resultater. Respondentene til denne studien ble funnet gjennom først å avdekke hvilke avdelinger i Forsvaret som jobber innenfor tematikken. Som et ledd i å få flest mulig nyanser på bordet ble det valgt respondenter både fra teknisk side ved systemstyring og DVU, samt fra prosjekt og "brukersiden". Dette for å få belyst implikasjoner ved informasjonsdeling fra flere vinkler og ståsteder. Deretter ble snøballmetoden brukt for å identifisere den aktuelle respondent. Dette ble gjort gjennom samtale med kollegaer som jobbet i aktuell avdeling, og kunne rute forsker til kandidater som hadde inngående kjennskap til problemstillingen. Forsker var oppmerksom på ulempene ved snøballmetoden og søkte å kompensere ved å innhente forslag fra flere personer i aktuell avdeling. Videre ble ikke alle intervjuer avtalt i starten av intervjufasen for å gi rom for justeringer underveis. Respondentene (direkte kjennskap) og informantene (indirekte kjennskap) (Jacobsen, 2015, s.

178) er blitt anonymisert og samtlige er forelagt samtykkeerklæring for deltagelse (vedlegg B). De er der også gjort oppmerksom på at deltagelsen er frivillig, og at alle data samlet inn under arbeidet ville bli slettet ved studiens slutt. Det fremkommer også av samtykkeerklæringen at studien er meldt inn og godkjent av Norsk Samfunnsvitenskapelig Datatjeneste (NSD) ved prosjekt nr. 46088.

Empirien består av dybdeintervju med respondenter som har en rolle inn mot tilrettelegging for utveksling av informasjon, er ansvarlig for rammefaktorene for informasjonsutvekslingen, samt brukere av Forsvarets systemer der samhandling med sivile inngår i stillingen. Respondent 1 (R1) kommer fra CTO/systemstyring. Avdelingen er det sentrale drift og styringssenteret med ansvar for blant annet Forsvarets Sikre Plattformer (FSP) og nettverksinfrastruktur. Respondent 2 (R2) kommer fra CTO/Drift og videreutviklings avdeling (DVU). Avdelingen har blant annet ansvaret for innføringen av ERP systemet SAP i Forsvaret, samt drift og forvaltning av dagens FIF løsning. Av underlagte avdelinger av betydning for denne studien Logistikk, plattformforvaltning og applikasjonsforvaltning. Respondent 3 (R3) kommer fra Operasjonsstøtte avdelingen til Hæren ved Østerdalen Landverksted. Avdelingen er ansvarlig for planlegging og gjennomføring av vedlikehold av kjøretøy. De representerer bruker av informasjonssystemet ved samhandling mot eksterne verksteder. Respondent 4 (R4) kommer fra FMA/Landkapasiteter ved prosjektavdelingen. Avdelingen er blant annet ansvarlig for anskaffelse av reservedeler, verktøy og teknisk dokumentasjon til kampvognprosjektet. Avdelingen er også ansvarlig for å få inn data fra leverandørene, og inn til logistikkprosjektet for vognene. Respondent5 (R5) kommer fra FLO/stab/økonomistyring/driftsanskaffelser. Avdelingen er merkantil saksbehandler ved anskaffelser til forsvaret, og har blant annet ansvar for å sikre kodifisering på deler av materiellporteføljen. Respondent 6 (R6) er fra FMA/luftkapasiteter ved prosjektavdeling nye kampfly F35. Avdelingen er blant annet ansvarlig for anskaffelsen av Autonomic Logistics Information System (ALIS) og ivaretakelse av informasjonsutveksling og integrering av denne. Respondent 7 (R7) kommer fra DVU/logistikk. Avdelingen er ansvarlig for ivaretakelse av SAP applikasjoner, herunder logistikkprosjektet og implementeringen av materielldata. NSM var plukket ut som respondent 8 (R8) for å få belyst de sikkerhetsmessige aspektene ved studien, men jeg har ikke lykkes i å få til et intervju.

Avdeling	Respondent	Tidspunkt	Merknader
CYFOR/CTO/Systemstyring	R1	2016-03-04	Kolsås på kontoret
CYFOR/CTO/DVU	R2	2016-03-05	Langkaia på kontoret
Hæren/OPSSTØ/ØLV/Plan & Drift	R3	2016-03-14	Rena på møterom
FMA/Landkap/prosjektavd P5444 Kampvogn	R4	2016-03-17	Kolsås på møterom
FLO/Stab/ØS/DA/Innkjøp felles	R5	2016-04-01	Kjeller på kontoret
FMA/Luftkap/prosjekt avd nye-kampfly progsj-matr plattform	R6	2016-04-01	Kjeller på møterom
CYFOR/CTO/DVU/Logistikk	R7	2016-04-04	Oslo/Havnelageret på møterom
NSM	R8	-	Ikke gjennomført

Tabell 1 Respondenter innsamling av primærdata

2.6 Sjette fase - Hvordan analysere data

Etter ferdig transkribering av intervjuene vil forskeren sitte med en anselig mengde ustrukturert informasjon. For å finne essensen i datamaterialet vil forskeren derfor gjennomføre en strukturering og sammenstilling av informasjonen slik at den blir håndterbar. Studien har benyttet Jacobsens fire faser i prosessen med å finne kjernen i informasjonsmengden. Disse fasene var dokumentere, utforske systematisere og kategorisere, og sist sammenbinde (Jacobsen, 2015, s. 199). Intervjuene ble transkribert med struktur fra intervjuguide, deretter så jeg gjennom etter trekk som gjentok seg, eller som var felles fra flere respondenter. Tekstene ble deretter systematisert etter de enkelte faktorer og sentrale momenter ble markert, før forskeren søkte å dra sammen essensen innen de enkelte spørsmålsområdene.

2.7 Syvende fase - Kvalitet på resultater

For at studien skal være en studie og ikke bare en fortelling, må den tilfredsstille kravene til reliabilitet eller pålitelighet og validitet eller gyldighet. Påliteligheten går på at om en annen forsker gjennomfører samme studie, skal denne forskeren komme frem til de samme resultater. Gyldigheten på sin side sier noe om en faktisk måler det en ønsker å måle (Jacobsen, 2015; Ringdal, 2013, s. 96). Dette støttes oppunder av Jacobsen som fremhever en pragmatisk

tilnærming der en stiller seg spørsmålet ved *"...hvorvidt det er samsvar mellom virkeligheten og forskerens beskrivelse av denne virkeligheten*." (Jacobsen, 2015, s. 228). Jacobsen (2015) påpeker også at det inne forskningsmiljøene er ulikt syn på begrepene pålitelighet og gyldighet og viser til Thagaard (1998).

I denne studien har forskeren søkt å skaffe de riktige kildene for intervju ved å forhøre seg med flere kollegaer som jobber innenfor fagfeltet. Gjennom å få flere innspill på aktuelle avdelinger og personer som har nøkkelkompetanse innen emnet, har jeg søkt å få de riktige respondentene i tale. Som et ledd i å sikre en god gyldighet i studien, har jeg ved utvalg av respondentene forsøkt å få personer med førstehånds kjennskap til forskningsspørsmålene, og fortrinnsvis med så lang erfaring som mulig. Konteksten datainnsamlingen ble foretatt i ble gjennomført så skjermet og avslappet som mulig, for å sikre at respondenten følte seg så fri som mulig. Intervjuene ble gjennomført på møterom eller vedkommendes kontor for å få til denne riktige atmosfæren. Det ble også gjennomført intervju med personer fra forskjellige funksjoner for å få en mer "gyldig" beskrivelse av situasjonen. For å sikre nøyaktige data, ble samtalen tatt opp med mobil og transkribert. Forsker la også inn egne notater der det var av interesse for problemstillingen for å sikre at momenter ikke falt ut. Deretter ble teksten analysert og kategorisert etter emner for lettere å kunne se mønstre. Påliteligheten i studien er søkt ivaretatt ved å i stor grad referere til hvor informasjon er hentet fra. Videre er det prøvd å tydelig få frem hvilke avdelinger og vurderinger som er lagt til grunn for analysen.

En styrke ved kvalitative studier er muligheten for å avdekke spesielle forutsetninger for at noe skal ha en effekt (Jacobsen, 2015, s. 237). Svakheten er at en bare studerer ett, eller noen få enheter, og derigjennom ikke har belegg for å generalisere funnene for en større populasjon (Jacobsen, 2015, s. 237). Denne studien ser på hva som påvirker- og konsekvenser av informasjonsdeling mellom graderingsnivåer. Studien vil således kunne ha en viss overførbarhet til andre institusjoner som politi, helsevesen og andre som også opererer med skjermingsverdig informasjon i lovens forstand. Men det største bidraget vil være økt kunnskap i egen organisasjon om hvilke konsekvenser en dreining mot økt sivilisering av logistikken vil kunne ha.

2.8 Åttende fase - Tolkning av resultater

Gjennom hele studien har forskeren forholdt seg til den nasjonale forskningsetiske komité for samfunnsvitenskapelig humanioras (NESH) retningslinjer for hvordan en studie skal gjennomføres. Av de generelle retningslinjene kan de viktigste oppsummeres i krav om: Sannhetsbestrebelse, kvalitet, frivillighet, konfidensialitet, habilitet, redelighet, tilgjengeliggjøring av resultater og god henvisningsskikk (De nasjonale forskningsetiske komiteene, 2016). Prinsippene om respekt for personer som deltar i forskningen, gode konsekvenser og akseptable uheldige konsekvenser, samt krav til integritet og rettferdighet har ligget i bakhodet gjennom hele prosessen hos forskeren (De nasjonale forskningsetiske komiteene, 2016).

Forsker forholdt seg objektiv til innsamlet informasjon, men erkjenner at egne erfaringer og kompetanse vil kunne påvirke vurderingene som er gjort. Ved tvil om hva respondenten har ment er denne kontaktet for utdypende kommentarer. Det er gjennom utøvelsen av studien søkt å være bevisst kravene til pålitelighet, begrepsmessig gyldighet (har vi fått svar på det vi ønsker å få svar på), og intern- og ekstern gyldighet. Forsker har for de enkelte faser gått tilbake til utgangspunktet for å sikre at kravene har vært valide.

3 Litteraturstudie/teoretisk forankring

For å bedre se hva som fører til behov for økt informasjonsdeling mot sivile aktører vil det i denne delen sees på litteratur inn mot problemstillingen i Forsvaret. Det vil også sees på det teoretiske bakteppet for utviklingen. Det er viktig å kjenne til hva som er av empiri på området i Forsvaret fra tidligere for å kunne bygge videre på det, samt hva teorien sier om prinsippene for hva som fører til gode løsninger innenfor tematikken.

3.1 Litteratur inn mot problemstillingen i Forsvaret

Det er begrenset med litteratur som omhandler informasjonsdeling og konsekvensene av dette i en militær setting i Norge som er allment tilgjengelig. Av litteratur som berører området har det vært en utfordring å holde denne studien på et ugradert nivå. Dette skyldes at mye av den mest sentrale litteratur jeg har funnet på området i en forsvarskontekst har enten vært *unntatt offentlighet*, BEGRENSET, begge deler, eller ikke publisert per skrivende stund. Disse studiene er brukt som bakteppe ved gjennomføring av studien, men det er søkt å finne andre åpne kilder for å muliggjøre etterprøvbarhet. Av litteratur som berører problemstillingen trekkes noen av de viktigste åpne arbeidene frem i det følgende.

Det ble vinteren 2015 skrevet to masteroppgaver ved Forsvarets høgskole (FHS) av henholdsvis Gunn Elisabeth Håbjørg (2015) og Mona Elise Aar (2015). Den ene ser på prestasjonsbasert logistikk i Forsvaret og hvilke faktorer som fremmer eller hemmer denne typen kontrakter (Håbjørg, 2015). Håbjørg (2015) tar for seg en case studie der hun ser på erfaringer med PBL fra C-130 Hercules transportfly og vedlikehold av F100 motor til F16 kampfly. Studien er relevant for denne oppgaven da den konkluderer med at informasjonsdeling er ett av forholdene som fremmer bruken av PBL avtaler i norsk militær kontekst.

Den andre masteroppgaven omhandler PBL avtaler i et kunde-leverandør samarbeid og er også en casestudie av C-130 Hercules transportfly (Aar, 2015). Aar (2015) ser på samarbeidet mellom kunde (Forsvaret) og leverandør og hvordan dette utøves. Studien er relevant for denne oppgaven da den tar opp både sikkerhet- og informasjonsmessige utfordringer ved PBL samarbeid.

En annen master fra FHS som berører temaet i denne oppgaven er Atle Instanes sin fra 2013 (Instanes, 2013). Instanes (2013) undersøker i sin studie hvilken påvirkning utformingen av forsyningskjeden har opp mot beredskap, og hvilke utfordringer som ligger i dagen beredskapslogistikk. Han trekker frem at

> *… logistikkløsningen for Nansen kl. fregatter på noen områder kan sammenlignes med en forsyningskjede i et SCM perspektiv, men lav integrasjonsgrad i IKT- løsningen, begrenset fokus på forsyningskjedens risiko, risikoledelse, samt forsyningskjedens utstrekning, underbygger at Forsvarets ledelse i forsyningskjeden ikke kan betraktes SCM* (Instanes, 2013, s. 80).

Studien er relevant for denne oppgaven da Instanes (2013) belyser utfordringer innen beredskap og IKT-løsninger i forsyningskjeden. Det at oppgaven tar for seg en case studie mot Fregattene gir også en større bredde da begge de andre studiene angår luftforsvaret.

Innenfor ERP er studiene til Frøyland (2015), Melbo (2006) og Finnanger (2012) brukt som grunnlag. Disse omhandler IT-styring, suksesskriterier og innføring av ERP løsninger. Studiene er relevante da alle tre tar opp aspekter ved informasjonsdeling og integrasjon, der Frøyland og Finnanger ser på SAP løsningen i Forsvaret, mens Melbo ser på offentlig sektor generelt (Finnanger, 2012b; Frøyland, 2015; Melbo, 2006).

Forsyningskjeden er tema i studien til Strandskog (2015) om informasjonsdeling mellom kjøper og leverandør. Studien ser ikke på Forsvaret spesifikt, men tar for seg forutsetninger for informasjonsdeling og integrasjon mellom aktørene (Strandskog, 2015).

Av viktigste graderte, ikke publiserte, eller unntatt offentlighet, studiene som er brukt i studien er ”*Rammevilkår for fremtidig logistikk, bruk av ytelsesbaserte kontrakter (PBL) i Forsvaret – muligheter og konsekvenser*” (Forsvaret, 2015b). Den studien er *Vedlegg U4* til grunnlagsutredning for FMR. Studien er i sin helhet FORTROLIG, så forskeren har måttet vurdere å avklare vedrørende henvisinger til den. Studien er relevant da den tar opp problemstillinger rundt ytelsesbasert logistikk, risiko og informasjonssikkerhet (Forsvaret, 2015b).

En ikke publisert (per 2016-02-11) FFI rapport om ”Forsvarets forsyningsberedskap og avhengighet av sivile aktører” (Birkemo & Kuran, 2015) omhandler deler av kjernen i forskningsspørsmålet. Rapporten belyser blant annet problemstillinger rundt informasjonsdeling og sikkerhet**.** Rapporten er i sin helhet gradert BEGRENSET, så forskeren har måttet vurdere og avklare vedrørende henvisninger til denne.

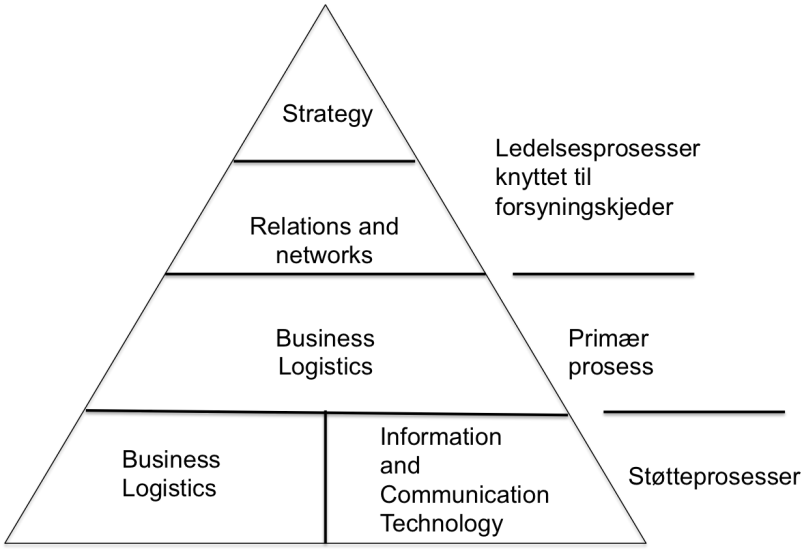
Det ble i forbindelse med anskaffelsen av F35 kampfly gjennomført en studie på *”Joint Strike Fighter International Information Interoperability Initiative”* (JSF4I) som treffer mye av kjernen i denne studien, men den er unntatt offentlighet (Forsvaret, 2008).

Prosjekt 8154 Fleksible løsninger for sikker informasjonsutveksling har utarbeidet et konseptuelt grunnlag. Denne inneholder blant annet beskrivelse av dagens situasjon, aktører innenfor domenet og oversikter på informasjonsdeling. Grunnlaget er gradert, men gir en god oversikt på Forsvarets informasjonsutveksling (Forsvaret, 2016).

3.2 Supply Chain Management (SCM) og forsyningskjeder

SCM har sitt utspring i mulighetene for å kutte kostnader og oppnå konkurransefortrinn. Tradisjonelt sett har kommunikasjonen mellom kunde og leverandør ved et kjøp foregått ved bruk av ordre. Disse ordrene kommer som følge av ferdig prosessert data om behov fra kunden, og skjuler således den faktiske etterspørselen i markedet (Li, Sikora, Shaw, & Tan, 2006, s. 254). Dette vil da kunne føre til den såkalte bullwhip-effekten der små endringer i etterspørselen nedstrøms (kunde) vil akkumuleres oppover i forsyningskjeden og kunne gi store utslag hos leverandørene (Li et al., 2006, s. 254). Ut fra dette kan en trekke konklusjonen om at ”*For at en bedrift skal kunne koordinere verdikjeden sin må de nødvendigvis ha kunnskap om partnerens aktiviteter”* (Strandskog, 2015, s. 4). Gjennom å knytte kunden nærmere til seg gjennom for eksempel integrerte IKT løsninger, sikrer leverandørene seg tidsriktig informasjon og kunnskap om hva kundens behov er. På den måten får de en redusert Bullwip-effekt og kan optimalisere sin produksjon, lager og distribusjon, noe som gir reduserte kostnader og bedret konkuranseevne. Kunden på sin side sitter igjen med bedret tilgang på etterspurt vare til en lavere pris. En slik form for informasjonsintegrering har blant forskere blitt sett på som en kritisk komponent og et suksesskriterium for effektiv SCM (Kulp et al., 2004, s. 431; Mentzer et al., 2001, s. 8; Mohr & Spekman, 1994, s. 139; Porterfield, 2008, s. 42). Et særtrekk ved en militær forsyningskjede er at

kravet om informasjonssikkerhet vil påvirker flyten av informasjon mellom Forsvaret og eksterne aktører. En vil derfor kunne få en dårligere informasjonsflyt. Dette i kombinasjon med stor grad av materiell som skal på vedlikehold eller reparasjon, medfører at det i en militær forsyningskjede er en økt sannsynlighet for-, og en kan risikere en dobbel Bullwip-effekt (Nilsen & Steder, 2010, s. 13). Som det visualiseres i figuren under over ledelse av integrerte forsyningskjeder, ligger informasjonsdeling og kommunikasjonsteknologi som en støtteprosess i bunn av pyramiden. En ser derav at dersom denne ikke er tilstede, vil en heller ikke kunne nå neste nivå.



Figur 6 Ledelse av integrerte forsyningskjeder (Persson & Grønland, 2002, s. 15)

En kan si at gjensidig informasjonsdeling kan sees på som en forutsetning for å kunne få en effektiv SCM. Dette gjelder spesielt for overvåking av de enkelte prosesser i forsyningskjeden, så vel som planlegging (Mentzer et al., 2001, s. 8).

Ut fra den beskrevne teori om SCM og forsyningskjeder er kravet om informasjonsdeling og integrasjon sentrale faktorer som går igjen for å sikre ønsket effekt for virksomheten. Studien vil derfor bruke faktorene *informasjonsdeling* og *integrasjon* i analyse og drøfting i kapittel 7.

3.3 Performance Based Logistics (PBL)

Med stadig mer teknologisk avansert og komplekse våpensystemer og våpenplattformer er det rimelig å anta at det vil bli økt bruk av PBL kontrakter også i Forsvaret i tiden fremover (Lien & Strand, 2011, s. 48). Innføring av nye Fregatter, NH90 Helikopter, F35 kampfly og nye

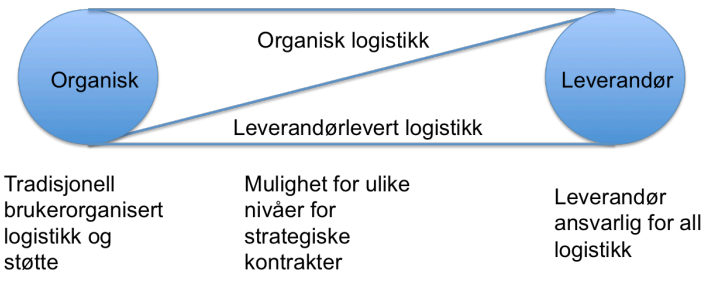
kampvogner er noen eksempler på systemer og kapasiteter der PBL står sentralt ved forvaltningen av systemet.

Det er mye litteratur om PBL innenfor den sivile sektor, men når det kommer til litteratur på området innen Forsvaret i Norge er det mindre dokumentasjon å hente. Det har dog de siste årene vært et økende fokus på området i Forsvaret. Det ble i 2015 levert to masteroppgaver på PBL ved FHS og det er i 2016 flere som skriver om emnet i en militær kontekst. Det er også utarbeidet flere studier ved FFI som en del av Logistikk og Støtte 2020 (LOGOS) prosjektet som berører emnet (Gulichsen, Reitan, & Listou, 2011; Lien & Strand, 2011).

PBL også omtalt som ytelsesbasert logistikk, har historisk sett sitt utspring i det amerikanske forsvaret. Som følge av reduserte budsjetter etter den kalde krigens slutt var det ett behov for å tenke på en ny måte. Secretary of Defense fikk i 1998 følgende oppdrag gjennom National Defense Autorization Act seksjon 912 (c).

> *Reengineer the product support process to use best commercial practices (BCPs), competitively source product support, modernize through spares, establish program manager oversight of life cycle support (PMOLCS) and greatly expand Prime Vendor (PV) and Virtual Prime Vendor (VPM) programs (Vitasek & Geary, 2008, s. 11).*

Hovedprinsippene i dette oppdraget er det vi i dag kjenner som PBL. I dag er PBL en stor og integrert del av det amerikanske forsvaret, og siden 2001 har det også vært den foretrukne forsyningsstrategien (Assistant Secretary of Defense Logistics & materiel readiness, 2016, s. 10). Innføring av PBL medfører en endring i filosofien fra en *"oss og dem"* tankegang til en mer *"vi"* filosofi (Vitasek & Geary, 2008, s. 14). Grunnprinsippet innen PBL er at en inngår ett langsiktig samarbeid med leverandøren der denne så påtar seg ansvaret for leveranse av en tilgjengelighet, ytelse og eller tjeneste som eksempelvis en gitt tilgjengelighet på kampfly eller ett våpensystem. En betaler med andre ord ikke for en artikkel som tidligere, men for tilgjengeligheten (Assistant Secretary of Defense Logistics & materiel readiness, 2016, s. 11).



Figur 7 Illustrasjon skalaen mellom tradisjonell transaksjonsbasert logistikk og ytelsesbasert logistikk (Forsvaret, 2015b, s. 5)

Ved ytelsesbaserte kontrakter, til forskjell fra transaksjonsbaserte, så vil utbetalingen til leverandør være knyttet opp mot dennes evne til å holde en gitt definert status (Forsvaret, 2015b, s. 5). Det være seg for eksempel tilgang på et gitt antall tilgjengelige flytimer for kontraktsperioden. Hovedpoenget med å inngå denne typen langsiktige kontrakter er bedre operativ evne gjennom bedret tilgjengelighet til en lavere kostnad. Dette skal oppnås som følge av samvirket mellom kunde og leverandør der en omgjør målbare ytelser til målbare kundekrav som reguleres i kontrakten. En vil så gjennom incentiver motivere leverandør til å holde avtalt kvalitet eller bedre gjennom kontraktsperioden. Dette kan være incentiver som tilbakehold av betaling dersom leveranse ikke er i samsvar med kontrakt, samt en form for bonus dersom det leveres utover det som er avtalt (United States Government Accoutability Office, 2008, s. 10). Kontraktene kan være av varierende omfang, men en studie på bruk av ytelsesbaserte kontrakter innen den sivile luftfartsindustrien konkluderer med at de beste resultatene oppnås ved å inngå avtaler på komponent nivå. Eksempler på dette kan vær en flymotor, ett skrog eller avionikk (Lund, 2014; United States Government Accoutability Office, 2008).

For at PBL kontrakter skal gi ønsket effekt påpekes det flere forhold eller faktorer som spiller inn. Dette er faktorer som enten kan fremme eller hemme effekten av inngåtte kontrakter. Håbjørg (2015) viser i sin studie til at PBL er i endring og at faktorene som fremmer eller hemmer ikke bare er i endring, men også varierer mellom de enkelte nasjoner (Storbritannia, USA og Tyskland). Videre påpekes det at faktorer som på ett tidspunkt ansees som en hemmer senere kan endre seg til å bli en fremmer og visa versa. Hun trekker også frem at flere undersøkelser viser til kompetanse og kunnskap som en type faktor som initialt er til hinder, men etter hvert som organisasjonen blir mer moden går over til å bli en faktor som fremmer PBL (Håbjørg, 2015, s. 43).

Håbjørg (2015) har i sin studie av faktorer som fremmer eller hemmer PBL kontrakter i en Norsk kontekst kommet frem til følgende forhold. Av faktorer som fremmer trekkes forbedret leveranse, informasjonsdeling og tillitsrelasjoner frem. Av faktorer som bare hemmer er manglende vektlegging av Supply Chain Management (SCM) den eneste. Derimot er det noen faktorer som kan hemme eller fremme avhengig av hvilken kontekst en ser faktoren i. Disse faktorene er økonomi, beredskap, kompetanse, systemkompleksitet, strategi og lover og regler (Håbjørg, 2015, s. 45).

Der PBL setter ut hele eller deler av en tjeneste har en i transaksjonsbasert logistikk en mer tradisjonell forsyningskjede. For å få en økt effektivitet innenfor den transaksjonsbaserte logistikken har en derfor gått i retning av en mer integrert prosess der også. For å få til en slik integrering må en ha en styring av forsyningskjeden omtalt som SCM. Det er mange likhetstrekk mellom PBL og SCM og mange setter likhetstegn mellom de to, eller at den ene har erstattet den andre. Geary og Vitasek (2008, s. 14) hevder at *"PBL is a fundamental business model paradigm shift in how the government and the contractor do business."*.

Ut fra den beskrevne teori om PBL er kravet om informasjonsdeling og integrasjon sentrale faktorer som går igjen for å sikre ønsket effekt for virksomheten. Denne studien vil derfor bruke faktorene *informasjonsdeling* og *integrasjon* i analyse og drøfting i kapittel 7.

3.4 Enterprise Resource Planning (ERP)

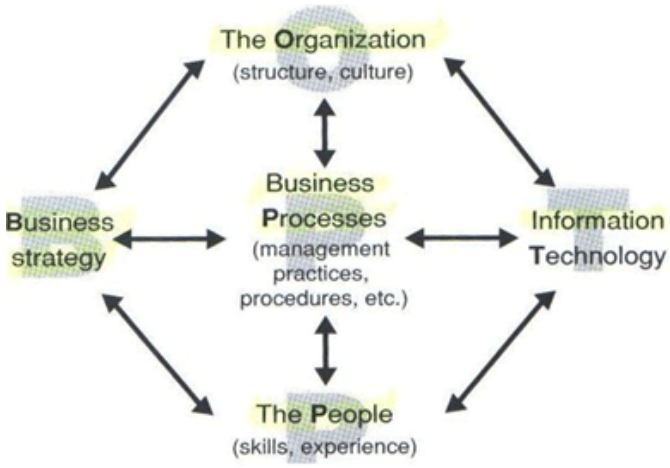
Forsvaret har i dag en felles integrert forvaltningsplattform (FIF) som har et Enterprise Resource Planning (ERP) system som er basert på softwaren til firmaet *Systems, Applications, and Products in Data Processing* i dagligtale omtalt som SAP. Et ERP system er i det grunnleggende en administrativ programvare som har til hensikt å "*integrere transaksjonsdata og forretningsprosesser i hele organisasjonene til ett informasjonssystem."* (Frøyland, 2015, s. 12). Integrasjon vil i den sammenheng si at systemet integrerer virksomhetens informasjonsflyt teknisk sett, slik at den blir tilgjengeliggjort for de prosesser som har behov for den i sann tid. For å få til dette må systemet konfigureres til å understøtte de valgte forretningsprinsipper innen de implementerte ERP modulene. Dette kan være moduler som typisk styrer informasjonsflyten innen personell, materiell, økonomi og styring og ledelse (Melbo, 2006, s. 10). ERP systemer er en pakkeløsning der "best practices" innen forretningsområdene legges til grunn fra systemleverandøren. Det betyr i praksis at systemet er standardisert og bedriften må tilpasse seg applikasjonens forretningsprosesser. Det innebærer også at kunden knytter seg veldig sterkt til leverandøren av systemet noe gir økt sårbarhet og redusert forhandlingskraft (Melbo, 2006, s. 10). Det at prosessene er basert på nøye utvalg fra organisasjoner og industrier som representerer målgruppen for systemet, medfører at det er vesentlig at softwaren er oppdatert med de nyeste alternativene (Melbo, 2006, s. 10). Men selv om de generiske prosessene baseres på det som ansees som best, vil det kunne være fristende å gjøre tilpasninger til egen organisasjon. Dette

anbefales dog ikke da endringer i ERP systemet innebærer stor risiko og høye kostnader (Melbo, 2006, s. 10).

Innen offentlig forvaltning påpeker Krokan (2010) at det er et stort mangfold av systemer som ikke nødvendigvis henger sammen eller kan utveksle datainformasjon seg imellom. Dette gjør at det innen offentlig forvaltning er *"...umulig å utføre arbeidsoppgaver på betryggende og effektive måter..."*(Krokan, 2010, s. 259). Denne fragmenterte systemarkitekturen med silotenking[6], der de enkelte systemer i sin tid er anskaffet for å dekke de enkelte forretningsområdene uten å se helheten i virksomheten, påpekes også som en utfordring internt i Forsvaret (Frøyland, 2015, s. 12-13). Forsvarets IKT-strategi sier at *"...det skal etableres enhetlige og gjennomgående prosesser som raskt omformer ressurser til tjenester med merverdi for Forsvaret"* (Forsvarssjefen, 2013, s. 5) Som ett tiltak for å nå det strategiske målet må en ha en god forståelse for hvilke og hvordan prosessene i organisasjonen er.

Prosessene gir en beskrivelse av aktiviteter som i kombinasjons med en ressursinnsats skal gi en merverdi til organisasjonen. Iden (2013) viser til Willoch som har definert en prosess til å være *"En arbeidsprosess er et sett med sammenhengende aktiviteter som skaper kundeoppfattet verdi"* (Iden, 2013, s. 37). For å kunne se gangen i prosessene, må en også vite hvordan informasjonsflyten i organisasjonen er. En må forstå hvordan virksomhetsprosessene er og ha oversikt over hva som er primær-, støtte- og ledelsesprosesser. Dernest må man ha kunnskap om hvordan teknologien kan understøtte informasjonsdelingen av data (Frøyland, 2015, s. 22). Av det kan en trekke ut at uten en velfungerende informasjonsdeling i organisasjonen vil en ikke få ut gevinsten av virksomhetens ERP system. Ved analysen av virksomhetens prosesser er det viktig å gjøre en grundig kartlegging av hele organisasjonen. Aalders visuelle fremstilling viser hvordan de enkelte forretningsområdene er gjensidig avhengige av hverandre.

[6] Silobasert vil si at arkitekturen består av enkeltstående applikasjoner som har hver sin arkitektur og oppbygging (Lange, 2012, s. 8)



Figur 8 BTOPP: Business, Technology, Organization, Process, People (Aalders & Hind, 2002, s. 4)

Ved å ha perspektiv på at IT ikke bare er en frittstående del, men snarere en premissgiver for flyten i forretningsprosessene som må tas med i vurderinger av hvordan en opererer, vil en ha bedre forutsetninger for å få en gevinst ved et ERP system. Dette gjøres gjennom å ha en god IT-styring der det utøves kontrollhandlinger for å sikre tilfredsstillende datakvalitet. Det er mange kritiske suksessfaktorer for at et ERP system skal være vellykket. Melbo (2006) har i sin studie om suksesskriterier for ERP systemer i offentlig sektor kommet frem til kriteriene i tabellen nedenfor.

Forankring i toppledelsen
Effektiv prosjektledelse
Styringskomité
Valg av ERP-løsning
Prosjektforkjemper
Ressursallokering
BPR
Datakvalitet
Implementeringsstrategi
IT infrastruktur
Kompetanse i prosjektteam
Endringsledelse
Klare mål
Opplæring og kursing
Brukerinvolvering
Bruk av konsulenttjenester
Parametersetting
Feilsøking og testing
Minimum av skreddersøm
Effektiv kommunikasjon
Organisasjonskultur

Tabell 2 Kritiske suksessfaktorer for ERP systemer (Melbo, 2006, s. 75)

For denne studien er de mest relevante kriteriene:

Datakvalitet: Det er vesentlig at datakvaliteten holder tilfredsstillende nivå for at informasjonsdelingen skal kunne finne sted. De enkelte modulene i ERP systemet er tett integrert i hverandre, så dårlig datakvalitet vil kunne stoppe prosessen, eller produsere unøyaktige og feilaktige svar (Melbo, 2006, s. 62). Alle data som skal inn i systemet må derfor identifiseres, kvalitetssikres og konverteres til et hensiktsmessig format. Dette er en meget omfattende og kompleks jobb som krever kompetanse innen håndtering av integrering mot tilstøtende systemer internt i virksomheten, så vel som mot eksterne kilder utenfor egen organisasjon (Melbo, 2006, s. 62). Med hensyn til denne studien blir da datakvaliteten hos leverandør av interesse, samt hvilke utfordringer konvertering og implementasjon mellom Forsvaret og de sivile leverandørene. Som støtte til en slik konverteringsjobb og datautvekslingsjobb er det utviklet flere typer programvare som en kan bruke som mellomledd. Denne typen programvare omtales som "middelware " og blir liggende som form for filter mellom basene informasjonen skal flyte mellom. Programvaren er spesielt utviklet for å integrere programmer fra forskjellig leverandører og sikrer at de ulike programmene kan utveksle datainformasjon.

IT Infrastruktur: Selv om et ERP system som SAP vil kunne dekke mye av Forsvarets behov for prosesstyring, vil det ikke kunne dekke alle områder. Det vil fortsatt være enkelte komplementære applikasjoner. Det må derfor gjennomføres en analyse på hvilke systemer som skal migreres inn og hvilke som vil måtte bestå på utsiden (Melbo, 2006, s. 51). Forsvaret er en kompleks organisasjon med en mengde *legacy systems*[7] noe som vil påvirke måten forretningsprosessene gjennomføres på (Melbo, 2006, s. 51). Ved innføring av ERP systemet eller ny moduler til eksisterende ERP system, må en stille seg en del kritiske spørsmål. Melbo (2006) påpeker at litteraturen primært ser på hensynet til organisatoriske og menneskelige forhold. Men han etterlyser større fokus på hvilke områder som ERP systemet ikke støtter. Han trekker i den sammenheng frem datasikkerhet *"...sikkerhetsrutiner, brannmurer virusbeskyttelse og backupløsninger..."* (Melbo, 2006, s. 52). Et siste poeng som særlig treffer Forsvaret er at *"..offentlig sektor kanskje sitter på kanskje [sic] enda mer sensitive opplysninger enn private organisasjoner..."* (Melbo, 2006, s. 52). Forsvaret har til forskjell fra de fleste sivil aktører en rolle å spille ikke bare i fred, men også i krise og krig. Det er derav vesentlig større konsekvenser

[7] Legacy system er eksisterende informasjonssystemer i en virksomhet ved innføring av et ERP system.

og strengere krav til sikkerhet og IT-infrastruktur for Forsvaret, da det i ytterste konsekvens kan handle om rikets sikkerhet.

Minimum av skreddersøm: Det er store kostnader knyttet til skreddersøm eller tilpasning av en virksomhets ERP system fremfor å endre virksomhetens prosesser. Det anbefales derfor å tilpasse prosessene fremfor skreddersøm (Melbo, 2006, s. 55). Kostnadene til skreddersøm knytter seg til ikke bare til selve implementeringen, men vel så mye i et lengre perspektiv ved vedlikehold av systemene. Det gir økt sannsynlighet for feilkilder, samt kan hindre gevinster ved senere oppgraderinger fra leverandør som følge av at de ikke kan implementeres uten å gjennomføre en verifikasjon opp mot skreddersømmen først (Melbo, 2006, s. 55).

Effektiv kommunikasjon: Det hevdes at *"Communication is the oil that keeps everything working properly"* (Somers & Nelson, 2001, s. 5). Det er med andre ord vesentlig at informasjon flyter mellom de enkelte aktører som berøres av et ERP system for å kunne få ut ønskede gevinster. Denne påstanden underbygges også av Finnangers (2012) studie på området i en norsk militær kontekst. Han hevder at *"Better sharing of information vill lead to a better-shared situational awareness…"* (Finnanger, 2012b, s. 6). For å legge til rette for en god informasjonsflyt samt muliggjøre utveksling av informasjon til og fra andre systemer anbefales det å benytte seg av *service-oriented architecture* (SOA). SOA vil være nødvendig som verktøy for å få utvekslet informasjon mot Forsvarets legacy systemer, eller mot leverandører av PBL løsning som for eksempel kampfly F35 med ALIS (Finnanger, 2012a, s. 3).

Ut fra beskrevet teori om ERP fremgår det at samling av informasjonsdata i ett system (SAP) og datakvalitet er vesentlige faktorer for å oppnå ønsket effekt av systemet. Studien vil derfor bruke faktorene *datakvalitet* og samling av data, benevnt som *sentralisering,* som faktorer i analyse og drøfting i kapittel 7.

4 Aktuelle aktører

Det er flere aktører som har en rolle inn mot IKT området direkte eller indirekte, og derigjennom også en rolle i å tilrettelegge eller skape premisser for effektiv informasjonsdeling i Forsvaret. Det er ingen enkel sak og danne seg et bilde av de forskjellige aktørene og de enkeltes ansvarsområder, men McKinesey (2015) rapporten har oppsummert de grove trekk som følger:

> *I Forsvaret finnes det fire rendyrkede IKT-enheter: Cyberforsvaret, FLO* [FMA] *IKT-kapasiteter, Forsvarets FIF-administrasjon (FFA) og LOS-programmet. Sjefen for Cyberforsvaret er CIO* [Chief Information Offiser] *med fagmyndighet for cybermilitær virksomhet og det teoretiske ansvaret for IKT i Forsvaret. Han har derimot ingen kommandomyndighet over FLO* [FMA] *IKT, FFA eller LOS. FLO* [FMA] *IKT har fagansvar for IKT-materiell og er ansvarlig for konfigurasjonsstyring samt fremskaffelse og godkjenning av alle innkjøp og investeringer. FFA har det funksjonelle eierskapet for de deler av IKT-virksomheten som er tilknyttet FIF, mens LOS-programmet står for prosjektgjennomføring av FIF* (McKinsey & Company, 2015, s. 52).

Den siste større endring innen aktørene var etableringen av FMA i januar 2016. FMA har overtatt mange av funksjonene til tidligere FLO. Denne studien vil ikke ta for seg alle aktørene, men se på de mest sentrale med hensyn til forskningsspørsmålene.

FMA: består av, utover stabsfunksjonene, av en investeringsavdeling, drifts- og økonomiavdeling og materiellavdeling med underavdelingene land-, maritime-, luft-, IKT-, og felleskapasiteter.

FMA luftkapasiteter: er fagkapasiteten i Forsvarsmateriell som har ansvaret for å kjøpe, utvikle og forvalte Forsvarets fly, helikopter, droner og luftvernmateriell. De er blant annet ansvarlig for koordinering av drift- og vedlikehold av luftkapasiteter. Gjennom overvåkning av systemtilstand, gjennomføre ROS-analyser med påfølgende avvikshåndtering, styre vedlikeholdsarbeider, forsynings- og modifikasjonsbehov og kontroll på systemkonfigurasjon sikrer luftkapasiteter at luftflåten holder en operativ akseptabel stand. De er også ansvarlig for anskaffelse av nye kapasiteter som nye kampfly F35, NH-90 og AW101-helikopter (Forsvaret, u.å.-e). Innføringen

av kampfly F35 med tilhørende forvaltningssystem ALIS krever nybrottsarbeid ved integrasjon mot dagens FIF plattform. Studien kommer tilbake til det under drøftingen.

FMA landkapasiteter: har ansvar for utvikling, kjøp og eierskapsforvaltning av det meste av Forsvarets landmateriell og våpen. Landkapasiteter har materiell som panserkanoner, tunge og lette maskingevær og elektrooptisk materiell. Det er store investeringer innen landkapasiteter i perioden fremover, med dertil-hørende materiell som skal innordnes i forsyningssystemene (Forsvaret, u.å.-d). Dette innebærer omfattende kodifiseringsarbeider og samhandel med leverandørene for å sikre tilstrekkelig datakvalitet, slik at ERP systemet kan utnytte sitt potensiale.

FMA IKT-kapasiteter: har fagansvaret for IKT og skal forvalte sikker bruk av IKT i den daglige drift så vel nasjonalt som utenlands. De er ansvarlige ved anskaffelser av ” *nytt datasystem, nye sensorar eller applikasjonar…”* (Forsvaret, u.å.-c). Avdelingen eier og forvalter IKT materiellet samt systemene og har derigjennom et ansvar for tilrettelegging og muliggjøring av nettverksbasert forsvar (NbF).

FMA felleskapasiteter: har fagansvaret for anskaffelse, utvikling og forvaltning av alt materiell som er felles for de ulike forsvarsgrenene. Herunder konfigurasjon, kodifisering og oppfølging av vedlikeholds krav. Dette kan typisk være materiell som spenner fra telt til drivstoff, ammunisjon og eksplosiver, verktøy, sanitetsmateriell og veterinærtjenester (Forsvaret, u.å.-b). En del av materiellet er særegent men i lite kvantum, som for eksempel lagertelt, så det gjøres løpende kost nyttevurderinger på hvorvidt materiellet kodifiseres og legges inn i SAP eller ikke, men det tilstrebes at mest mulig legges inn. Studien kommer tilbake til det under drøftingen.

FMA maritime kapasiteter: har fagansvaret for anskaffelse og forvaltning av fartøyene i hele levetiden. De skal sikre at fartøyet med tilhørende våpensystemer forvaltes og følges opp med konfigurasjonskontroll, delelager, vedlikehold med mer på lik linje som luft-, land- og felleskapasiteter men innenfor det maritime domenet (Forsvaret, u.å.-f). Det som er særegent ved det maritime er at fartøyet i seg selv fungerer som en autonom plattform som ikke har tilgang på faste linjer inn i forvaltningssystemet.

NSM: er det sentrale direktoratet og nasjonale ekspertorganet for informasjons- og objektsikkerhet. Det er også det nasjonale fagmiljøet for IKT-sikkerhet. NSM skal sikre *"...beskyttelse av informasjon og infrastruktur av betydning for samfunnskritiske og andre viktige samfunnsfunksjoner."* (FDs cyberretningslinjer, 2014, s. 18). NSM har det utøvende ansvar for forbyggende sikkerhet. Av oppdrag til direktør NSM ligger blant annet sikkerhetsgodkjenning av informasjonssystemer der dette er tillagt NSM, samt å ivareta rollen som sertifiseringsmyndighet for IKT-sikkerhet i produkter og systemer (FDs cyberretningslinjer, 2014, s. 18). Med det menes å

> *Ivareta materiellsikkerheten for det materiell som skal brukes/utprøves i etaten, herunder drifte, bruke og vedlikeholde materiell etter krav fra fagmyndighet materiell samt godkjenne materiell for bruk i egen etat* (Forsvarsdepartementet, 2016b, s. 6).

Det er med andre ord NSM som er godkjenner sikkerhetsløsninger og materiell som skal inn på forsvarets sikre plattformer. Som faginstans er det også de som kan, om dokumentasjon og løsningen som sådan er god nok, godkjenne overføringsmekanismer mellom graderingsnivåer. Eksempel på en slik løsning som har fått godkjenning er dagens tonivå løsning på FISBasis der en via en Citrix løsning kan overføre dokumenter opp til en gitt størrelse mellom BEGRENSET side og over til ugradert. Løsningen fungerer begge veier og har flere lag av sikkerhet for å sikre at gradert informasjon ikke kommer over på ugradert side.

Cyberforsvaret: har ansvar for drift, sikring og forsvar av Forsvarets datasystemer, nettverk og plattformer. Cyberforsvaret skal videre lede utviklingen av NbF gjennom eksperimentering og konseptutvikling (Forsvaret, u.å.-a). Dette materialiserer seg ved for eksempel utvikling av systemarkitekturarbeid. En felles systemarkitektur er en vesentlig rammefaktor for å sikre enhetlige systemer. Cyberforsvaret har to underavdelinger. Den ene er Cyberforsvarets kompetanse- og transformasjonsavdeling (CKT) som blant annet utvikler og etablerer informasjonssystemer for å sikre kommunikasjon i operasjonsområdet (Forsvaret, u.å.-a). I dette ligger at systemene må kunne ha tilgang på nødvendige forvaltningsverktøy for gjennomføring av operasjoner i inn-, og utland. Den andre er Cyberforsvarets avdeling for cybertjenester og -operasjoner (CTO). CTO har ansvaret for drift og videreutvikling av Forsvarets sikre plattformer (FSP), tjenesteleveranser. CTO er også ansvarlig for Forsvarets IKT-infrastruktur og leveranser av virksomhetskritiske tjenester til sentrale deler av statsforvaltningen (Forsvaret, u.å.-a). Det er CTO ved avdeling for drift og videreutvikling (DVU) som står som ansvarlig for teknisk implementasjon og forvaltning av FIF. Som en del av det ligger innføringen av nye moduler i

SAP ved økonomiprosjektet (2008) Human Resource Management (HRM)-prosjektet (2014), og sist nå logistikkprosjektet som er i utrullingsfasen i skrivende stund. Cyberforsvaret er således en meget sentral aktør med hensyn til forsyningskjeden, informasjonsflyt og datakvalitet.

De nevnte avdelinger er på ingen måte utfyllende for alle aktører som i en eller annen form berører denne studien, men de ansees som de mest sentrale med hensyn til drøftingen. Det er en utfordring å få oversikt over hvem som har de forskjellige roller og ansvar innenfor IKT domenet, noe som også påpekes i McKinsey rapporten. McKinsey skriv at:

> *Det er videre store uklarheter i ansvarsforhold og ingen unison begrepsbruk mellom funksjoner. Dette driver både duplisering av funksjoner, eksempelvis i skillet mellom forvaltning og drift, og uløste oppgaver, eksempelvis rundt brukerstyring av systemer* (McKinsey & Company, 2015, s. 51).

videre står det at:

> *Forsvaret har en fragmentert organisasjonsmodell for anskaffelser som fører til småskalaproduksjon og gjør det vanskelig å bygge kompetanse og opprettholde standarder (McKinsey & Company, 2015, s. 117)*.

Ut fra de beskrevne aktører med påvirkning på informasjonsdeling i forsyningskjeden vil jeg bruke faktoren *aktører og arkitektur* til analyse og drøfting i kapittel 7.

4.1 Trusselaktører

Hvem og hva er truslene ved digital informasjonsdeling? Dette har tradisjonelt vært enkeltindivider eller mindre grupper som utførte IKT kriminalitet. Men med fremveksten- og anvendelsen av internett har dette utviklet seg til også å omfatte organisert kriminalitet, organisasjoner og nasjoner. Intensjonen bak angrepene favner vidt fra økonomisk vinning og meningsytringer, til å ramme nasjonal kritisk infrastruktur gjennom cyberangrep i den hensikt å skaffe informasjon eller oppnå et fortrinn ved for eksempel å sette kritiske systemer ut av spill. Det skilles ofte mellom fire kategorier av trusler og hvem som er aktørene bak.

Cyberkriminalitet: er som annen kriminalitet ulovlige aktiviteter, men innenfor cyberdomenet. Dette kan være svindel, økonomisk utroskap, omsetning av ulovlige gjenstander, substanser eller mennesker med mer via internett. Dette utføres oftest av enkeltindivider, grupper eller

organiserte kriminelle som har økonomisk vinning som motivasjon. Det er enn så lenge ikke gjennomført terroraksjoner via cyberspace i Norge (Meld. St. 37 (2014-2015), 2015, s. 28).

Aktivisme: aktørene har til hensikt å få medieoppmerksomhet eller påvirke andres atferd. Dette gjøres for eksempel ved å overta websider eller datamaskiner hos virksomheter eller myndigheter. For eksempel ble den amerikanske sentralkommandoen angrepet via twitterkontoen av hackere som hevdet å representere Islamic State of Iraq and the Levant (ISIL) (Meld. St. 37 (2014-2015), 2015, s. 29).

Etterretning: dette er den mest alvorlige trusselen mot norske interesser. I fredstid er aktørers innsyn i sensitiv informasjon rundt politiske beslutninger, industrispionasje, intellektuell eiendom eller forsvarshemmeligheter det mest alvorlige. Flere nasjoner har over tid målrettet bygget denne typen kapasiteter, og det er avdekket aktiviteter med informasjonsinnhenting i Norge. NSM har hatt en tredobling av IKT hendelser i perioden 2007-2011 og i 2011 ble en serie målrettede angrep mot olje- og gassektoren, energisektoren og forsvarsindustrien avdekket av NorCERT[8] (Meld. St. 29, 2011-2012, s. 104). Av nasjoner som ansees å ha størst kapasitet og aktivitet på området er USA, Kina og Russland de ledende. Russisk etterretning antas å ha størst skadepotensiale for norske interesser (Politiets sikkerhetstjeneste, 2015).

Digital krigføring: her anvendes cyberdomenet for nettverksoperasjoner som vil være en integrert del av kampanjen for å sabotere eller hemme en motstander isolert sett, eller for å støtte oppunder konvensjonelle militære operasjoner. For eksempel antas

> *CyberBerkut, en prorussisk gruppe av hackere, å stå bak angrep mot regjeringens websider i Tyskland, Polen og Ukraina, samt flere av NATOs nettsider. Disse angrepene antas å være koblet til konflikten i Ukraina* (Meld. St. 37 (2014-2015), 2015, s. 30).

For å sikre forsyningskjeden og Forsvarets informasjon fra ikke ønskede hendelser effektuert fra trusselaktørene er det essensielt at *sikkerhet* har fokus i alle virksomhetens ledd. Studien vil derfor benytte faktoren *sikkerhet* ved analyse og drøfting i kapittel 7.

[8] NSM NorCERT er Norges CERT-funksjon. CERT er et kjent begrep internasjonalt. CERT står for Computer Emergency Response Team og er en koordinerende enhet for informasjonssikkerhet. NorCERT er den operative delen av NSM (Nasjonal Sikkerhetsmyndighet, u.å.).

5 Rammefaktorer

Forsvaret har på lik linje som andre aktører i Norge en mengde lover, regler og instrukser å forholde seg til. I tillegg vil Forsvaret som medlem i NATO måtte forholde seg til anbefalinger derifra. Det har til denne studien vært en utfordring å få oversikt over alle de relevante krav som stilles til informasjonsforvaltningen i Forsvaret eller som indirekte gir rammefaktorer som Forsvaret må forholde seg til. Dette støttes også av utsagn fra flere av respondentene som heller ikke var kjent med skriftlige føringer for forvaltning av informasjon utover de som er nedfelt i lovverket.

Av sentrale lover som gir føringer for Forsvaret er Sikkerhetsloven den mest aktuelle for informasjonsdeling mellom Forsvaret og sivile leverandører. Det er i Sikkerhetsloven §13 om sikkerhetsmessig godkjenning av informasjonssystemer nedfelt krav om at:

> *Før skjermingsverdig informasjon behandles, lagres eller transporteres i et informasjonssystem, skal Nasjonal sikkerhetsmyndighet, eller den Nasjonal sikkerhetsmyndighet bemyndiger, godkjenne systemet for angjeldende sikkerhetsgrad* (Sikkerhetsloven, 1998§13).

Videre står det at NSM *"...er sertifiseringsmyndighet for informasjonssystemer som skal håndtere skjermingsverdig informasjon."* og at de kan *"...godkjenne at andre virksomheter utfører tjenester for sikring av informasjonssystemer som skal håndtere skjermingsverdig informasjon."* (Sikkerhetsloven, 1998§13). Det er med andre ord NSM som har ansvaret for at Forsvarets systemer for informasjonsforvaltning herunder FIF og SAP settes opp og forvaltes i henhold til regelverket. For personellet som skal ha tilgang til skjermingsverdig informasjon er det krav om at disse skal autoriseres i henhold til §19. Denne studien ser på informasjonsutveksling mellom FIF ved SAP som er gradert BEGRENSET (B), og de sivile leverandørene som i all hovedsak opererer på utsiden av Forsvarets infrastruktur. Studien rammes således ikke av kravet om sikkerhetsklarering for personell som i sitt arbeid vil kunne få tilgang til KONFIDENSIELL (K) informasjon, men problemstillingen vil allikevel være av interesse da implikasjonen vil gjelde for enkelte leveranser. Dette være seg leveranser av en gitt art til Forsvarets spesialstyrker (FS) eller sensor-, våpendata eller annen informasjon som er høyere gradert.

Vedrørende sammenkobling av informasjonssystemer er det nedfelt i Forskrift om informasjonssystemer at

> *Såfremt ikke NSM bestemmer annet, gjelder at informasjonssystemer med: 1. Dedikert operasjonsmåte skal bare tilknyttes systemer med samme graderingsnivå, autorisasjonskrav og tjenstlige behov* (FOR-2001-07-01-744: Forskrift om informasjonssikkerhet, §5-8).

Det er med andre ord ikke gitt rom for sammenkobling av systemer med ulikt graderingsnivå. For denne studiens del betyr det at SAP basen som ligger på B plattform ikke kan kobles mot ugradert (U) side med mindre NSM godkjenner løsningen.

Lov om elektronisk kommunikasjon (ekomloven) regulerer virksomheten for elektronisk kommunikasjon. For Forsvaret som er i en særstilling, som følge av kravet om å virke i fredstid så vell som krise og krig, gir ekomloven mulighet for å pålegge leverandører av elektroniske kommunikasjonstjenester tilgang til nettverk. Loven åpner også for å gi føringer om tiltak hos leverandør slik at sikkerhet og taushetsplikt hos leverandør opprettholdes (Ekomloven, 2003).

Anskaffelsesregelverk for forsvarssektoren (ARF) gir føringer for hvordan anskaffelser og investeringer skal gjennomføres. Paragrafer som er av særlig interesse for denne studien er de som berører grensesnitt for informasjonsutveksling og sikkerhetsaspekter ved anskaffelser. Loven regulerer områder innen arkivering, innsyn, sikkerhetsgraderte anskaffelser og habilitet i kapittel 2 (Anskaffelsesregelverk for forsvarssektoren (ARF), 2013). ARF §2-9 regulerer sikkerhetsgraderte anskaffelser av varer og tjenester. Det er der nedfelt at det skal gjennomføres en vurdering på hvorvidt

> *…anskaffelsen vil innebære utlevering av skjermingsverdig informasjon til leverandøren, om leverandøren får behov for å tilvirke skjermingsverdig informasjon, eller om selve anskaffelsen må sikkerhetsgraderes (Anskaffelsesregelverk for forsvarssektoren (ARF), 2013§ 2-9)*.

Det er NSM som fagansvarlig som svarer på spørsmål ved denne typen anskaffelser. Det er i §6-5 nedfelt krav om å definere hvem som har systemansvaret for leveransen. Grunnregelen er at dette legges til leverandør, med mindre det kan dokumenters at det er mest fordelaktig at Forsvaret tar ansvaret. §12-5 og §12-6 gir føringer for bruk av standarder og spesifisering av grensesnitt. Det gis der føringer for at Forsvaret skal bruke åpne standarder ved spesifisering av teknisk kravspesifikasjon. Dette er standarder som STANAG, AQAP, Forsvarets Standard, OSO,

DIN, Norsk Standard med flere *(Anskaffelsesregelverk for forsvarssektoren (ARF), 2013§12-5)*. Grensesnittet skal være basert på "*…mest mulig åpne grensesnitt" (Anskaffelsesregelverk for forsvarssektoren (ARF), 2013§12-6)*. §13-5 stiller krav til et kvalitetsstyringssystem hos leverandør for å sikre at denne kan dokumentere tilfredsstillende systemer for ivaretakelse av kontraktsfestede krav. §13-8 stiller krav til dokumentasjon og planer til blant annet konfigurasjonsstyring, kvalitet og sertifikater som bekrefter personellets kompetanse. Gjennom fremlagt dokumentasjon vil anskaffelsesmyndigheten sikre seg et tilfredsstillende fokus på sikkerhetsaspektene ved leverandøren. Det er også krav i §13-9 om at leverandøren har avtalefestet tilsvarende krav med sine underleverandører slik at disse også følger samme kvalitetssikringskrav som hovedleverandør *(Anskaffelsesregelverk for forsvarssektoren (ARF), 2013)*.

Kapittel 14 er i sin helhet viet krav til konfigurasjonsstyring. Oppsummert gis det føringer for at

> *Konfigurasjonsstyring må følges opp nøye for blant annet å kunne fastslå konsekvensene av endringer, holde oversikt over hvilke tekniske løsninger som tidligere er innført, eventuelt forkastet (historikk, sporbarhet) og sikre at det finnes dokumentasjon som viser om senere versjoner av produktet er kompatibelt med hva som er levert tidligere* (Anskaffelsesregelverk for forsvarssektoren (ARF), 2013§14-1).

Der er også krav i §15-1 om at alle forsyningsartikler i forsvarssektoren skal kodifiseres i henhold til NATO kodifiseringssystem. §31-2 Krav om informasjonssikkerhet, sier at *"Forsvarssektoren skal kreve dokumentert at leverandøren er i stand til å oppfylle de kontraktsrettslige forpliktelsene som forsvarssektoren stiller.*" (Anskaffelsesregelverk for forsvarssektoren (ARF), 2013). Det er med andre ord en forpliktelse hos leverandør å stille nødvendig dokumentasjon til rådighet for Forsvaret.

Av andre sentrale publikasjoner for denne studien nevnes:

- 1510 - Bestemmelser for integrert logistikkstøtte, systemteknikk og informasjonshåndtering i Forsvaret
- 1770 – Reglement om utøvelse av materiellregnskap i Forsvaret
- 773 - Reglement for telling og avvikshåndtering av materiell i Forsvaret

Disse publikasjonene stiller blant annet krav om at *"All relevant informasjon skal forvaltes i FIF med tanke på tilgjengelighet og gjenbruk"* (Forsvarets Logistikk Organisasjon, 2010, s. 7). Det er i 1770 krav om at

> *Anskaffelse av materiell skal gjøres elektronisk, slik at all ankomst og mottak registreres og alt materiell blir synliggjort med tanke på telling, fakturabetaling og utlevering. Materiellet skal være kodifisert eller etablert i SAP slik at elektronisk system kan vise historikk* (1770 - Materiellregnskap, 2014, s. 11).

Reglement for telling og avvikshåndtering gir føringer for hyppigheten og utøvelsen av telling for de forskjellige materiellkategorier. Det er for eksempel krav om at *"Våpen ved brukende avdelinger, uansett type og verdi, skal det telles 100% minimum en gang hvert år."* (773 Reglement for telling og avvikshåndtering av materiell i Forsvaret, 2010, s. 5).

Ut fra det ovenstående, som ikke på noen måte er utfyllende for rammefaktorer en må ta hensyn til ved forvaltningen i Forsvaret, ser en at det er sterke føringer med hensyn til sikkerhet i informasjonssystemene og forvaltningen av dem og informasjonen de inneholder. Denne studien vil derfor bruke samlebegrepet *rammefaktorer* i analyse og drøfting i kapittel 7.

6 Faktorer til analyse

Det er ut i fra litteraturstudiet i kapittel 3, aktuelle aktører i kapittel 4 og rammefaktorer i kapittel 5 redegjort for valg av faktorer. Faktorene vil danne rammeverket for analysen av de enkelte forskningsspørsmål i kapittel 7. Nedenfor følger en oversikt av valgte faktorer med en kort beskrivelse av hvorfor disse er valgt.

Utledede faktorer	**Utledet beskrivelse**
Informasjonsdeling	Er en forutsetning for en velfungerende SCM, PBL eller forsyningskjede
Integrasjon	For å kunne samle all informasjon i ett system ved en ERP løsning må en ha løsninger for integrasjon av informasjon fra systemer som ikke kan løses av ERP systemet.
Datakvalitet	Er en forutsetning for et velfungerende ERP system, som igjen er forutsetning for god informasjonsdeling.
Sentralisering av data	Grunntanken ved et ERP-system er å samle all informasjon i en database for derigjennom muliggjøre effektiv informasjonsutveksling.
Rammefaktorer	Lover, regler, føringer som påvirker mulighetsvinduet for informasjonsdeling.
Aktører og arkitektur	Påvirker utvikling, variantbegrensning og enhetlige prosedyrer. Har innvirkning på variantbegrensing og konfigurasjonskontroll.
Sikkerhet	Ufravikelig rammefaktor som må hensynstas i alle Forsvarets beslutninger. I Forsvarssammenheng ofte knyttet opp mot sikkerhetsloven.

Tabell 3 Utledede faktorer

7 Analyse og drøfting av data

Dette kapitlet inneholder analyse og drøfting av de data som fremkommer fra gjennomførte intervjuer. Analysen av intervjuene vil sees i lys av teori og empiri redegjort for i litteraturstudien i kapittel 3, samt utledede faktorer oppsummert i kapittel 6. Kapitelet er strukturert slik at det først vil ses på forskningsspørsmålene samlet opp mot den enkelte faktor. Deretter vil det komme en oppsummering for det enkelte forskningsspørsmål.

7.1 Forskningsspørsmål

For å besvare problemstillingen i studien er det utarbeidet to forskningsspørsmål. Disse er henholdsvis:

> *Hvilke konsekvenser får økt sivilisering av forsyningskjeden for informasjonssikkerheten?*

og

> *Hvilke konsekvenser får økt sivilisering av logistikken med hensyn til forvaltningen av understøttelsessystemet?*

Ved gjennomgang av litteraturstudiet ble det avdekket en del områder som fremstår som essensielle for å ha en velfungerende forsyningskjede. Disse områdene danner grunnlaget for faktorene *informasjonsdeling, integrasjon, datakvalitet, sentralisering av data, rammefaktorer, aktører og arkitektur* og ikke minst *sikkerhet.*

Forsvaret har vært gjennom en periode med store omstillinger de senere år, så også innenfor IKT området med innføringen av FIF og etablering av Cyberforsvaret (McKinsey & Company, 2015, s. 16). McKinsey (2015) konkluderer i sin analyse av IKT området i Forsvaret med at

> *Videre eksisterer det ingen omforent oversikt over alle systemene i sektoren og hvem som har ansvaret for disse.",* og videre *"...har sektoren valgt en uegnet organisering av IKT. Modellen bidrar til ansvarspulverisering og uløste oppgaver.* (McKinsey & Company, 2015, s. 51).

Med det som bakteppe skal en så søke å gå i retning av økt informasjonsdeling mellom Forsvarets systemer og sivile. I det følgene vil det drøftes mulige utfall av en slik utvikling med henblikk på faktorene sammenfattet i kapittel 6.

7.1.1 Informasjonsdeling

Etter gjennomført analyse av intervjuene fremstår det som omforent fra respondentene at effektive løsninger for informasjonsutveksling er helt nødvendig for at Forsvaret skal kunne realisere gevinster ved ERP så vel som SCM, forsyningskjeden eller PBL kontrakter. Dette underbygges av utsagn vedrørende mangelfull informasjonsdeling som ”*Det kan du sitere meg på! at da flyr ikke flyet! Da får vi ikke operert flyet, da står de på bakken etter veldig kort tid!”* (R6), og med hensyn til ERP system*”…egentlig er hele hovedpoenget med det, er at med en gang det har skjedd en endring, så vil andre aktører se det.”* (R7). For koordinering av vedlikehold ”*Så der har vi ett slikt samarbeidsrom da, der vi kan logge oss på og finne informasjon om den bilen.”* (R3). Disse utsagnene stemmer godt overens med funnene i litteraturstudien der viktigheten av informasjonsdeling er nevnt en rekke ganger. Men en ting er å ha et teoretisk og empirisk grunnlag om viktigheten, noe helt annet er hvorvidt den fungerer tilfredsstillende, og hva utvekslingen vil ha å si for informasjonssikkerheten og forvaltningen av understøttelsessystemene i Forsvaret.

Ved økt bruk av sivile aktører vil det nødvendigvis bli økt behov for å utveksle informasjon. Det som i liten grad er gjort funn av innen litteraturen er hva det vil ha å si i et sikkerhetsperspektiv. Forvaret er der, som et politiske virkemiddel for ivaretakelse av rikets sikkerhet, i en særstilling ved at Forsvarets systemer befinner seg på en gradert plattform. Nå er riktignok mye av informasjonen om materielldata ugradert, men all den tid den ligger på en gradert plattform, må en være bevisst hva en deler. Videre kan deler av informasjonen som leverandør trenger tilgang til være gradert, noe som gir utfordringer om ikke leverandør har systemer for ivaretakelse av informasjonen etter gjeldene føringer. Dette er forhold som stiller helt andre krav til utvekslingsmekanismer enn når en generell detaljist skal knytte seg opp mot en leverandør. Forsvaret må derfor sikre seg at den informasjon som utveksles blir håndtert på en sikkerhetsmessig tilfredsstillende måte. Funn i analysen tyder på at sikkerhetsfokuset på hva en deler har en fremtredende rolle. Noe som underbygges av en *”Need to know basis”* (R4) og *”Vi deler ingenting om vi ikke har et behov som gir en beredskapsmessig merverdi”* (R1), så det fremstår som om hva en kan og vil dele har et fokus. På den annen side var det noe mer sprikende med hensyn til hvilke føringer som regulerer hva som må- og kan deles. De fleste trakk frem sikkerhetsloven som rammeverket som regulerte hva de kunne dele, men det ble også trukket frem lov om offentlige anskaffelser som den mest sentrale. Denne divergensen kan ha sammenheng med hvilken organisatorisk funksjon respondent skulle fylle. Det anses ikke

usannsynlig at en avdeling som skal drifte og ivareta FSP har et helt annet behov og syn på informasjonsdeling, enn en aktør som skal sikre koordinering og utøvelse av vedlikehold på Forsvarets lette kjøretøy mot sivil leverandør. Noe som ble viet mye fokus var viktigheten av en solid analyse over hva behovet for informasjonsdeling egentlig var. Hva trenger leverandør å vite, og hva trenger Forsvaret å vite om leverandøren. Et eksempel på den typen utfordring kan være for kampfly F35 der Lockheed Martin (LM) *"...kommer og sier at vi trenger den og den informasjonen."* (R6), hvor prosjektet må vurdere *"..trenger dere den informasjonen da? Vi sier nei, dere trenger ikke den informasjonen, også får de heller komme tilbake."* (R6). Noe som fører til en runddans, der forespørsler og svar går frem og tilbake mellom kunde og leverandør. Rasjonale bak er trolig at som sivil aktør ligger det et krav om økonomi på bunnlinjen og det enkleste for leverandøren er jo å ha tilgang på "all" informasjon. Det som trekkes frem som en utfordring i så måte er tilstrekkelige personellressurser for å ivareta og gjennomføre den vurderingen av hvorvidt informasjonen bør/kan deles eller ikke. Viktigheten av personell med rett kompetanse og forståelse for hva leverandør trenger av informasjon er derav nødvendig for å få gode avtaler. Det bemerkes at miljøene finnes, men de er spredt utover i forskjellige avdelinger, så *"...det er ikke noe felles miljø med kraftsamling nei"* (R6).

Et annet moment som ble trukket frem var viktigheten av dyktige kontraktsforvaltere. Behovet for informasjonsdeling oppstår som følge av en anbudsrunde der valgt leverandør trekker det lengste strået. Det er derfor avgjørende viktig at kravstiller stiller de rette kravene og får disse inn i kontraktsform ved utlysning. Er det ikke stilt krav til leverandørens informasjonsbehandling, vil en ikke kunne ekskludere denne heller.

> *Det er vel så enkelt at setter en det bort til en god leverandør som har kontroll og styring og vet hva han driver med, herunder informasjonsstyring og sikkerhet, stålkontroll, så vil du som kunde få klare og ryddige data og leveranser, mens er det en rotekopp så får du leveranser deretter.* (R2).

Men det er en kjensgjerning at sikkerhet koster, så om en ikke er nøye i kravstillingen vil en fort kunne få en tilbyder som kanskje ikke har tilfredsstillende fokus på sikkerhetsaspektet, men som er billigst som følge av et lavere sikkerhetsfokus. Et annet forhold som underbygger viktigheten av kompetanse ved kontraktsinngåelse er at *"...nå har vi begrensede muligheter for å ekskludere leverandører..."* (R5). Utfordringen er at på den ene siden har en da en mulighet for å sette krav om for eksempel "erfaringer med leverandør" (R5), men på den annen side fordrer det at

> *...da må vi også ha det på de leverandørene vi ikke har erfaring med fra andre igjen, så det er et veldig vanskelig tema å snakke om slike ting som ikke er målbare eller konkrete* (R5).

Det er med andre ord ingen enkel løsning for å sikre seg gode leverandører all den tid Forsvaret i stor grad styres mot billigste tilbyder.

Med hensyn til forvaltningen av informasjonssystemene, der en fra et driftsteknisk perspektiv ønsker en enhetlig forvaltning og færrest mulig systemer, vil en økt sivilisering gi flere systemer å holde kontroll på. Ett eksempel er ALIS for F35 kampfly. Så der en fra driftssiden ønskes *"Ett system per graderingsnivå"* (R1), vil en økt bruk av PBL gå i motsatt retning. Det vil bli flere systemer, kompleksiteten vil derav øke, og kreve mer ressurser for å ivareta de underliggende systemer. En annen faktor som også trekkes frem med hensyn til forvaltningen av systemene er bruk av eksterne. Ved innføring av nye systemer som ALIS vil det være en *"...utfordring at de som skal forvalte systemene ikke er kjent med det nye systemet. De må kurses opplæres..."* (R6). Så enten må en øke forvaltingskapasiteten og kompetansen i Forsvaret for de enkelte systemer eller benytte eksterne for ivaretakelsen av systemet. Ved å bruke eksterne trekkes det frem en utfordring ved at *"Det er problemet med disse eksterne, du trenger en hel haug med mennesker for å kontrollere og følge dem opp i alle dimensjoner."* (R1). Dimensjonene som trekkes frem er økonomisk, avtalemessig og sikkerhetsmessig.

7.1.2 Integrasjon

Integrasjon mellom kunde leverandør er fremtredende i litteraturen både inne SCM, PBL og forsyningskjeder. Med hensyn til ERP er det den interne integrasjonen innad i virksomheten som har mye fokus, men også der er mekanismene for integrasjon og utveksling av informasjon med eksterne ved for eksempel SOA arkitektur en viktig bit. Imidlertid er integrasjon mot Forsvarets systemer en utfordring all den tid systemene som skal kobles sammen ikke er på samme graderingsplattform. For at en skal kunne få gjort det må en etablere mekanismer for sikker informasjonsutveksling som må godkjennes av NSM for det enkelte tilfelle. Ut fra analysen påpekes det at det per i dag er liten grad av integrasjon. Av systemer som nevnes er det FISBasis tonivå som går igjen. En har der mulighet for overføring av informasjon begge veier, men det er en manuell prosess, der utøvende part må godkjenne det enkelte objekt som skal overføres. Det er også en begrensning i filstørrelsen som skal overføres, noe som gjør løsningen

uhensiktsmessig ved større filer. Det fremkom med andre ord ingen integrert automatisk overføring. På den annen side har en flere muligheter for informasjonsutveksling ved at en kan benytte godkjent Lok-It minnepenn (USB-stikk), brenne ut CD eller skrive ut. Det som derimot er samlende for alle disse metodene er at det er en manuell prosess. Det medfører dermed et tidstap og krever ressurser ved at "noen" faktisk utfører jobben. På den annen side kan det gi bedret informasjonssikkerhet ved at det må gjennom en manuell kontroll for å overføres. Det gir god sikkerhet mot inntrenging fra trussel aktører ved at det ikke er mulig å få tilgang på informasjonen fra utsiden, men at en må være bruker på innsiden. Men personellet er ansett som den største sikkerhetstrusselen. Noe om underbygges av *"Nesten uten unntak så er det menneskelig svikt"* (R1) som årsak til kompromittering av data. Så integrasjon er således et tveegget sverd, der en må vurdere fordelene opp mot risiki.

Dagens løsning ved for eksempel utsetting av vedlikehold av en Scania lastevogn på Rena, er at det skrives vedlikeholds ordre i SAP, som så overføres via tonivå til ugradert side og sendes til Bertil og Steen (B&S) på Hamar som har rammeavtale på verkstedtjenester. Når bestilt vedlikehold er sluttført påføres fakturaen hva som er gjort spesifisert etter krav på hva det skal rapporteres på og sendes til Forsvarets regnskapsavdeling (FRA). FRA skanner fakturaen og knytter denne opp mot innkjøpsordren som innkjøper så kan kvalitetssikre opp mot hva som ble bestilt og hva som er utført fra B&S. Om ordre og leveranse stemmer overens må så utført vedlikehold registreres inn i SAP igjen med oppdaterte data. Oppsummert fra ansvarlig for vedlikeholdet

> *Det er greit med innkjøpsordre og kontering, men de tekniske dataene som står på fakturaen må løftes over og punches i SAP", "Vi bruker mye tid på den prosessen selv om det bare er en liten del av vedlikeholdet* (R3).

Det fremkommer i analysen at en ikke får utnyttet potensialet som ligger i Forsvarets ERP systemet som følge av manglende integrering.

> *Det er mye mer effektivt og raskt for planleggeren min å gjennomføre vedlikeholdet her, for da har vi arbeidsordrene på bordet her og det blir skrevet og punchet der og da! Skal den til Hamar er det mye mer administrativt arbeid!* (R3).

Som følge av den manuelle prosessen med å overføre og legge inn data manuelt, trekkes også sannsynligheten for menneskelige feil frem som en utfordring. Dette både med hensyn til tidstap og punchefeil som går utover datakvaliteten. Det fremkommer også forslag om fremfor å sende vognene til verksted, heller hente inn verkstedpersonell fra B&S. Men det ansees som minst like

krevende med hensyn til klarering, autorisasjon og oppfølging av personellet, da det også forefinnes gradert materiell på Forsvarets verksted. Så fra et vedlikeholds perspektiv ville en integrasjon, der leverandør kunne registrere vedlikeholdet direkte, eller pakket informasjonen i et format som kunne importeres via SOA gitt store besparelser. Nå har forsvaret allerede godkjente løsninger for deler av dette gjennom for eksempel import av persondata fra det sentrale folkeregister (DSF).

> *Kilden til det hele er folkeregisteret, DSF kopi, som kopieres over relativt ofte"* (R2).
> Men også der *"Utvekling mellom B/U er filbasert og det er en del arbeid med å trekke ut formatere flytte og pakke ut på den andre siden* (R2).

Men denne importen er bare fra ugradert og inn til FIF på gradert side. Det er ingen informasjon som går andre veien fra gradert til ugradert, og i en forsyningskjede går prinsipielt informasjon fra kunde til leverandør, og varestrøm fra leverandør til kunde. Så løsningen dekker i beste fall halve utfordringen, samt at det fortsatt er en manuell prosess som utfører selve importen.

En annen utfordring ved manglende integrasjon som fremkommer i analysen er tidsfaktoren. Det er noen typer informasjon som er tidskritisk både for Forsvaret og leverandør. Sikkerhet trekkes frem gjennom hele analysen som en flaskehals og *"...sikkerhet på grunn av det, informasjon fra Forsvaret til leverandør, jeg vet F35 vil det, vil forsinke mye av informasjonen som jeg vet de trenger i sann tid."* (R6). Men det påpekes at utfordringen også går andre vegen. Så det å få på plass en godkjent løsning for MLS mellom Forsvaret og leverandører av varer og tjenester ville vært gunstig for å kunne utnytte mulighetene i innførte systemer i Forsvaret. Det er derav betimelig å anta at ved en økt bruk av sivile tjenester og leveranser i Forsvaret vil konsekvensen av manglende integrasjon akkumuleres. Utfordringen blir å fremskaffe en arkitektur og prosedyre som ikke bare ivaretar integrasjonen teknisk sett, for det har vi, men også tilfredsstiller NSMs krav til ivaretakelse av blant annet informasjonssikkerheten ved integrasjonen.

Forsvaret har ved dagens SAP løsning ett ERP system som er tilrettelagt for integrasjon. Det påpekes at *"SAP legger til rette for tjenesteorientert arkitektur, et såkalt SOA", "Så det er ikke applikasjonen i SAP det er vanskelig å jobbe videre med"* (R7). Det som derimot trekkes frem som en utfordring med hensyn til integrasjon er de sikkerhetsmessige utfordringene ved å fremskaffe en NSM godkjent løsning.

7.1.3 Datakvalitet

Som det påpekes i kapitel 3 er tilstrekkelig datakvalitet en forutsetning for at Forsvarets ERP system skal kunne gi en positiv effekt. Situasjonen i Forsvaret er påpekt i rapporten til McKinsey som oppsummerer med at:

> *Datakvaliteten er kritikkverdig. Lav datakvalitet på innkjøpsordrene gjør det krevende å analysere kostnader og følge opp bruk av rammeavtaler, da bruk av varegrupper, materialnummer, rammeavtalenummer og artskonto er mangelfull og/eller inkonsekvent. Dette medfører også betydelig manuelt arbeid for Forsvarets ressurser innen anskaffelser og er en av forklaringene til merforbruket av ressurser sammenlignet med andre organisasjoner* (McKinsey & Company, 2015, s. 117).

Videre påpeker rapporten at *"…datakvaliteten på innkjøpsordrene er urovekkende lav."* (McKinsey & Company, 2015, s. 128)

Gjennom analyse av gjennomførte intervjuer, virker det som om det er et noe divergerende syn på hva respondenten legger fokus på. Noen respondenter har fokus på resistente og korrekte data, mens andre fokuserer mer på informasjonen dataene gir. Eksemplifisert ses det på om importerte data har rett format med hensyn til import til SAP, mens det andre fokuset kan være om lagerbeholdning er oppdatert og viser rett mengde. Men dette er på mange måter to sider av samme sak, all den tid, en trenger rett format for å få dataene inn, mens det andre fokuset går på anvendelse av informasjonen. Årsaken til denne divergensen skyldes muligens hvilken rolle de forskjellige respondentene har i organisasjonen. I det legges at dersom en jobber innenfor drift vil en ha fokus på det tekniske for å sikre at informasjonsdata flyter i ERP systemet, mens de på verkstedet vil ha fokus på anvendelsen av informasjonen og mindre fokus på hvilket format som nyttes for å få tilgang på informasjonen.

Innenfor konfigurasjonskontroll vil en være avhengig av god datakvalitet for å sikre seg for eksempel oversikt over hvilke oppgraderinger som er gjort på hvilke motorer? hvor mange km eller timer har de enkelte motorer gått? eller når ble siste vedlikeholds intervall gjennomført? Eksempelvis ved lastevognprosjektet der det før innlegging av data fra leverandør gjennomføres kontroll

> *Vi får jo informasjon på et PLCS format, XLS format så sjekker vi at den informasjonen henger korrekt sammen og at informasjonen ser korrekt ut[,]..i tillegg så går vi inn og*

sjekker at informasjonene på det fysiske, da tenker jeg på vogn, stemmer overens med informasjonen vi får tilsendt, det kan være det at leverandøren gjør, har feil informasjon som da vi får tilgang på (R4).

For å sikre at datakvaliteten er tilstrekkelig også hos leverandør, gjennomføres også tilsvarende kontroll med datainformasjon som eksporteres fra Forsvarets base til leverandøren. På den måten sikrer en seg at datainformasjonen holder god kvalitet hos begge parter. Utfordringen som trekkes frem er den manuelle prosessen som ved tidskritiske data vil gi en forsinkelse, samt muligheten for menneskelige feil.

7.1.4 Sentralisering av data

Det er tidligere redegjort for at all relevant informasjon skal forvaltes i FIF. Videre skal materiellet være kodifisert eller etablert i SAP. Dette er rammefaktorer som stemmer godt overens med forutsetningene for å få ønsket effekt av Forsvarets ERP system SAP. Det teoretiske grunnlaget for dette er redegjort for under ERP i kapittel 3.4. Det fremkommer imidlertid av analysen at det er en viss divergens mellom teori og praksis på området i Forsvaret. Det har gjennom arbeidet med SAP i de senere år vært gjennomført et omfattende arbeide for å redusere antall legacy systemer i forsvaret og migrere dataene over i SAP. Siste tilskudd er logistikkprosjektet som startet implementering i januar 2016. Dette medførte at noen av respondentene nylig hadde fått nye systemer å forholde seg til. Det kan igjen svekke relevansen av utfordringene de står overfor ved at det ikke er bygget erfaringer på det nye systemet enda. På den annen side er det rimelig å anta ut fra analysen at flere av utfordringene vil bestå også etter overgangen til SAP som system for understøttelse av forsyningskjeden. Det begrunnes ved at endringene i SAP skal sikre bedre intern informasjonsdeling og kontroll, mens denne studien konsentrerer seg om utveksling av informasjon mot eksterne.

Det som ble trukket frem som en av utfordringene var manglende kodifisering av materiell. Årsaken til denne mangelen, er for noe av materiellet at prosjektet ikke er ferdig med konvertering fra EDBVT[9], mens det for andre deler av materiellet skyldes endrede rammefaktorer etter anskaffelse av materiellet. Slike endringer begrunnes med utsagn rundt anskaffelsen av nye MAN lastevogner som skal erstatte dagens Scania. Respondenten forteller at

[9] EDBVT er et elektronisk databehandlingssystem for verkstedtjenesten. Dette er et system for registrering av vedlikehold på teknisk materiell på individnivå (kjøretøy, våpen, ingeniør- og sambandsmateriell) (Eilertsen, Hestvik, & Nilsen, 1999, s. 8).

> *...så ble det bestemt at vedlikeholdet skulle settes bort. Så vi anskaffet MAN uten dokumentasjon, for den skulle vi ikke skru på. Så vi har verken håndbøker, delekatalog eller noe som helst, og trengte heller ikke kodifisere noen deler, for det skulle vi ikke bruke* (R3).

Etter endrede føringer som følge av at de skulle til Afghanistan trengtes det kompetanse og deler. Så en *" ...sitter da med utfordringen i dag da det ble snudd om og vi skulle skru på den* [lastevognen] *allikevel."* (R3).

Av det som trekkes frem som positivt ved en sentralisering av datainformasjon påpekes forhold som variantbegrensning og sikkerhet. Ved å samle informasjonene i en base kan en ta ned legacy systemer som EDBVT. Det gjør at en får frigjort driftsressurser og en kan kraftsamle rundt ett system. Det trekkes også frem at det letter muligheten for å holde sikkerheten i systemet på et høyere nivå ved at en har ett system fremfor mange forskjellige. Likevel fremstår det ikke slik at en økt bruk av PBL kontrakter mot det sivile vil hjelpe Forsvaret med å få samlet all informasjon på ett sted. Ved innføring av ALIS for å understøtte F35, vil en få et eget system som blir liggende på utsiden av SAP. Dette tvinger seg frem som følge av kontrakten som er inngått med LM. Det er med andre ord lite som tyder på at Forsvaret vil nå målet om å få samlet alle materielldata i ett system. Dette fremkommer tydelig gjennom utsagn som

> *...den herre tanken om at vi skulle ha et FIF som skulle ivareta alt i Forsvaret, det er* [sic] *vel de fleste innsett at ikke ble sånn* [og] *...vi kommer nok til å ha mange systemer på utsiden.* (R6).

For å kunne ivareta denne strukturen må en derfor opparbeide tillit til systemene slik at disse kan brukes som hovedsystem så en unngår dagen dobbelføring.

7.1.5 Rammefaktorer

Gjennom studiens analyse av gjennomførte intervjuer fremkommer det at samtlige respondenter med unntak av én, trekker frem sikkerhetsloven som den mest sentrale faktor med hensyn til utveksling av data mellom Forsvaret og eksterne aktører, så vel som innad i virksomheten. Den siste respondenten anså lov og forskrift om offentlige anskaffelser som den mest sentrale for sitt virke. Det kan derav trekkes slutningen om at sikkerhetsloven er en premissgiver for hvordan utveksling av datainformasjon kan gjennomføres. For å kunne få informasjonsdeling på en mer strømlinjeformet måte, en dagens manuelle prosesser, må hver enkelt løsning det være seg en

integrasjon, kobling eller et system, godkjennes av NSM. Som det fremkommer av teorien og funn i studiens analyse så *"...skal vi ha PBL kontrakter, så må vi ha informasjonsdeling, hvis ikke vil det aldri fungere."* (R6). Når det er sagt, så må det ikke nødvendigvis være en integrasjon, men det må forefinnes en eller annen form for *"...kontrollert flytting av informasjon slik at vi vet nøyaktig hva som blir utvekslet."* (R6). Det vil være de samme sikkerhetsmessige utfordringer ved utveksling av informasjon uavhengig av om det er en PBL avtale, en rammeavtale for vedlikehold eller noe annet. Dette skyldes at det er selve utvekslingen som er den sikkerhetsmessige utfordringen mer enn i hvilken hensikt den må utveksles.

Forsvaret har riktignok en løsning for utveksling mellom B og U via tonivåløsningen på FIF, men den fremstår ikke som egnet ved utveksling av større mengder informasjon. En annen mulighet som trekkes frem er at leverandør har tilgang på FISBasis slik at informasjonsutvekslingen kan skje der. I noen tilfeller er det mulig og det er per i dag noen få aktører som har dette. Utfordringen ved den løsningen er at da må leverandøren tilfredsstille Forsvarets krav til sikkerhet i installasjonen. Nok en utfordring ved rammebetingelsene er om leverandøren befinner seg i et annet land. Det har, for eksempel ved innføringen av ALIS, vært og er flere utfordringer ved informasjonsdelingen med USA og LM. Dette skyldes at disse opererer med andre graderingsnivåer enn vi gjør. En utfordring da blir når *"...veldig mye av den informasjonen vi etterspør, spesielt i forhold til sikkerhetsgodkjenning, så er det ikke releasable til oss. Det er US only!"* (R6). Det blir da problematisk å fremlegge dokumentasjon mot NSM for godkjenning av løsningen.

Andre utfordringer som kommer frem ved analysen er at ved "*økt bruk av sivile leverandører så mister vi kontrollen på de kravene til regelverksetterlevelse som det offentlige har satt til sine anskaffelser"* (R5). I dette legges at det offentlige har større krav til regelverksetterlevelse enn det sivile ved anskaffelser. Så ved å sette ut anskaffelsene til sivile vil en kunne gå utenom en del av disse kravene. Dette kan for eksempel være krav om konkurranse. Det må derfor reguleres gjennom kontrakten hvilke krav som gjelder til anskaffelsen og hvordan informasjon skal håndteres for å sikre at det skjer innenfor regelverket.

7.1.6 Aktører og arkitektur

Innenfor anskaffelser er det mange aktører som har sine fagområder og anskaffer og skriver kontrakter for respektive avdelingers ansvarsområder. Det er med andre ord mange parallelle aktiviteter i forskjellige avdelinger i Forsvaret som jobber med de samme tingene. Det viser seg av de gjennomførte intervjuer at det i stor grad er opp til den enkelte anskaffer eller prosjektarbeider hvilke løsninger som velges. Det etterlyses en felles arkitektur for hvordan de enkelte systemer skal settes opp og et felles rammeverk for hvordan informasjonsdata bør overføres. Det fremkommer at arkitekturressursene også er spredt og at de i sum ikke har kapasitet til å støtte ved forespørsel. Konsekvensen blir en fragmentert og divergerende arkitektur på de enkelte systemer. Dette er forhold som også er påpekt i McKinsey rapporten der det stadfestes at det blant annet finnes hele 70 forskjellige ugraderte nett i Forsvaret (McKinsey & Company, 2015, s. 55-56). Dette medfører vesentlige utfordringer med hensyn til understøttelse av de enkelte systemene da manglende variantbegrensning og arkitektur gjør de enkelte systemer forskjellige fra hverandre. En slik fragmentert silobasert arkitektur er også sikkerhetsmessig uheldig og krever kompetanse på det enkelte system og oppfølging med hensyn til oppdateringer og konfigurasjon.

7.1.7 Sikkerhet

Sikkerhet i Forsvarets systemer er ufravikelig krav som det ikke kan eller bør lempes på. Det må være slik at informasjonen som ligger lagret der opprettholder sin konfidensialitet, integritet og tilgjengelighet. Ved en økning av sivile aktører er det redegjort for behovet for økt informasjonsdeling eller tilgang på informasjonsdata mellom kunde og leverandør. Utfordringen ligger i å få det til på en slik måte at ikke konfidensialiteten og integriteten blir brutt. Det finnes aktører der ute som ønsker tilgang på informasjon vi ikke ønsker de skal ha, og en må da sikre seg så godt som mulig mot at denne informasjonen kommer på avveie. En typisk slik aktør i militær sammenheng er fremmed etterretning, men også organiserte kriminelle kan søke å skaffe seg informasjon for økonomisk vinning. Kjennskap til viktigheten av sikkerhet er noe som bør gjennomsyre virksomheten i forsvaret. Fokuset på sikkerhet fremkommer derfor blant annet gjennom krav om risiko- og sårbarhetsanalyser (ROS) samt reguleringer av aktiviteten ved utdanningsdirektiv (UD) 2-1[10]. Men hvordan er det med sikkerheten innenfor forsyningskjeden? Er sikkerhet bare en hemsko som hindrer utnyttelse av mulighetsvinduet? Utsagn om at det er

[10] UD2-1 er forsvarets sikkerhetsbestemmelser for landmilitær virksomhet.

"sikkerhetskravene som hindrer oss i en god utnyttelse av forvaltningssystemene!" (R3) tyder på at Forsvaret, som følge av sin særegenhet med hensyn til sikkerhet, ikke drar samme effekt av for eksempel et ERP system som teorien fra sivil side tilsier. Dette gjelder ikke bare ved samhandel eksternt, men også på innsiden av Forsvarets ERP system. Dette begrunnes med at før innføringen av FIF hadde en for eksempel løsning for RFID[11] lesing av delenr på lageret. En kunne dermed raskt og effektivt gjennomføre lagertelling og hadde til enhver tid kontroll på hvilket materiell som var der. Etter innføringen ble dette ikke lenger godkjent av sikkerhetsmessige årsaker. Resultatet ble at en gikk tilbake til en manuell prosess der en må logge seg inn i SAP og registrere de enkelte komponenter eller transaksjoner manuelt. Et annet eksempel er ved de pålagte halvårlige inspeksjonene av materiell, som våpen eller annet attraktivt materiell. Bruk av RFID ville der gitt vesentlig redusert arbeidsmengde, samt bedret datakvalitet og kontroll på materiellet ved at punchefeil blir borte og derigjennom feilføringer. Så ved at en ikke lenger får bruke RFID leser blir det et større rom for menneskelig svikt ved at det punches feil, et vesentlig merarbeid og generelt dårligere kontroll på materiellet.

Det fremgår av analysen at det er stor forståelse for at sikkerhet er viktig, og at en ikke skal lempe med den, men det fremgår og at*"...noen ganger drar sikkerhetsregimet så langt at sikkerhet blir sikkerhets verste fiende."* (R1). I det legges at om sikkerhetsregimet blir uhåndterbart vil en finne andre løsninger for å få utført de oppgavene en er pålagt. Imidlertid er

> *Sikkerhet er en slik greie en kan bruke utømmelig med penger på, men så er systemene gått ut på dato før en får det implementert eller er ferdig med sikkerhetsvurderingene* (R1).

En må derfor søke å finne en balansegang mellom hva som er "godt nok" og vurdere dette i en kost nytte analyse. Dersom gevinsten forvaltningsmessig klart overstiger risikoen for uheldige hendelser så bør en kanskje vurdere å ta en operasjonell risiko på den delen. En mulig løsning det sees på i kampflyprosjektet er at det *"...lages en Gateway med krypteringsløsning, så vi kan monitorere, filtrere og kontrollere all informasjon."* (R6). Kampflyprosjektet kan i så måte bli en brekkstang for andre tilsvarende løsninger i Forsvaret for fremtiden slik at gevinstpotensialet i større grad kan realiseres. Men en slik Gateway er ikke hyllevare og må skreddersys inn mot den enkelte leverandør noe som er meget ressurskrevende. Løsningen er også avhengig av sikkerhetsmessig godkjenning fra NSM før den kan tas i bruk for det enkelte system.

[11] Radio Frequency Identification, RFID) er en metode for å lagre og hente data ved hjelp av små enheter kalt RFID-brikker.

En annen sikkerhetsmessig utfordring som er trukket frem er akkumulert informasjon. Med det menes at om en samler tilstrekkelig med informasjonsdata vil graderingsnivået kunne stige. Eksempelvis er ikke vedlikeholdsstatus på en Scaniamotor nødvendigvis gradert isolert sett, men har en status på alle Scaniamotorene i Forsvarets kjøretøypark blir det en helt annen sak. Det vil da være informasjon som sier noe om evne til forflytning av materiell, og graderingsnivået vil kunne øke. Det er med andre ord ikke slik at selv om de enkelte datainformasjonselementene er ugradert, så kan en se bort fra sikkerhetsaspektet ved informasjonsutvekslingen. Ved økt bruk av sivile aktører vil da også informasjonsflyten over til sivil side øke, med det til følge at risikoen øker for uønsket innsamling av data.

7.2 Oppsummering

Det er i det foregående gjennomført en analyse og drøfting av de data som fremkom fra gjennomførte intervjuer. Analysen av intervjuene og drøftingen er basert på teoriene redegjort for i kapittel 3. Det teoretiske grunnlaget er deling av datainformasjon og dennes rolle i forsyningskjeden, SCM, PBL og ERP systemer. For å belyse forskningsspørsmålene er de utledede faktorene: *informasjonsdeling, integrasjon, datakvalitet, sentralisering av data, rammefaktorer, aktører og arkitektur* og *sikkerhet* brukt som rammeverk.

7.2.1 Forskningsspørsmål 1

Det første forskningsspørsmålet som ble drøftet var

Hvilke konsekvenser får økt sivilisering av forsyningskjeden for informasjonssikkerheten?

Det fremstår etter studien som tydelig at en effektiv utveksling av datainformasjon mellom Forsvaret og leverandør er sett på som helt avgjørende for å få ønskede resultater. For eksempel vil ikke kampfly F35 kunne ta av og fly om ikke nødvendig informasjons deles med ALIS. Dette er funn som stemmer godt overens med det teoretiske grunnlaget. Det fremkommer også som tydelig at det er avgjørende å ha en god intern informasjonsflyt for å kunne være kapabel til å dele med eksterne.

For å få til en effektiv utveksling av informasjonsdata mellom Forsvaret og leverandør sier teorien at integrasjon er viktig. Her fremkommer det en divergens mellom teori og praksis i Forsvaret som skyldes kravet til sikkerhet. Samlet sett fremkommer det at integrasjon anses viktig i Forsvaret, i tråd med teorien. Men analysen avdekker at det i liten grad eksisterer eller

brukes integrerte løsninger per i dag. Årsakene som trekkes frem er manglende sikkerhetsmessig godkjente løsninger. Konsekvensen blir at informasjonsdata pakkes og overføres manuelt, eller mottas og kvalitetssikres før de legges inn. Flere funn i studien peker på at dette er en meget ressurskrevende prosess som også tar tid, slik at tidskritisk informasjon ikke nødvendigvis kommer frem til ønsket tid. Det trekkes frem at dagens ordning er sikkerhetsmessig god, da en får god kontroll på hvem som har tilganger, men at den også hindrer Forsvaret i å hente ut effektiviseringsgevinstene som løsningene er designet for. Det anses som vesentlig å få på plass en godkjent MLS løsning for å i større grad hente ut gevinstene.

Informasjonsdata av tilstrekkelig kvalitet er i litteraturstudiet sett på som et premiss for at et ERP system skal kunne fungere. Funn i analysen understøtter dette og det trekkes frem som kritisk at Forsvaret må få økt kvaliteten på sine data. Det pågår arbeider med det, men det er ett stykke igjen før en har et tilfredsstillende nivå. Manglende datakvalitet settes også i sammenheng med muligheten for en god konfigurasjonskontroll på Forsvarets materiell. Det igjen påvirker informasjonssikkerheten og forvaltningen av understøttelsessystemene.

Sentralisering av data er kjernen i et ERP system for at de aktørene som har behov for informasjonen skal kunne få det samtidig og derigjennom redusere saksbehandlingstid og styrke muligheten for planlegging. Funn i studien viser en divergens mellom teori og praksis ved uttalt ønske om å sentralisere all informasjon og innføring av PBL kontrakter. PBL kontrakten kan medføre at masterdata blir liggende ett annet sted enn i SAP som eksempelvis ved ALIS kontrakten. Ett annet moment som trekkes frem er manglende kodifisering på materiell som skulle vært i SAP. Dette enten som følge av manglende kapasitet på saksbehandlere, eller som følge av endrede forutsetninger etter anskaffelse av materiellet. Et eksempel kan være at en skulle ha en vedlikeholdsavtale ved kontraktsinngåelse, men så endres det i ettertid til at en må ta vedlikeholdet selv. For forvaltning av understøttelsessystemer fremstår en sentralisering eller samling av data som gunstig, da det det gir bedre variantbegrensning og derigjennom også bedre systemsikkerhet.

Det viktigste forholdet ved en økt informasjonsdeling som følge av økt bruk av sivile aktører i forsyningskjeden er sikkerhet. Gjennomgående i hele analysen trekkes sikkerhet frem som det parameter som i størst grad påvirker om informasjonsdelingen er mulig og hvordan den kan utføres. Det trekkes også frem andre forhold som felles arkitektur og målbilde for å få mer

effektive og funksjonelle løsninger. Men når det kommer til stykket, er det NSM som må godkjenne løsningene. Flere respondenter påpeker et behov for en mer pragmatisk tilnærming der en kost nytte vurdering kan legges til grunn. I det legges at dersom gevinsten klart overstiger risikoen så bør en kanskje akseptere en operasjonell risiko. Det trekkes frem at problemstillingen i mange henseender er ung, og det festes lit til at F35 kampfly vil kunne fungere som en brekkstang for å få på plass godkjente MLS løsninger.

Det er på sikkerhet at Forsvarets som organisasjon ikke lenger har mulighet til å følge teorien i praksis. Sikkerheten setter per i dag en effektiv stopp for integrasjon og sømløs utveksling av informasjonsdata ut mot eksterne parter. Således kan en si at ett av de viktigste premissene for at gevinster som bedret datakvalitet, hurtighet i anskaffelser gjennom bruk av ERP, SCM, PBL eller integrasjon i forsyningskjeden ikke er tilstede i Forsvaret per i dag. Det er først når en får på plass en godkjent MLS løsning at en vil kunne få ønsket effekt. Det er dog viktig å huske at en slik løsning også vil kreve vesentlige ressurser i forvaltning og konfigurasjon opp mot den enkelte aktør det skal utveksles informasjon med.

7.2.2 Forskningsspørsmål 2

Det andre forskningsspørsmålet som er drøftet er:

> *Hvilke konsekvenser får økt sivilisering av logistikken med hensyn til forvaltningen av understøttelsessystemet?*

Det fremstår etter studien som tydelig at en økt sivilisering vil gi et økt behov for å styrke kompetansen og kapasiteten på merkantil side ved kontraktsinngåelser, da det er kontrakten som legger premissene for hva og hvordan informasjonsdelingen skal ivaretas. Det fremkommer også et behov for økt kompetanse og kapasitet på teknisk side for å ivareta systemforvaltningen. Nye systemer vil trenge ny kunnskap, samt at integrasjonsløsninger må utarbeides og forvaltes for det enkelte system.

Et moment som kommer tydelig frem ved analysen er konsekvensene dersom en ikke får på plass en effektiv løsning for informasjonsutveksling. En vil da, ved økt bruk av sivile aktører i forsyningskjeden, få en vesentlig økt ressursbruk for å utveksle informasjonsdata, ivareta understøttelsessystemene og informasjonssikkerheten. Dette som følge av at det blir manuelle

prosesser som ikke bare er meget ressurskrevende og tar mye tid, men også gir rom for menneskelig feil.

Ett annet funn er at det teoretiske rammeverket for forsyningskjeder, SCM, PBL og ERP løsninger ikke harmonerer med funn i studien. Dette ugyldiggjør ikke teoriene, men kan indikere at virkeområdet for teorien kanskje ikke er egnet for Forsvaret. Noe som underbygges av at all den tid premisset for effektiv informasjonsutveksling ikke er tilstede, vil gevinstpotensialet ved anvendelsen blir vesentlig redusert eller negativt. Men på den annen side, hva er alternativet? Som den ene respondenten så godt oppsummerte det:

> *Det er uunngåelig i fremtiden at vi ikke skal dele informasjon. Det blir mer og mer av det, så vi må bare bli bedre til å håndtere det, og vite hvordan vi skal tilnærme oss det!* (R6).

8 Konklusjon

Bakgrunnen for denne studien er å analysere noen av de konsekvensene en økt sivilisering av logistikken vil kunne medføre sett i et cyberperspektiv. Hva vil et økende behov for informasjonsutveksling mellom BEGRENSET plattform ved FISBasis og ugradert sivil side bety for Forsvaret?

Den overordnede problemstillingen for denne studien var:

> *Hvordan påvirker økt bruk av sivile aktører i forsyningskjeden informasjonsdelingen mellom Forsvaret og sivile leverandører?*

For å besvare problemstillingen ble det utarbeidet to forskningsspørsmål:

> F1: *Hvilke konsekvenser får økt sivilisering av forsyningskjeden for informasjonssikkerheten?*
>
> F2: *Hvilke konsekvenser får økt sivilisering av logistikken med hensyn til forvaltningen av understøttelsessystemet?*

Grunnlaget for det første forskningsspørsmålet var en antagelse om at sikkerhet ville ha en stor innvirkning på mulighetene for å dele informasjon, samtidig som sikkerhetsutfordringen er noe som skiller Forsvaret fra de beskrevne casene i litteraturen. Det andre forskningsspørsmålet hadde til hensikt å avdekke konsekvensene for understøttelsessystemene.

For å besvare forskningsspørsmålene ble det med utgangspunkt i teorien utarbeidet syv faktorer som analysen av gjennomførte intervjuer ble vurdert opp mot. Disse faktorene var henholdsvis: *Informasjonsdeling, integrasjon, datakvalitet, sentralisering av data, rammefaktorer, aktører og arkitektur* og *sikkerhet.*

Etter gjennomført analyse har studien kommet frem til følgende hovedfunn:

- Manglende MLS løsning medfører økt ressursbruk, og hindrer Forsvaret i å realisere gevinstpotensialet.
- Det er behov for å styrke merkantil side på kapasitet og kompetanse, da de kontraktfester premissene for hva og hvordan informasjonsdelingen skal ivaretas.
- Det er avgjørende med effektive løsninger for informasjonsdeling for å få ønskede resultater.

- Inngåelse av PBL kontrakter som for kampfly F35 øker kompleksiteten i systemene og motvirker samling av all informasjon i en felles løsning som ønsket.
- Det må på plass en mer enhetlig arkitektur og konsolidering av systemer på driftssiden der det er mulig.
- Endrede føringer fra anskaffelse til drift gir dårlig datakvalitet og medfører økt ressursbruk.

Ut fra hovedfunn er det rimelig å anta at en økt bruk av sivile aktører i forsyningskjeden vil, all den tid vi ikke har på plass en løsning for effektiv informasjonsutveksling, medføre en vesentlig økt ressursbruk. Dette er ressurser for å ivareta den manuelle prosessen med å utveksle informasjonsdata, understøttelsessystemene og informasjonssikkerheten.

Ett annet funn er at det teoretiske rammeverket for forsyningskjeder, SCM, PBL og ERP løsninger ikke harmonerer med funn i studien all den tid premisset for effektiv informasjonsutveksling ikke er tilstede. Dette ugyldiggjør ikke teoriene på noen måte, men anskueliggjør at gevinstpotensialet ved anvendelsen blir vesentlig redusert. Som følge av det er kanskje ikke økt sivilisering av forsyningskjeden vegen å gå ut fra et økonomisk perspektiv, men på den annen side, hva er alternativet?

Som den ene respondenten så godt oppsummerte det:

> *Det er uunngåelig i fremtiden at vi ikke skal dele informasjon. Det blir mer og mer av det, så vi må bare bli bedre til å håndtere det, og vite hvordan vi skal tilnærme oss det!* (R6)

8.1 Mulige utviklingstrekk og videre forskning

Denne studien har søkt å analysere hvilke konsekvenser en økt sivilisering av forsyningskjeden vil ha i et cyberperspektiv med henblikk til informasjonssikkerhet og forvaltning av understøttelsessystemene. Det antas at et økende behov for utveksling av informasjon nok er kommet for å bli, all den tid Forsvarets materiell, våpenplattformer og våpensystemer bare blir mer og mer avanserte. Det vil for en liten nasjon ikke være mulig å ha deler og kompetanse på alt i egen organisasjon så det tvinger seg frem andre og nye måter å ivareta materiellet på. Noe som også samsvarer med trenden i andre mindre nasjoner. I den forbindelse bør Forsvaret akseptere gjeldene rammevilkår og se fremover for å finne gode løsninger på hvordan en skal løse problemstillingene for å være best mulig rustet for fremtiden. Av forskning som vil bidra med å bygge ett bedre situasjonsbilde ville det vært interessant å se på blant annet:

- Utarbeide forslag til løsning for MLS. Denne studiens hovedfunn er at manglende MLS løsning trekkes frem som et viktig premiss for å få ønsket effekt i forsyningskjeden. En studie der en går inn på mulige tekniske løsninger og avklarer med NSM hva mulighetsvinduet er ville derfor være ett viktig bidrag til å finne en løsning på utfordringen.
- En tekniske studie som analyserer mulighetene for å få en godkjent "RFID" løsningen eller tilvarende. Som det fremkommer i denne studien vil en "RFID" løsning gi bedret datakvalitet og redusert ressursbruk for å holde kontroll på materiellet. En studie som tar for seg mulige løsninger fra et teknisk/sikkerhetsmessig perspektiv vil kunne gi viktig kunnskap og rede grunnen for en eventuell anskaffelse.
- Gjennomføre en tilsvarende studie som denne på en eller flere konkrete kontrakter for derigjennom styrke eller avkrefte funn i denne studien. Denne studien har sett på informasjonsdeling og konsekvensene for noen områder. Ved å gjennomføre en tilsvarende studie inn mot andre områder som for eksempel fregatt eller NH90 helikopter vil en kunne styrke eller avkrefte denne studiens funn..

8.2 Studiens styrker og svakheter

En svakhet ved denne studien er at empiri er hentet fra få respondenter, samt at de representerer forskjellige funksjoner og avdelinger. Det medfører at en kan gå glipp av nyanser innad i de enkelte miljø. Videre er snøballmetoden nyttet ved utvalg av respondenten, noe som også kan gi en feilaktig representasjon. Men det positive er at respondentene gjennomgående hadde lang fartstid innen fagområdet, noe som gir tyngde i uttalelsene. Videre dekker analysen over flere fagfelt, noe som gir større bredde i nyansene. Det at respondentene fremstår som samstemte i hva som anses å være den største utfordringen er også noe som styrker de funn som er gjort. Studien vil derav, om ikke å være generaliserbar, så kunne gi en god indikasjon på mulige komplikasjoner ved informasjonsdeling i virksomheter som har skjermingsverdig informasjon i lovens forstand.

En svakhet ved studien er at jeg ikke har lyktes i å få NSM på banen for å få deres syn på de sikkerhetsmessige utfordringene. Det ville kunne tilført studien en dypere forståelse av hvorfor ting er som det er og ikke bare konsekvensene av det.

Avslutningsvis reflekteres det over kompleksiteten ved informasjonsdeling mellom Forsvaret og sivile aktører. De enkelte faktorene henger tett sammen og det kan være en utfordring å skille de fra hverandre når en skal analysere hva som påvirker hva. Men det som er sikkert er at Forsvaret uansett vil måtte forholde seg til sivile aktører også i fremtiden. Så det må Forsvaret ta innover seg, og finne gode løsninger på hvordan de skal samhandle på en mest mulig hensiktsmessig måte innenfor gjeldene rammeverk.

Forkortelser

Forkortelse	Betydning
ALIS	Autonomic Logistics Information System, forvaltningssystem for F35 kampfly
B&S	Bertil og Steen, leverandør av verkstedtjenester og deler til kjøretøy
CIO	Chief Information Offiser
CKT	Cyberforsvarets kompetanse- og transformasjonsavdeling
Cluster	Sammenkobling av flere servere eller maskiner
CTO	Cyberforsvarets cybertjenester og operasjoner
CYFOR	Cyberforsvaret
DSF	Det sentrale folkeregister
DVU	Drift og videreutvikling
EDBVT	Elektronisk databehandlingssystem for verkstedtjenesten
ERP	Enterprise Resource Planning
F35	Nytt kampfly
FFA	Forsvarets FIF-administrasjon
FIF	Felles integrert forvaltningssystem
FISBasis	Forsvarets informasjonssystem Basis
FLO	Forsvarets logistikk organisasjon
FMA	Forsvarsmateriell
FRA	Forsvarets regnskapsavdeling
FSP	Forsvarets sikre plattform
HRM	Human Resource Management
IKT	Informasjons- og Kommunikasjonsteknologi
ISIL	Islamic State of Iraq and the Levant
LM	Lockheed Martin, leverandør av F35 kampfly
NBF	Nettverksbasert Forsvar
NSM	Nasjonal sikkerhetsmyndighet
PBL	Performance based logistics
PLCS	Programmable logic controllers
RAID	Teknologier for samkjøring av harddisker med sikte på økt ytelse og feiltoleranse først og fremst for lagring fra servere
RFID	Radio-frequency identification
ROS	Risiko og sårbarhetsanalyse
SAP	Systems, Applications, and Products in Data Processing, leverandør av

Forkortelse	Betydning
	Forsvarets ERP system
SCM	Supply change management
SOA	Service oriented architecture
UD 2-1	Utdanningsdirektiv 2-1, Forsvarets sikkerhetsbestemmelser for landmilitær virksomhet
XLS	eXceL Spreadsheet, filformat

Tabell 4 Forkortelser

Litteraturliste

773 Reglement for telling og avvikshåndtering av materiell i Forsvaret. (2010). *773 Reglement for telling og avvikshåndteringa av materiell i Forsvaret*. Oslo: Forsvarets logistikkorganisasjon.

1770 - Materiellregnskap. (2014). *1770 - Reglement om utøvelse av materiellregnskap*. Oslo: Forsvarets logistikkorganisasjon.

Anskaffelsesregelverk for forsvarssektoren (ARF). (2013). *Anskaffelsesregelverk for forsvarssektoren (ARF)*. Hentet fra https://lovdata.no/dokument/INS/forskrift/2013-10-25-1411/* - KAPITTEL_1.

Assistant Secretary of Defense Logistics & materiel readiness. (2016). *PBL Guidebook: A guide to developing performance-based arrangements (2016 release)*. acc.dau.mil: DoD Hentet fra https://acc.dau.mil/adl/en-US/706766/file/81707/PBL Guidebook Release March 2016 final.pdf.

Birkemo, G. A., & Kuran, C. H., A,. (2015). *Forsvarets forsyningsberedskap og avhengighet av sivile aktører [BEGRENSET]*. FFI-rapport 2015/00031. ikke publisert.

Borgen, L. (2013). Sivilisering av den operative logistikken - hvor går grensen? *Norsk Militært Tidsskrift, 2-2013*, 7.

De nasjonale forskningsetiske komiteene. (2016). Generelle forskningsetiske retningslinjer. Hentet 26. feb, 2016, fra https://www.etikkom.no/globalassets/documents/publikasjoner-som-pdf/fek_generelle_retningslinjer.pdf

Dey, I. (1993). *Qualitative data analysis : a user-friendly guide for social scientists*. London: Routledge.

Didriksen, H. (2008). *Informasjonssikkerhet i et ledelsesperspektiv - Utredning i fordypninsområdet Strategi og ledelse.* Siviløkonom, Norges Handelshøyskole, Bergen. Hentet fra http://hdl.handle.net/11250/170332

Direktoratet for samfunnssikkerhet og beredskap. (2014). *Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen*. dsb.no: Hentet fra http://www.dsbinfo.no/DSBno/2014/Tema/veiledertilhelhetligrisikoogsrbarhetsanalyseikommunen/.

Eilertsen, K.-E. B., Hestvik, R., & Nilsen, J. M. (1999). *Informasjonsinfrastruktur i Hæren IN-IS.* Studentoppgave, Universitetet i Oslo, Institutt for informatikk, Oslo. Hentet fra http://heim.ifi.uio.no/~rhestvik/inis/oblig3.pdf

Ekomloven. (2003). *Lov om elektronisk kommunikasjon,*. Hentet fra https://lovdata.no/dokument/NL/lov/2003-07-04-83 - KAPITTEL_1.

FDs cyberretningslinjer. (2014). *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i Forsvaret*.

Finnanger, T. (2012a). CS5565 Service- Oriented Architecture. Hentet fra https://www.academia.edu/24529735/CS5565_Service-Oriented_Architecture_Student_number_1039033

Finnanger, T. (2012b). *NATO Network Enabled Capability (NNEC) maturity improved by military ERP*. Masteroppgave, Brunel University West London, London. Hentet fra https://www.academia.edu/14737560/NATO_Network_Enabled_Capability_NNEC_maturity_improved_by_military_ERP

FOR-2001-07-01-744: Forskrift om informasjonssikkerhet. *Forskrift om informasjonssikkerhet,*. Hentet fra https://lovdata.no/dokument/SF/forskrift/2001-07-01-744.

Forsvaret. (2008). Joint Strike Fighter International Information Interoperability Initiative (JSF4I) [Unntatt Offentlighet]. Ikke publisert.

Forsvaret. (2015a). *Et forsvar i endring, Forsvarssjefens fagmilitære råd*. Forsvaret.no: Hentet fra https://forsvaret.no/fmr.
Forsvaret. (2015b). Forsvarssjefens fagmilitære råd 2015, Grunnlagsutredning - Rammevilkår for fremtidig logistikk - Bruk av ytelsesbaserte kontrakter (PBL) i Forsvaret - muligheter og konsekvenser [FORTROLIG]. DocuLive.
Forsvaret. (2016). Konseptuelt grunnlag P8154 Fleksible løsninger for sikker informasjonsutveksling [BEGRENSET]. DocuLive.
Forsvaret. (u.å.-a). Cyberforsvaret. Hentet 19.april, 2016, fra https://forsvaret.no/cyberforsvaret
Forsvaret. (u.å.-b). Felleskapasitetar. Hentet 19. april, 2016, fra https://forsvaret.no/forsvarsmateriell/om-forsvarsmateriell/felleskapasiteter
Forsvaret. (u.å.-c). IKT-kapasitetar. Hentet 19.april, 2016, fra https://forsvaret.no/forsvarsmateriell/om-forsvarsmateriell/ikt-kapasiteter
Forsvaret. (u.å.-d). Landkapasitetar. Hentet 19.april, 2016, fra https://forsvaret.no/forsvarsmateriell/om-forsvarsmateriell/landkapasiteter
Forsvaret. (u.å.-e). Luftkapasitetar. Hentet 19.april, 2016, fra https://forsvaret.no/forsvarsmateriell/om-forsvarsmateriell/luftkapasiteter
Forsvaret. (u.å.-f). Maritime kapasitetar. Hentet 19. april, 2016, fra https://forsvaret.no/forsvarsmateriell/om-forsvarsmateriell/maritime-kapasiteter
Forsvarets Logistikk Organisasjon. (2010). *1510-Bestemmelser for integrert logistikkstøtte, systemteknikk og informasjonshåndtering i Forsvaret*. Oslo: Forsvarets Logistikk Organisasjon,.
Forsvarsdepartementet. (2014). *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren "FDs cyberretningslinjer"*. Regjeringen.no.
Forsvarsdepartementet. (2016a). *Retningslinjer for Logistikkvirksomheten i forsvarssektoren*. DocuLive.
Forsvarsdepartementet. (2016b). *Retningslinjer for materiellforvaltningen i forsvarssektoren*. DocuLive.
Forsvarssjefen. (2013). *Forsvarets IKT strategi*. Forsvarsstaben.
Frøyland, J. (2015). *It-styring - visjon eller virkelighet - En Casestudie av ERP-systemet Felles Integrert Forvaltningssystem (FIF)*. Masteroppgave, Universitetet i Oslo, Oslo. Hentet fra http://urn.nb.no/URN:NBN:no-52813
Gulichsen, S., Reitan, J., & Listou, T. (2011). Prestasjonsbasert logistikk (PBL) - muligheter og utfordringer. Kjeller: Forsvarets forskningsinstitutt (FFI).
Heier, T. (2011). *Nytt landskap - nytt forsvar: norsk militærmakt 1990-2010*. Oslo: Abstrakt forl.
Håbjørg, G. E. (2015). *Prestasjonsbasert logistikk i Forsvaret. Faktorer som fremmer eller hemmer prestasjonsbasert logistikk i Forsvaret.* Masteroppgave, Forsvarets Høgskole, Oslo. Hentet fra http://hdl.handle.net/11250/297389
Iden, J. (2013). *Prosessledelse*. Bergen: Fagbokforl.
Information Assurance Directorate. (2008). *U.S. Government Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness Version 1.68*. Hentet fra https://www.niap-ccevs.org/pp/draft_pps/archived/pp_draft_mlos_mr_v1.68.pdf.
Instanes, A. (2013). *Bærekraftig logistikk Nansen klasse fregatter : En case-studie av logistikkstøttekonseptet.* Masteroppgave, Forsvarets høgskole, Oslo. Hentet fra http://hdl.handle.net/11250/100075
Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser? : innføring i samfunnsvitenskapelig metode* (3. utg. utg.). Oslo: Cappelen Damm akademisk.
Krokan, A. (2010). *Den digitale økonomien : om digitale tjenester, forretningsutvikling og forretningsmodeller i det digitale nettsamfunnet*. Oslo: Cappelen akademisk.
Kulp, S. C., Lee, H. L., & Ofek, E. (2004). Manufacturer Benefits from Information Integration with Retail Customers. *50*(4), 431-444. doi: 10.1287/mnsc.1030.0182

Lange, C. E. d. (2012). *SOA-prosjeter i praksis: Erfaringer fra en casestudie i Skatteetaten.* Masteroppgave, Universitetet i Agder, Kristiansand. Hentet fra https://brage.bibsys.no/xmlui/bitstream/handle/11250/136127/Christer Eikrem de Lange oppgave.pdf?sequence=1

Li, J., Sikora, R., Shaw, M. J., & Tan, G. W. (2006). A strategic analysis of inter organizational information sharing. *Decision Support Systems, 42* 251-266.

Lien, G., & Strand, K. R. (2011). Fremtidige utfordringer for Forsvarets logistikk - en trendanalyse *FFI-rapport*. Oslo: Forsvarets forskningsinstitutt.

Lund, M. C. E. (2014). *Prestasjonsbasert logistikk en strategisk kostnadsanalyse.* Masteroppgave, NTNU, Lund, Maren Cecilie Eid.

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

Melbo, H. K. (2006). Kritiske suksessfaktorer for ERP-systemer i offentlig sektor : en litteraturstudie.

Meld. St. 29. (2011-2012). *Samfunnsikkerhet*. Regjeringen.no: Justis og beredskapsdepartementet.

Meld. St. 37 (2014-2015). (2015). *Globale sikkerhetsutfordringer i utenrikspolitikken - Terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom*. Hentet fra https://www.regjeringen.no/contentassets/bdf4bd40d57d4dc79409de87419a2217/no/pdfs/stm201420150037000dddpdfs.pdf.

Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., & Zacharia, Z. G. (2001). Defining Supply Chain Management. *Journal of Business Logistics, 22*(2), 1-25.

Mohr, J., & Spekman, R. (1994). Characteristics of partnership success: Partnership attributes, communication behavior, and conflict resolution techniques. *Strategic Management Journal, 15*(2), 135-152. doi: 10.1002/smj.4250150205

Nasjonal Sikkerhetsmyndighet. (u.å.). Norges nasjonale cybersenter - Håndtering av dataangrep. Hentet 10. mai 2016, fra https://www.nsm.stat.no/norcert

Nilsen, T., & Steder, F. B. (2010). Effektive forsyningskjeder *FFI-rapport*. Oslo: Forsvarets forskningsinstitutt.

NOU 2015:13. (2015). *Digital sårbarhet - sikkert samfunn*. Regjeringen.no: Hentet fra https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf.

Oates, B. J. (2006). *Researching information systems and computing*. London: Sage Publications.

Persson, G., & Grønland, S. E. (2002). Supply chain management: en flerdisiplinær studie av integrerte forsyningskjeder (I. f. logistikk, Trans.) (Vol. 9). Oslo: Handelshøyskolen BI.

Pindyck, R. S., Rubinfeld, D. L., & Synnestvedt, T. (2013). *Introduksjon til mikroøkonomi*. Harlow: Pearson.

Politiets sikkerhetstjeneste. (2015). *Åpen trusselvurdering 2015*. Hentet fra http://www.pst.no/media/75480/PSTs_tv2015.pdf.

Porterfield, T. E. (2008). Diversity in Business-to-Business Information Exchange: An Empirical Analysis of Manufacturers and their Trading Partners. *Transportation Journal, 47*(3), 36-47.

Ringdal, K. (2013). *Enhet og mangfold : samfunnsvitenskapelig forskning og kvantitativ metode* (3. utg. utg.). Bergen: Fagbokforl.

Sikkerhetsloven. (1998). *Lov om forebyggende sikkerhetstjeneste*. Hentet fra https://lovdata.no/dokument/NL/lov/1998-03-20-10/KAPITTEL_1 - KAPITTEL_1.

Skoglund, P. (2012). Sourcing decisions for military logistics in Peace Support Operations: A case study of the Swedish armed forces.

Somers, T., M,, & Nelson, K. (2001). The impact og Critical Success Factors across the Stages of Enterprise Resource Planning Implementations. *Proceedings of the 34th Havaii International Conference on System Sciences - 2001*.

Strandskog, B. H. (2015). *Informasjonsdeling mellom kjøper og leverandør i varehandelsverdikjeder - Driver, forutsetninger og utfall.* Masteroppgave, NTNU, Trondheim. Hentet fra http://hdl.handle.net/11250/2353026

United States Government Accoutability Office. (2008). Impoved Analysis and Cost Data Needed to Evaluate the Cost-effectiveness of Perfomance based Logistics.

Vitasek, K., & Geary, S. (2008). *Performance-based logistics : a contractor's guide to life cycle product support management*: Supply Chain Visions.

Yin, R. K. (2012). *Applications of case study research* (3rd ed. utg.). Los Angeles: SAGE.

Zhao, X., Huo, B., Selen, W., & Yeung, J. H. Y. (2011). The impact of internal integration and relationship commitment on external integration. *Journal of Operations Management, 29*(1), 17-32.

Østre, S. (2014). Perfekte markeder – finnes de? Hentet fra http://hdl.handle.net/11250/191167

Aalders, R., & Hind, P. (2002). *The IT manager's survival guide*. Chichester: Wiley.

Aar, M. E. (2015). *Performance Based Logistics og kunde-leverandør- samarbeid. En casestudie av luftforsvarets transportfly C-130J.* Masteroppgave, Forsvarets Høgskole, Oslo. Hentet fra http://hdl.handle.net/11250/297649

Vedlegg A: Intervjuguide

Innledning
Dette er en individuell masteroppgave tatt ved Forsvarets høgskole.
Oppgaven ser på konsekvenser av økt sivilisering av forsyningskjeden i lys av informasjonsdeling.
Oppgaven er gjennomført som en case studie, hvor teori innen SCM/PBL og Forsvarets rammebetingelser for forvaltning av IKT-plattform gir den teoretisk bakteppet for oppgaven.

Kort om formalia
- Jeg ønsker et semi-strukturert en-til-en intervju med bruk av lydopptager og samtidig gjøre noen notater.
- Intervjuet vil bli transkribert, og det er mulig å få det tilsendt for gjennomlesing og kommentarer dersom du ønsker dette.
- Varigheten er estimert til 1-1,5 time
- Har jeg ditt samtykke for deltagelse? Underskrive samtykkeerklæring.
- Semi-strukturert intervju er valgt for å kunne være mer fleksibel i hvordan du ønsker å respondere på spørsmålene. Jeg ønsker at vi i løpet av samtalen/intervjuet kommer innom alle spørsmålene som jeg har notert. Dette er mitt ansvar.
- Hva som sies er "on the record" and for the "for the record".
- Anonymisering. Du vil ikke bli navngitt i oppgaven, men hvilken funksjon og avdeling du tilhører vil kunne bli brukt.
- Oppgaven er ugradert – ved eventuelle svar som er gradert må det gis beskjed om dette slik at lydbånd kan slåes av – undertegnede har klarering til hemmelig.
- Du kan når som helst trekke deg fra intervjuet.
- Studien er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste AS
- Har du noen spørsmål til ovennevnte eventuelt er det noe som er uklart?

Spørsmål

Bakgrunn – Erfaringer:
1. Hva er din nåværende stilling og funksjon?
2. Hvilken rolle eller tilknytting har du i forbindelse med informasjonsdeling i Forsvaret?
3. Kan du kort fortelle litt om din bakgrunn, og hvor lenge har du jobbet med fagområdet?

Informasjonsdeling
4. Kan du gi en beskrivelse av dagens løsning/løsninger for informasjonsutveksling mellom Forsvarets og sivile leverandører?
5. Finnes det godkjente løsninger for utveksling av informasjon mellom graderingsnivåer?
   -Ja
   -Nei
6. Hvis ja, hvordan gjennomføres den?
7. Går informasjonsutvekslingen begge veier?
8. Hvilke konsekvenser vil et økt behov for informasjonsutveksling kunne få?
   -informasjonssikkerhet?
   -forvaltning av system for informasjonsdeling?
   -variantbegrensning?
   -konfigurasjonskontroll?

-systemsikkerhet?
-annet?

9. Hvordan kvalitetssikres mottakers behandling av tildelt informasjon?
10. Synes du dette er tilstrekkelig?

Ved innføring av større kapasiteter som F35 og helikopter følger det med dedikerte forvaltningssystemer som ikke er integrert i dagens plattform.

11. Hvilke konsekvenser vil en slik utvikling ha dersom det blir flere tilsvarende løsninger?

Rammefaktorer

Forsvarssjefen ønsker å gå i retning av økt bruk av sivile aktører i forsyningskjeden. FLO ønsker å samle all materiellinformasjon i SAP.

12. Hvordan tror du dette vil påvirke forvaltningen av info- og infosys?
13. Er det motstridene krav/føringer/ønsker som er problematisk for forvaltningen av informasjonssystemene?
    -har du eksempler?
14. Er de gjeldende sikkerhetskrav til hinder for Forsvaret i å ta i bruk MLS?
15. Hvilke rammefaktorer mener du fremmer eller hemmer informasjonsdelingen?
16. Eventuelt hvilke sikkerhetskrav er de mest avgjørende?
17. Hvilken betydning vil det ha dersom nåværende sikkerhetskrav reduseres?
18. Er du kjent med om det jobbes med å endre disse kravene?
    -ja, hvem? Mandat? I hvilken retning jobber de?
    -nei
19. Hvem jobber med den videre utviklingen av modeller/arkitekturer/strategier innen informasjonsdeling i Forsvaret?
    a) Hvordan er progresjonen i arbeidet? Forklar.
    b) Hvilke deler av en eventuell løsning er det de jobber med?
20. Hvilke konsekvenser tror du en innføring av MLS vil få for Forsvaret som organisasjon?
    a. Sikkerhet, organisering, kompetanse, kapasitet, avhengighet, økonomi, annet?
21. Er informasjonsformatet (kodeverket) tilpasset forvaltningen av informasjonsdeling?
    -Konvertering mellom formater?
22. Hva mener du er de viktigste tiltakene for å bedre informasjonsutvekslingen mellom Forsvaret og leverandør?
23. Ser du noen graderingsrelaterte utfordringer?
    -Hvordan håndteres dette?

"alt" materiell skal kodifiseres og inn i SAP

24. Hvilke utfordringer og fordeler ser du i den sammenheng i forhold til informasjonsdeling og sårbarhet mtp informasjonssikkerhet?
25. Hvilke forvaltningsmessige utfordringer og fordeler ser du dersom materiell IKKE ligger i SAP?
26. Noe informasjon regnes som tidskritisk, Hva mener du er flaskehalsen for å få rett informasjon til rett sted og rett tid (Forsvaret – Leverandør)
27. Er det forskjell på hvilken informasjon dere deler med leverandørene?
28. Hvordan og hvor ofte deles denne informasjonen

Integrasjon

29. Hvilke føringer kjenner du til ifm deling av informasjon med leverandører?
30. Hvilke kategorier leverandører snakker vi om?

31. Hvordan og på hvilket nivå tas beslutningen om å dele informasjon med leverandører på?
32. Hvor unike er leverandørene som det tales om?
33. Er dette typiske leverandører eller er informasjonsdeling mer unntaket for noen av leverandørene?
34. Er det et felles IT-/ERP-system hos den enkelte leverandør, og hvem har i så fall tilgang?
35. Hvordan sikrer leverandørene at informasjon fra eller om Forsvaret behandles iht våre behov og krav til sikkerhet?
    a. Hvordan følges dette opp fra Forsvaret?

Avslutning

36. Er det andre implikasjoner/fordeler ved informasjonsdeling som burde belyses i studien?
37. Er det noe du ønsker å tilføre som vi ikke har snakket om?
38. Kan jeg sende oppfølgingsspørsmål på mail?

Ber om:

- Forslag til skrevne kilder
- Avslutte lydopptaket.

Avslutning

Takke for intervjuet.

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

Takke igjen!

Vedlegg B: Samtykkeerklæring

" Hvordan påvirker økt bruk av sivile aktører i forsyningskjeden informasjonsdelingen mellom Forsvaret og sivile leverandører?"

Bakgrunn og formål
Jeg skriver en masteroppgave ved Forsvarets høgskole. Forsvaret anbefaler i FMR å gå mot økt sivilisering av logistikken. Cyberforsvaret har i oppdrag å understøtte Forsvarets virksomhet med styringssystemer og IKT-infrastruktur. Oppgaven har til hensikt å belyse noen av de implikasjonene en økt sivilisering av logistikken vil kunne medføre sett i et cyberperspektiv. Hva betyr det for Cyberforsvaret at det er et økende behov for informasjonsdeling mellom gradert plattform (FISBasis B) og ut til sivile leverandører og visa versa. Er det ut fra gjeldende lover, regler og føringer mulig å understøtte Forsvarets virksomhet på en god måte? Studien er vitenskapelig og praktisk relevant da det det ikke er nyere studier på hvilke konsekvenser et slikt økt informasjonsdelingsbehov vil ha. Derimot er det mye litteratur som peker på at informasjonsdeling og integrasjon mellom kunde (Forsvaret) og leverandør er en forutsetning for en velfungerende forsyningskjede. Det er ikke gjennomført studie på informasjonsdeling i Norsk militær sammenheng tidligere, og hensikten med denne masteren er å bygge empiri rundt implikasjoner for informasjonsdeling.

Hva innebærer deltakelse i studien?
Med bakgrunn i din erfaring og kunnskap til informasjonsdeling ønsker jeg å intervjue deg. Det krever ingen forberedelse til intervjuet. Intervjuet antas å vare ca 1-1,5 time. Jeg vil ta opp samtalen for transkribering i etterkant, og ta notater. Dette for bedre å kunne analysere innholdet i etterkant.

Hva skjer med informasjonen om deg?
Alle personopplysninger vil bli behandlet fortrolig. Sitater og utsagn vil bli anonymisert i oppgaven. Prosjektet skal etter planen avsluttes i juni 2016. All informasjon innhentet i forbindelse med intervju vil bli slettet når sensur på oppgaven faller i juni 2016.
Studien er meldt inn og godkjent av Norsk Samfunnsvitenskapelig Datatjeneste (NSD) ved prosjekt nr. 46088.

Frivillig deltakelse
Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi noen grunn. Dersom du ønsker å delta eller har spørsmål til studien, ta kontakt med Anders Bestum

Samtykke til deltakelse i studien

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

---

(Signert av prosjektdeltaker, dato)

☐ Jeg samtykker til å delta i intervju