FFI-RAPPORT

21/00136

Bruk av skytjenester i Forsvaret

— muligheter og utfordringer

Ketil Lund
Frank Trethan Johnsen
Arild Bergh

Bruk av skytjenester i Forsvaret
– muligheter og utfordringer

Ketil Lund
Frank Trethan Johnsen
Arild Bergh

Forsvarets forskningsinstitutt (FFI) 19. januar 2021

Emneord
Digitalisering
Informasjonsinfrastruktur
Informasjonsteknologi
Systemarkitektur
Tjenesteorientert arkitektur

FFI-rapport
21/00136

Prosjektnummer
1431

Elektronisk ISBN
978-82-464-3320-2

Engelsk tittel
Military use of cloud services – possibilities and challenges

Godkjennere
Trude Hafsøe Bloebaum, *forskningsleder*
Jan Erik Voldhaug, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

I løpet av de siste 10 til 15 årene har skytjenester fått stor utbredelse, og svært mange organisasjoner har allerede tatt i bruk slike tjenester eller vurderer å gjøre det. Selve begrepet skytjeneste har også blitt godt etablert i samfunnet, og de fleste vil antakelig vil forbinde det med funksjoner eller tjenester som er tilgjengelige over Internett. Imidlertid er det mange ulike oppfatninger av hva skytjenester faktisk innebærer, teknologisk og forretningsmessig.

Denne rapporten har to formål. For det første ønsker vi å gi en innføring i teknologien bak skytjenester, og forklare hva skytjenester er. For det andre ser vi på hvordan Forsvaret skiller seg fra sivile organisasjoner når det gjelder bruk av IKT, og vi drøfter faktorer som må tas i betraktning ved innføring av skytjenester. For det andre formålet har vi konsentrert oss om den operative delen av Forsvarets IKT-bruk, da det primært er her de skiller seg fra sivil IKT-bruk.

For å sikre at vi dekker flest mulige relevante egenskaper ved Forsvaret har vi tatt utgangspunkt i et eksisterende rammeverk utviklet i Forsvaret for bruk i forbindelse med IKT-investeringer. Rammeverket består av et sett med syv såkalte løsningsegenskaper, som vi har sammenholdt med egenskapene som karakteriserer skytjenester.

Vi fant at de store leverandørene av skytjenester håndterer sikkerhet på en god måte, men skytjenester for gradert informasjon er en stor utfordring. Mye er fortsatt uavklart rundt hvordan sikkerhetsgraderte skybaserte informasjonssystemer skal kunne sikkerhetsgodkjennes. I den grad slik godkjenning blir mulig vil sikkerhetskravene sannsynligvis innebære at en del av stordriftsfordelene ved skytjenester går tapt. I tillegg kan nye muligheter for maskinbasert dataanalyse av store datamengder bidra til at informasjon som i utgangspunktet ikke er skjermingsverdig likevel blir det, eksempelvis dersom mye slik informasjon samles i en skytjeneste.

Videre kan en rekke faktorer bidra til å redusere tilgjengeligheten av skytjenester, eksempelvis uklare ansvarsforhold mellom leverandører, endrede politiske forhold i leverandørers hjemland og vilje og evne hos sivilt driftspersonell til å opprettholde tjenestekvaliteten i en krise- eller krigssituasjon. Det er også viktig, så langt som mulig, å unngå leverandørlåsing, slik at det er mulig å flytte tjenestene til en annen leverandør om behovet skulle oppstå.

Ved å utnytte distribusjon og redundans har skytjenester potensial til å sørge for robust IKT-understøttelse av Forsvarets operative oppgaver, også på taktisk nivå. Imidlertid vil dette sannsynligvis innebære høyere kostnader enn man vanligvis ser for skytjenester. Dersom Forsvaret ønsker å benytte skytjenester operativt, og spesielt kampnært, anbefaler vi at det først gjøres en grundig evaluering av hva som er mulig og realistisk å få til innenfor tekniske, juridiske, økonomiske og sikkerhetsmessige rammer.

Summary

During the last 10 to 15 years, the use of cloud services has increased considerably, and a large number of organizations have switched to such services, or is considering doing so. The term ‘cloud service’ itself has also become well established, and most people probably associate it with functions or services available over Internet. However, there are many different opinions on what cloud services really are, in terms of both technology and business.

This report has two purposes. In part, we want to give an introduction to cloud services in general, and explain what they are and involve. In addition, we look at how the Norwegian Armed Forces differs from civilian organizations with respect to using cloud services, and we discuss factors to consider when introducing such services. For the latter, we have focused on the operative side of military ICT, since this is where we find the biggest differences from civilian use of ICT.

To ensure that we cover sufficiently many characteristics of the Norwegian Armed Forces, we have used an existing framework, consisting of seven *solution properties*: information system security, availability, functionality, robustness, sustainability, interoperability, and flexibility. We have then compared this framework with the properties that characterize cloud services.

We found that the major suppliers of cloud services are very good at handling security, but much is still unclear when it comes to approval of cloud services for classified information. To the extent that such approval will be possible, some of the economies of scale-benefits of cloud services will probably be lost. In addition, factors such as new possibilities for big data analysis may require care risk analysis, even when storing unclassified information in the cloud.

A number of factors may negatively affect the availability of cloud services, such as unclear sharing of responsibilities between providers, changed political conditions in the provider’s home country, and will and ability of civilian operating personnel to maintain the quality of service in a crisis or war situation. Therefore, it is important to avoid vendor lock-in as far as possible, so that the possibility of switching provider of cloud services remains open.

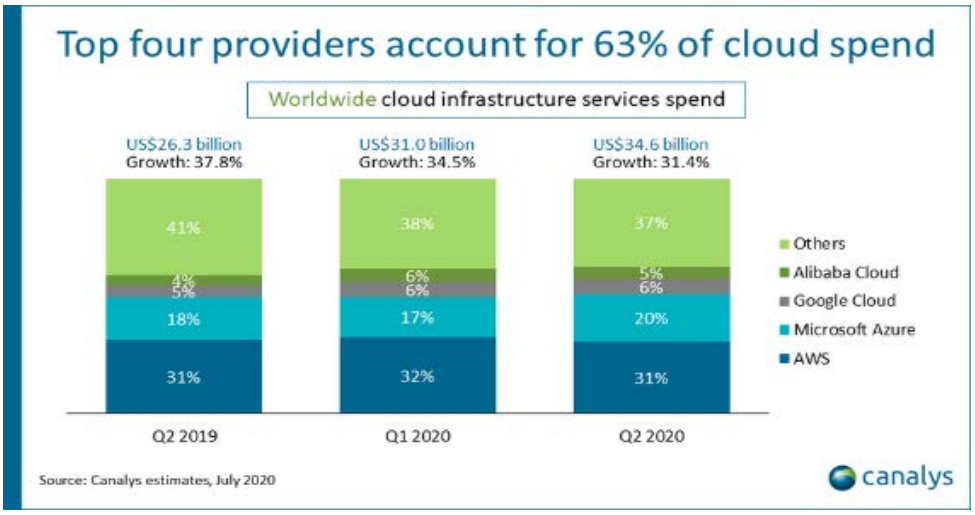
Using cloud services for operative tasks is possible, but as we show in this report, there are several factor to take into consideration. However, through effective use of distribution and redundancy, cloud services can be made very robust, but probably at a higher cost than is normally seen for cloud services. If the Norwegian Armed Forces wishes to use cloud services for operative tasks, and in particular, close to combat, we recommend to first perform a thorough evaluation on what is realistically possible within the constraints of technology, economy and security.

Innhold

1 Innledning

Det er noe uenighet om opprinnelsen til begrepet skytjeneste (*cloud computing*), men begrepet ble vanlig rundt årtusenskiftet. I dag vil antakelig de fleste forbinde det med funksjoner eller tjenester som er tilgjengelige over Internett. Noen av de første virkelig store tilbyderne av skytjenester var Amazon Web Services og Google med Gmail og Docs, som kom i 2006 (Birje, 2017).

Bruk av skytjenester har skutt i været de siste 10 årene. Per i dag er markedet verdt mer enn 210 milliarder dollar på verdensbasis, og prognoser fra Gartner (Gartner, 2020) estimerer at det skjer en økning på mer enn 40% i løpet av de neste to årene. Koronapandemien har også bidratt til en ytterligere vekst (Canalys, 2020). Per i dag er de fire største tilbyderne Amazon, Microsoft, Google og Alibaba, de to siste er dog adskillig mindre enn Amazon og Microsoft (se figur 1.1).



Figur 1.1 Analyse fra Canalys som viser prosentandel av inntekter fra skytjenester (Canalys, 2020).

Vi ser at bruken av skytjenester øker, også nasjonalt, inkludert i offentlig sektor. Eksempelvis sier Digitaliseringsrundskrivet (Kommunal- og moderniseringsdepartementet, 2019) følgende om digitalisering i offentlig sektor: «*Virksomheter som etablerer nye eller oppgraderer eksisterende fagsystemer eller digitale tjenester, eller endrer eller fornyer avtaler knyttet til drift, skal vurdere skytjenester på linje med andre løsninger. Når det ikke foreligger spesielle hindringer for å ta i bruk skytjenester, og slike tjenester gir den mest hensiktsmessige og kostnadseffektive løsningen, bør en velge slike tjenester*».

Det er derfor naturlig at man også i Forsvaret undersøker hva skytjenester eventuelt kan tilføre med hensyn til kostnadsbesparelser, økt operativ evne og økt robusthet. Forsvaret er så vidt i gang med å ta i bruk skytjenester, og gjennom programmet MAST (Militær Anvendelse av SkyTeknologi) skal anvendelsen utvides kraftig (Forsvarsmateriell, 2020).

Samtidig kan det se ut som skytjenester til en viss grad promoteres som «én størrelse passer alle»-løsning for svært forskjellige problemstillinger. Det er derfor viktig å forstå ulempene og utfordringene som ligger i teknologien. Det er ingen automatikk i at man sparer penger på å gå over til slike tjenester, og i forsvarssammenheng har man en del forhold og utfordringer som skiller seg fra resten av samfunnet, og som kan påvirke nytteverdien.

Denne rapporten er ment som en innføring i skytjenester og teknologien bak, primært for personell i forsvarssektoren som er interessert i bruk av skytjenester i operativ eller administrativ sammenheng, uten at de er teknologieksperter eller nødvendigvis jobber med informasjonsteknologi (IT) til vanlig. I tillegg setter vi bruken av skytjenester inn i en militær kontekst, og viser hvordan spesifikke militære problemstillinger og behov kan påvirke bruken av slike tjenester.

1.1 Problemstilling

En utfordring når skytjenester diskuteres er at det finnes ulike oppfatninger av begrepet, og at det legges ulike betydninger i det. Det kan gjøre det utfordrende å vurdere konsekvensene av å innføre skytjenester.

Det er også viktig å forstå begrensningene som ligger i bruk av skytjenester. Selv om Digitaliseringsrundskrivet (Kommunal- og moderniseringsdepartementet, 2019) pålegger virksomheter i offentlig sektor å vurdere skytjenester, ligger det også en reservasjon i pålegget. Denne sier at det ikke må foreligge spesielle hindringer for å ta i bruk skytjenester, og at slike tjenester må gi den mest hensiktsmessige og kostnadseffektive løsningen. I Forsvaret generelt, og på operativ side spesielt, er det en del forhold som gjør at denne reservasjonen er aktuell.

I denne rapporten vil vi derfor se nærmere på følgende spørsmål:

- Hva er egentlig skytjenester, og hvorfor er det nyttig i mange sammenhenger?
- Hvilke egenskaper og behov preger Forsvarets bruk av IKT?
- Hvilke avveininger bør gjøres i forbindelse med bruk av sky[1] i Forsvaret?

Disse spørsmålene drøftes i rapporten, og i konklusjonen oppsummerer vi svarene på spørsmålene gjennom å liste opp en del observasjoner og faktorer som vi mener det er viktig å ta hensyn til når bruk av skytjenester i operativ sammenheng vurderes.

Rapporten har som utgangspunkt at leseren kan lite eller ingenting om skytjenester. Det innebærer at noe av innholdet i kapittel 2, som forklarer skytjenester og teknologien bak, vil være kjent stoff for lesere med innsikt i denne typen tjenester. Kapittelet kan likevel være nyttig for

[1] I rapporten vil vi bruke begrepene skytjeneste og sky om hverandre.

disse, for å sikre at leseren og forfatterne har en noenlunde lik oppfatning av hva skytjenester innebærer, før rapporten går over til å se på mer militærspesifikke problemstillinger.

1.2 Metode

Et viktig premiss for denne rapporten er at Forsvaret har en del egenskaper og behov som gjør at organisasjonen skiller seg fra de fleste sivile organisasjoner med tanke på anvendelse av informasjons- og kommunikasjonsteknologi (IKT) generelt og skytjenester spesielt. Det er dermed ikke gitt at Forsvaret kan dra nytte av skytjenester på samme måte som en sivil organisasjon, og det er derfor viktig å se nærmere på hva disse egenskapene er og hvilken betydning de kan ha for bruk av sky i Forsvaret.

For å sikre at vi dekker flest mulige relevante egenskaper ved Forsvaret har vi sett behov for et rammeverk å ta utgangspunkt i. Vi har derfor benyttet et definert sett med *løsningsegenskaper*, som først ble introdusert i arbeidet med konseptuell løsning for taktisk ledelsessystem for landdomenet (Forsvarsdepartementet, 2017). Disse løsningsegenskapene ble der benyttet til å evaluere alternativer i alternativanalysen. De representerer målbare egenskaper ved IKT-systemer, og de kan knyttes til evnen til å understøtte effektiv ledelse av operasjoner i landdomenet.

Selv om disse løsningsegenskapene opprinnelig ble brukt innenfor landdomenet, mener vi de representerer et sett med egenskaper for IKT-systemer som er viktige for *hele* Forsvaret og som må tas i betraktning når innføring av skytjenester vurderes. Dette betyr ikke nødvendigvis at det ikke finnes ytterligere egenskaper som også er viktige for Forsvaret, men disse syv løsningsegenskapene utgjør et rammeverk som er utarbeidet og kjent i Forsvaret, og dermed et godt utgangspunkt.

De syv løsningsegenskapene er (Forsvarsdepartementet, 2017):

- **Informasjonssystemsikkerhet**: Evne til å unngå brudd i konfidensialitet, integritet, informasjonstilgjengelighet og autentisitet samt sikre ikke-fornektelse. I tillegg sikre at tjenester og informasjon er tilgjengelig til rett tid for personell som er viktige for gjennomføringen av en operasjon, slik at den kan foregå uhindret.

- **Tilgjengelighet**[2]: Evne til å yte avtalt funksjon eller oppfylle bestemte krav til stabilitet. Mobilitet og tempo som kreves i en militær operasjon må kunne understøttes, det samme gjelder den geografiske utstrekningen som en militær operasjon krever. I tillegg må klartider understøttes.

[2] I ny sikkerhetslov er tilgjengelighet sidestilt med konfidensialitet og integritet, og det kan derfor synes unødvendig med tilgjengelighet som en egen løsningsegenskap. I vårt arbeid har vi imidlertid valgt å forholde oss til løsningsegenskapene slik de opprinnelig ble definert. Dette har ingen betydning utover den rent tekstlige organiseringen i rapporten.

- **Funksjonalitet**: Evne til å utføre en oppgave eller funksjon, det vil si nødvendig funksjonalitet innenfor gjennomføringen av en operasjon.

- **Robusthet**: Evne til å tåle endringer og påkjenninger, både fiendepåførte og andre, både i det fysiske domenet, det elektromagnetiske domenet og cyberdomenet.

- **Opprettholdelse** (*sustainment*): Evne til å bevare ytelsesnivå og sikre kapasitetens eksistens over en ubestemt tidsperiode. Dette innebærer at nødvendige tjenester kan opprettholdes slik at igangsetting eller gjennomføring av en operasjon ikke hindres.

- **Interoperabilitet**: Evnen til å samhandle med andre for å nå et mål. Dette innebærer samvirke med overordnet, underordnede og sideordnede enheter, og med nødvendige allierte og sivile samarbeidspartnere.

- **Fleksibilitet**: Evne til dimensjonering og konfigurering til ulike situasjoner, inkludert ulike brukere, samarbeidspartnere, operasjonsmiljøer og -konsepter. I tillegg evne til videreutvikling ettersom forutsetninger og behov endrer seg.

I denne rapporten har vi prioritert å se på de delene av Forsvarets virksomhet som skiller seg fra resten av offentlig sektor. Vi har derfor primært sett på operativ virksomhet og håndtering av gradert informasjon. Vi har her benyttet IKT i en taktisk kommandoplass i landdomenet som et gjennomgående eksempel. Bakgrunnen for dette valget er at forfatterne har best kjennskap til IKT-bruk i landdomenet, samtidig som mange av utfordringene er felles for alle domener, eksempelvis håndtering av graderte data og begrensninger i nettverkenes overføringskapasitet.

Rapporten er videre basert på gjennomgang av relevant litteratur innen området. Fordi dette feltet fremdeles er i rask utvikling har vi i tillegg til akademiske artikler basert oss på en rekke andre kilder, som artikler fra teknologipublikasjoner, blogger fra teknologiselskaper og rapporter fra innføring av militære skytjenester i andre nasjoner.

1.3 Avgrensninger

Målet med rapporten er å gi en generell innføring i hva skytjenester er, og å gi leseren bedre forutsetninger for å forstå hensyn som må tas når slik teknologi vurderes for anvendelse i Forsvaret. Rapporten gir ikke konkrete anbefalinger med hensyn til hvor i Forsvaret slik teknologi bør anvendes, og den går heller ikke i dybden i særlig grad, innenfor noen av temaene. Dette er dels for å kunne holde rapporten ugradert, og dels for å holde rapporten på et nivå som ikke krever dyp teknologisk kunnskap hos leseren.

Videre har vi valgt å konsentrere oss om forsvarsspesifikke problemstillinger. Det er gjort mye arbeid innenfor temaet skytjenester i offentlig sektor generelt, og vi anser det derfor ikke som nødvendig å berøre dette temaet i særlig grad i denne rapporten. For mer informasjon om bruk av skytjenester i offentlig sektor kan vi for eksempel henvise til Nasjonal strategi for bruk av skytenester (Kommunal- og moderniseringsdepartementet, 2016), Digitaliseringsrundskrivet

(Kommunal- og moderniseringsdepartementet, 2019), Overordnede arkitekturprinsipper for digitalisering av offentlig sektor (Digitaliseringsdirektoratet, 2020) og Kartlegging av hindringer i regelverk for bruk av skytjenester (Kommunal-og moderniseringsdepartementet, 2015).

Bruk av skytjenester er et stort og komplekst område, spesielt for en såpass stor aktør som Forsvaret. Ambisjonen med denne rapporten har derfor vært å identifisere faktorer som kan ha betydning for valg som gjøres rundt bruk av skytjenester i Forsvaret.

1.4 Leserveiledning

I dette kapittelet har vi presentert rapportens forskningsmessige bakgrunn – hvilke problemstillinger diskuteres, forskningsmetodene som benyttes og avgrensningene som er foretatt. Kapittel 2 forklarer i detalj hva en skytjeneste er, hvilke egenskaper den må inneha for å være en skytjeneste, og egenskaper mange forbinder med skytjenester utover kjerneegenskapene. Deretter beskrives status for bruk av skytjenester i Forsvaret i dag i kapittel 3. Bakgrunnsinformasjonen fra kapitlene 2 og 3 trekkes sammen i kapittel 4 som diskuterer avveiningene som Forsvaret bør foreta når bruk av skytjenester vurderes. Rapporten oppsummerer observasjoner og anbefalinger i kapittel 5.

Siden vi har valgt å benytte norske begreper der slike finnes, har vi inkludert en norsk–engelsk ordliste for disse begrepene i vedlegg A. I vedlegg B forklarer vi de ulike byggesteinene som inngår i skytjenester, dette innebærer for en stor del helt grunnleggende begreper innen IKT. Til slutt gir vi en innføring i ulike typer av ressursoppdeling i vedlegg C.

2 Skytjenester – definisjon og egenskaper

I IKT-sammenheng brukes ofte begrepet *tjeneste* om funksjoner som leveres av programvare, og det finnes en formell definisjon av begrepet (OASIS, 2012). Det finnes imidlertid ikke en tilsvarende entydig definisjon av hva skytjenester er, heller ikke et fast sett med standarder som slike tjenester må møte. I dette kapittelet gir vi derfor en definisjon basert på et sett med egenskaper som skytjenester må ha. I tillegg beskrives de ulike typene av skytjenester, og vi forklarer de viktigste tjenestemodellene som finnes.

Det er viktig å skille mellom skytjenester som forretningsmodell og skytjenester som teknologi. Som forretningsmodell handler skytjenester om hvem som har ansvaret for å levere tjenester, enten det er organisasjonen som bruker skytjenestene eller det er en ekstern leverandør. Dette er nærmere beskrevet i kapittel 2.3.

For å definere begrepet skytjeneste fra et teknologisk ståsted har vi i stor grad basert oss på The National Institute of Standards (NIST) Definition of Cloud Computing (NIST, 2011), og lagt deres sett med egenskaper til grunn for å definere skytjenester gjennom egenskaper de må eller bør ha. Dette er for øvrig tilsvarende det som er gjort i «Nasjonal strategi for bruk av skytenester» (Kommunal- og moderniseringsdepartementet, 2016). Disse egenskapene er beskrevet i kapittel 2.1 og 2.2, og vi tar først for oss egenskaper som en tjeneste *må* ha for å kunne kalles en skytjeneste. Deretter beskriver vi en del egenskaper som er utbredte, men ikke strengt nødvendige.

2.1 Essensielle egenskaper

Egenskapene i tabell 2.1 finnes i alle skytjenester, hvis én eller flere av disse egenskapene mangler er det ikke en skytjeneste.

Tabell 2.1 Essensielle egenskaper som må oppfylles for at man skal kalle noe for en skytjeneste.

Egenskap	Kommentar
Generell tilgang via nettverk	Maskinvaren som skytjenesten benytter er ikke lokalisert der brukerne er, nettverkstilgang er derfor eneste måte å benytte skytjenester på. Interaksjon med tjenester i skyen skjer gjennom standardmekanismer, gjerne plattformuavhengige, med støtte for ulike klienter som PC-er og nettbrett.
Selvbetjent oppsett	Kunden kan sette opp og administrere tilgang til tjenestene de ønsker å bruke uten å involvere representanter fra leverandøren av tjenestene. Dette kan være alt fra å etablere en brukerkonto og betale for bruk av et online regneark til å angi hvor mye lagringsplass hver ansatt i et firma skal ha tilgang til.
Samling av ressurser	Selv om ressursene (prosessering, lagring, nettverk, osv.) bak skytjenester gjerne består av tusenvis av maskiner, fremstår de for kunden som samlet i ett «punkt» (grensesnitt). Dette oppnås vanligvis med *virtualisering*, som innebærer at de fysiske maskinene skjules bak et lag av virtuell maskinvare, det vil si en programvarebasert versjon av en datamaskin. Hvor mye av faktiske ressurser som settes inn bak hver enkelt virtuelle maskin kan varieres fortløpende. Kombinert med et stort antall brukere av datasenteret (såkalt flerbruk) gjør dette at ressursene i datasenteret kan utnyttes

	svært effektivt, fordi de hele tiden kan flyttes dit det er behov for dem. For mer informasjon om virtualisering, se vedlegg C.
Fleksibel og transparent dekning av ressursbehov	I motsetning til lokal, fysisk infrastruktur er skytjenester fleksible med hensyn til hvor mye man bruker av en ressurs. I perioder med større behov for en ressurs (f.eks. prosesseringskraft) kan man kjøpe tilgang til mer ressurser, for så å benytte mindre (og betale mindre) når behovet reduseres. Nødvendige endringer i ressurstilgjengelighet skjer normalt automatisk og umiddelbart.
Ressursbruk måles	Hver kundes forbruk av ulike ressurser (lagring, prosesseringskraft, osv.) måles kontinuerlig. Denne informasjonen benyttes eksempelvis til å ta betalt etter forbruk, ivareta sikkerhetshensyn og tildele mer ressurser.

2.2 Vanlige egenskaper

I tillegg til de essensielle egenskapene beskrevet i kapittel 2.1, finnes det et sett med egenskaper som man ofte finner hos skytjenester. Selv om disse egenskapene ikke er unike for skytjenester, så er de med på å differensiere skytjenester fra andre nettverkstjenester, for eksempel interne/ lokale filtjenere i en organisasjon. I tabell 2.2 har vi organisert disse i en tabell som viser sammenhengen mellom de forskjellige egenskapene.

Tabell 2.2 Vanlige egenskaper ved skytjenester.

Egenskap	Kommentar
Tjenesteorientering	Tradisjonelt vil en organisasjon kjøpe maskin- eller programvare, f.eks. en filtjener, som brukes internt i organisasjonen. I en skytjeneste kjøper man ikke maskin- eller programvare, men *tjenester* som gir den ønskede funksjonaliteten. Den fysiske filtjeneren i eksempelet over blir erstattet med tilgang til egen lagringsplass på en større filtjener, og man trenger ikke vite hvor dataene fysisk er lagret.
Ressursoppdeling	De fysiske ressursene deles mellom mange brukere, og denne delingen oppnås normalt gjennom teknologier som virtualisering og konteinere (se vedlegg C). Denne oppdelingen er det som gir fleksibilitet med hensyn til hva og hvor mye man gjør på samme maskinvare.

Homogenitet	Identiske tjenester kan tilbys til mange kunder eller brukere samtidig, det er med andre ord ikke skreddersydde tjenester for en enkelt bruker som tilbys. Merk at homogenitet her referer til tjenester hos én tilbyder, det betyr ikke at forskjellige skytjenesteleverandører nødvendigvis tilbyr identiske tjenester.

Tjenesteorientering, ressursoppdeling og homogenitet kombineres med:

Geografisk distribusjon av ressurser/data	Fordi tilgang til skytjenester skjer via nettverk kan disse tjenestene komme fra maskinvare i en hvilken som helst lokasjon med nettverks-tilgang. Tilsvarende kan brukerne av tjenestene være lokalisert hvor som helst så lenge de har nettverkstilgang.

Dette gir muligheten for:

Massiv skala	Offentlige nettskyer, som Microsoft Azure, har datasentre i mange land. Et datasenter ligger på en fysisk lokasjon hvor tusenvis av tjenere er installert, og hver tjener kan benyttes av mange kunder samtidig. Det er denne massive skalaen som gir den enkelte kunde illusjonen av å ha ubegrenset med ressurser tilgjengelig, ved at ressursene i et datasenter fordeles dynamisk mellom brukerne, og at prosessering og data kan flyttes dynamisk mellom sentre, ettersom hvor det er ledig kapasitet.

De ovenstående egenskapene kan benyttes for:

Motstandsdyktig data-behandling	Motstandsdyktig databehandling referer til måten skytjenester håndterer feil som oppstår i daglig bruk. Den vanligste formen for motstands-dyktighet består i å ha kopier av maskinvare som inngår i en automatisk form for *failover* (innsjalting av redundant kapasitet eller standby-ressurser for å kompensere for oppdukkende feil). Videre benytter man gjerne programvareløsninger i tillegg, som sørger for lastbalansering og distribuerer tjenester på tvers av fysiske steder.
Avansert sikkerhet	Skyleverandøren har spesialisert seg på datasenterdrift og har god kontroll på administrasjon, drift og sikkerhet. Dette er en av de store fordelene med å ta i bruk skytjenester, nemlig den iboende antakelsen om at leverandørens sikkerhetspersonell best ivaretar sikkerheten for den infrastruktur, plattform eller programvare de leverer. For små organisasjoner er dette sant, da de ikke vil ha ressurser til å bygge opp

	like bred sikkerhetskompetanse som en stor leverandør. For andre, eksempelvis Forsvaret, vil man også besitte en del egen sikkerhetskompetanse. Det er da viktig at de behov man har formidles klart overfor en eventuell leverandør, slik at de kan ivaretas.
Lav pris	For mange er forventingen om kostnadsbesparelser den største antatte fordelen ved bruk av skytjenester. Der hvor skyleverandørene tilbyr lave priser (for kunden) er dette mulig gjennom svært effektiv samordning av tusenvis av kunders IKT-behov gjennom deling av ressurser.

I mange tilfeller vil en styrke ved skytjenester være at en ekstern leverandør av tjenestene tar seg av hele eller deler av programvaren og infrastrukturen og lanserer regelmessige programvareoppdateringer – inkludert sikkerhetsoppdateringer – slik at organisasjonen ikke trenger å vedlikeholde systemet selv.

Dette betyr at organisasjonen kan fokusere på å rendyrke sine tjenester, fremfor å måtte bruke ressurser på driftsmessige forhold, og gjør at spesielt små organisasjoner med lite kapital likevel kan klare å lansere tjenester og produkter for et stort marked. For store organisasjoner innebærer dette en mulighet for kostnadsbesparelse i forhold til tidligere driftsmodeller, da en kan kjøpe tjenester og ressurser fortløpende etter behov, fremfor å eie, drifte og forvalte hele infrastrukturen selv. Generelt vil det å ta i bruk skytjenester innebærer reduserte investeringskostnader (gjerne kalt *capital expenditure* – CAPEX). Man kjøper fortløpende de tjenestene man trenger, og må dermed primært forholde seg til driftskostnader (*operational expenditure – OPEX)*, altså de løpende kostnadene fra den bruken man faktisk har.

Ett eksempel på fordelen med overgangen fra CAPEX til OPEX er Telenors satsing på strømmetjenesten Comoyo. Denne tjenesten ble lagt ned i 2013, men fordi den var basert på skytjenester fra Amazon unngikk Telenor tap på investeringer i infrastruktur som ikke lenger ble brukt (Kommunal- og moderniseringsdepartementet, 2016).

Nettopp slike kostnadsbesparelser er gjerne ett av de viktigste salgsargumentene for å ta i bruk skytjenester. Et mer nyansert bilde er at det i det minste blir et *annet* kostnadsbilde enn det man normalt har når alt driftes internt i en organisasjon, på egen maskinvare. Det å analysere kostnader og besparelser i forkant av en overgang til skytjenester kan imidlertid være utfordrende. Ofte er prismodellene komplekse, og det kan være utfordrende å sammenlikne to ulike leverandører direkte.

For større satsinger kan bildet være såpass komplisert at det er vanskelig i det hele tatt å gi et fornuftig prisestimat tidlig i prosessen. Et eksempel her er Direktoratet for forvaltning og økonomistyring (DFØ) som nylig har utlyst en rammeavtale om kjøp av skytjenester. DFØ har forsøkt å estimere, men har kommet til at det ikke er enkelt å kostnadsberegne slike anskaffelser, og estimerer derfor at kontrakten vil være verdt mellom 10 og 100 millioner kroner (Seglsten, 2020).

2.3 Skytyper

Som nevnt innledningsvis i dette kapittelet kan man skille mellom skytjenester som forretningsmodell og skytjenester som teknologi. Når organisasjoner ønsker å gå over til skytjenester kan motivasjonen i noen tilfeller være at man ønsker å sette ut ansvaret for driften av organisasjonens datatjenester, og ikke nødvendigvis behovet for skytjenester som sådan. Man ønsker altså å gå over til en annen forretningsmodell for datatjenestene organisasjonen benytter.

En inndeling i ulike *skytyper* er det som best indikerer hvilken forretningsmodell som benyttes. Tabell 2.3 viser de viktigste typene. Merk at for alle de ulike typene er teknologien bak tjenestene den samme, det som skiller de ulike typene er først og fremst hvor mange andre (og hva slags) kunder man deler dataressursene med, og til en viss grad hvem som har ansvar for å levere tjenestene. Fordi det ikke nødvendigvis er et én-til-én forhold mellom skytype og hvem som har ansvaret for å levere skytjenestene, blir skytypen likevel kun en indikasjon på forretningsmodellen.

Tabell 2.3 De viktigste skytypene.

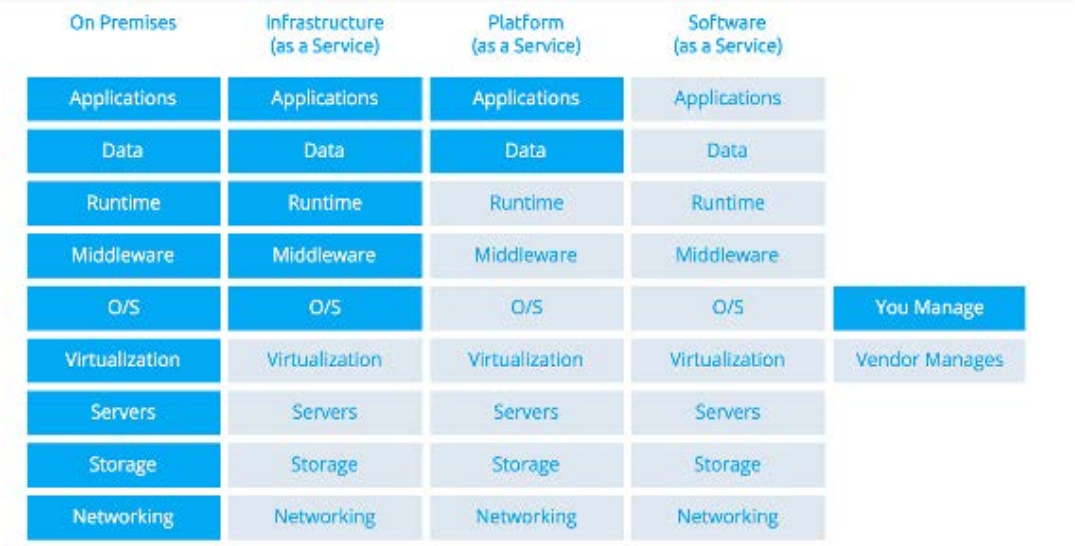
Skytype	Kommentar
Offentlig sky (*public cloud*)	Dette tjenester som er åpne for alle, og som for eksempel Google, Amazon og Microsoft tilbyr. Mange har benyttet tjenester som Google Mail eller Microsoft Office 365, som er representanter for denne typen tjenester. Fordi tjenestene i en offentlig sky benyttes av svært mange, oppnår tilbyderen stordriftsfordeler som gjør det mulig å holde en lav pris på tjenestene som tilbys.
Privat sky (*private cloud*)	Privat sky benytter tilsvarende teknologi som offentlige skyer, men dataressursene som leverer skytjenestene kjører på organisasjonens egen infrastruktur. Det finnes også en tilnærming kalt virtuell privat sky (*virtual private cloud*) der man får levert tjenestene fra en offentlig sky, men uten flerbruk på den fysiske tjeneren som leverer tjenestene. Således kan virtuell privat sky forstås som at den er administrert av et eksternt selskap, mens privat sky administreres internt i en organisasjon. En siste variant av privat sky har det fysiske datasenteret plassert hos kunden, mens en ekstern leverandør har ansvaret for driften av det. Eksempler på dette er AWS Outposts fra Amazon og Azure Stack fra Microsoft.

	I en privat sky blir det fysiske datasenteret som leverer tjenestene kun benyttet av én kunde. Dermed forsvinner mange av stordriftsfordelene man har i en offentlig sky, og kostnadene blir dermed høyere.
Hybride skyer (*hybrid cloud*)	En hybrid sky er en blanding av offentlig og privat sky. Eksempelvis kan sensitive data legges i en privat sky, mens øvrige data legges i en offentlig sky, for på den måten å oppnå noe større kostnadsbesparelser enn bruk av en ren privat sky vil kunne gi.
Gruppesky (*community cloud*)	Her er infrastrukturen delt mellom flere organisasjoner som har felles behov eller interesser. Ansvaret for administrasjon og drift av en slik gruppesky kan ligge hos de deltakende kundene eller hos en tredjepart. Kostnadene for infrastrukturen er spredt over færre brukere enn ved offentlig sky, og kostnadsbesparelsene er derfor gjerne også noe mindre.

2.4 Tjenestemodeller

Mens de ulike skytypene sier noe om hvem som har ansvar for leveransen av skytjenester, vil tjenestemodellen beskrive den «vertikale» ansvarsfordelingen mellom skyleverandør og kunde i noe mer detalj. Vi tar her utgangspunkt i en lagdelt modell, med fysiske ressurser (nettverk, lagring og prosessorer) nederst og applikasjoner på toppen.

Normalt skiller vi her mellom tre ulike tjenestemodeller: *infrastruktur som en tjeneste* (IaaS), *plattform som en tjeneste* (PaaS) og *programvare som en tjeneste* (SaaS). SaaS overlater mest ansvar til skyleverandøren, IaaS overlater mest til kunden, og PaaS ligger et sted imellom. Alle de tre modellene er nærmere beskrevet nedenfor, og illustreres i figur 2.1. I figuren er det også indikert hvem som har ansvaret for de ulike lagene – kunden eller leverandøren.



*Figur 2.1 IaaS, PaaS og SaaS sammenliknet med å eie infrastrukturen selv (såkalt «*On premises*») (ValueBlue, u.d.).*

2.4.1 Infrastruktur som en tjeneste (Infrastructure as a Service – IaaS)

IaaS er den mest grunnleggende tjenestemodellen. Den innebærer at leverandøren har ansvar for infrastrukturen (all nødvendig maskinvare for prosessering, lagring, nettverk) og tilbyr et sett virtualiserte ressurser til kunden. Leverandøren har gjerne mulighet for flere ulike operativsystemer (OS) som kan benyttes på deres IaaS, for eksempel Windows eller én eller flere varianter av Linux. I IaaS-modellen må kunden selv vedlikeholde OS-et (sikkerhetsoppdateringer m.m.) og programvaren som er installert på OS-et. Denne tjenestemodellen er typisk forbundet med lavere løpende kostnader hos leverandøren, men kunden må beregne kostnader for vedlikehold av OS og egne programmer på den infrastrukturen som tilbys. Eksempler på leverandører av IaaS er Amazon AWS, Microsoft Azure, Rackspace, GoGrid og Digital Ocean.

Dersom kunden behøver full kontroll over programvare og operativsystem vil dette være den beste modellen. Eksempelvis benytter Netflix IaaS fra Amazon for å distribuere video til kunder over hele verden. Netflix peker på stabilitet, skalerbarhet og kostnadsbesparelser som motivasjonen for å ta i bruk nettskyen (Donnely, 2016).

For en organisasjon som ønsker å ta i bruk skytjenester, men samtidig beholde eksisterende programvare, kan IaaS og såkalt «*lift and shift*» (IBM, 2019) være et alternativ. Da gjør man i praksis alt som før, bortsett fra at serveren befinner seg i nettskyen i stedet for lokalt. Et eksempel på dette er Circle K, som i 2018 flyttet hele sin databaseinstallasjon ut i skyen

(Vaughan, 2019). *Lift and shift* innebærer med andre ord å flytte et program eller et helt informasjonssystem med tilhørende data, uendret over til en virtualiseringsplattform[3].

Fordelen med denne fremgangsmåten er at det er relativt enkelt og billig å gjennomføre, samt at det i noen tilfeller kan være nødvendig fordi det ikke finnes SaaS-programvare som kan gjøre den samme jobben. I tillegg kan *lift and shift* gjøre det mulig å tilføre en eksisterende applikasjon flere ressurser (f.eks. mer prosesseringskraft) uten å måtte investere i ny maskinvare, som potensielt kan ha gått ut av produksjon.

2.4.2 Plattform som en tjeneste (Platform as a Service – PaaS)

Denne tjenestemodellen gir kunden tilgang til et operativsystem som leverandøren har ansvaret for, og som kunden kan kjøre egen programvare på. Utviklere bruker det gjerne for å kunne tilgjengeliggjøre applikasjoner uten å måtte investere i dyr infrastruktur.

Med PaaS-modellen har leverandøren driftsansvaret for infrastrukturen (slik som for IaaS) og for OS-et, slik at det som tilbys til kunden er en forvaltet plattform. Leverandøren er ansvarlig for å tilby et stabilt og sikkert OS på en stabil infrastruktur. Sammenliknet med IaaS er altså ansvaret for OS-et flyttet over fra kunden til leverandøren, og kunden får dermed noe redusert driftsansvar og trenger ikke bekymre seg for om det er nok maskinvareressurser (prosessorkraft, minne og lagring) tilgjengelig.

Eksempler på leverandører av PaaS er Google App Engine, Microsoft Azure[4], Heroku og OpenStack. Et eksempel på bruk av PaaS er Salesforce lightning, hvor kunder som bruker Salesforce sin kunderelasjonsapplikasjon kan tilpasse og utvide programvaren etter eget behov, samtidig som den kjører på en plattform i skyen.

2.4.3 Programvare som en tjeneste (Software as a Service – SaaS)

Privatpersoner som bruker skytjenester vil normal møte denne tjenestemodellen. Her har man tilgang til kjørende programvare som utfører en (type) oppgave eller tjeneste, og ofte brukes programvaren gjennom en nettleser. Noen av de tjenestene som tilbys i form av SaaS kunne ikke eksistert uten et åpent nettverk som Internett, for eksempel gratis videokonferanseverktøy og nettbaserte tekstbehandlere.

Med SaaS har leverandøren ansvaret for drift og vedlikehold av applikasjonen, i tillegg til OS og maskinvare. Dette er derfor den tjenestemodellen som er minst arbeidskrevende for kunden med tanke på vedlikehold. Det er derfor en populær modell ikke bare for hjemmebrukeren, men også for både små og store organisasjoner. Her tilbys spesifikk, forvaltet programvare, mens

[3] Normalt vil man benytte IaaS i forbindelse med *lift and shift*, og flytte applikasjonen med tilhørende operativsystem over til en virtualiserings- eller skyplattform. I noen tilfeller kan man imidlertid nøye seg med å flytte kun applikasjonen over, dvs. en PaaS-løsning, dersom det allerede finnes virtuelle plattformer som applikasjonen kan kjøres på.
[4] Microsoft Azure leverer både IaaS og PaaS.

plattformen den kjører på er skjult. Kunden trenger i utgangspunktet bare å spesifisere programvaren som ønskes, og så skal leverandøren håndtere resten.

Eksempler på SaaS er Microsoft Office 365, Google Docs og Adobe Creative Cloud. Der man tidligere kjøpte slik programvare og installerte den på egen PC, kjøper man funksjonaliteten som tjenester på Internett, gjerne organisert i form av et abonnement der man betaler fortløpende for bruken. Alt som har med oppdatering, vedlikehold og sikkerhet å gjøre håndteres av tjenesteleverandøren.

Det finnes også eksempler på SaaS som tilbys gratis til kundene, slik som mange av tjenestene for e-post som finnes på Internett i dag (f.eks. Gmail og Hotmail). I stedet for å kreve betaling av kunden direkte, finansieres tjenestene indirekte ved å indeksere kundenes e-post, bygge kundeprofiler og så auksjonere ut tilgang til å vise målrettet reklame basert på disse profilene.

I noen tilfeller ser man at SaaS og tradisjonell (lokalt installert) programvare brukes sammen. Et eksempel på dette er bruk av e-post i Microsoft Office. Det tradisjonelle oppsettet her er Outlook-klienter på brukernes PC-er som kommuniserer med en e-posttjener i form av Microsoft Exchange installert på organisasjonens tjenermaskiner.

Ved en overgang til Microsoft Office 365 kan brukerne fortsette å benytte den lokalt installerte Outlook-klienten, men den vil nå snakke med en skybasert e-posttjener. I dette tilfellet er e-posttjeneren SaaS, mens klientprogramvaren ikke er det. Hvis derimot brukeren benytter webmail-løsningen til Office 365, så er både e-postklienten og -tjeneren SaaS.

Det er også viktig å være klar over at selv om leverandøren har ansvar for drift og vedlikehold, så kan det fortsatt falle en del administrasjonsoppgaver på kunden. Eksempelvis vil det for en stor Office365-kunde kreves at kunden håndterer områder som autorisasjon av brukere, brukerstøtte, håndtering av fellespostbokser, administrasjon av klientutstyr og logging av aktivitet. Dette administrasjonsaspektet vil imidlertid være det samme, uavhengig av om man kjører på egen maskinvare eller benytter SaaS fra en ekstern leverandør.

Det kan også innebære merkostnader dersom en organisasjon har spesielle behov som gjør at skytjenestene som skal tas i bruk må skreddersys. Dersom «standard»-tjenester som allerede finnes ikke kan brukes, må gjerne konsulenter involveres for å tilpasse tjenestene. Dette vil bidra til å øke kostnadene ved overgang til skytjenester.

Et siste viktig poeng å legge merke til, er at med SaaS er det leverandøren som overtar ansvaret for håndteringen av data. Kunden vil dermed ha mindre kontroll på hvor og hvordan sine data blir håndtert. Dette kan ha betydning for virksomheter som håndterer sensitiv og/eller gradert informasjon.

2.5 Distribuert sky

I sammenheng med skytjenester er også begrepet *edge* eller *fog computing* mye brukt, og da som en del av en trelagsmodell, som omfatter sky, edge og sluttbruker. Skytjenestene som befinner seg «på toppen», kjører i store datasentre som kan ligge svært langt fra brukerne. Edge-tjenester befinner seg, som navnet antyder, «i utkanten», og leveres typisk fra små, lokale datasentre nær brukerne. Den enkelte bruker trenger ikke vite om en tjeneste leveres fra en sentral sky eller nærmeste edge-datasenter da dette skjer automatisk.

Innenfor distribuerte skytjenester opererer man med tre typer (C. Mouradian, 2017):

- *Cloudlets* skal først og fremst avlaste sluttbrukerenhetene ved å la ressurskrevende operasjoner foregå på små lokale datasentre (*cloudlets*). Det handler altså primært om å tilby datakraft til sluttbrukerne ved hjelp av små lokale datasentre som tilbyr en del av egenskapene til skytjenester. Cloudlets kan også fungere frittstående, uten kontakt mot internett og sentrale skytjenester.

- *Multi-Access Edge Computing* (MEC) handlet opprinnelig om å skaffe regnekraft til kanten (*edge*) av mobilnettverk og MEC-noder var gjerne samlokalisert med base-stasjoner for mobiltelefoni. Det er denne tette knytningen mot mobilindustrien som er hovedforskjellen på MEC og *cloudlets.* Senere ble begrepet utvidet til også å inkludere stasjonære nettverk. Fordi MEC er så tett knyttet til mobilindustrien har det vært et mål å standardisere denne skyplattformen så langt som mulig, for å fremme innovasjon og utvikling av mobile skytjenester (T. Taleb, 2017).

- *Fog computing* er, i motsetning til *cloudlets* og MEC, tett knyttet til eksistensen av sentrale skytjenester, og kan ikke fungere uten. Her opererer man dermed med trelags-modellen nevnt over, bestående av sentrale skytjenester, lokale (*fog*) skytjenester og sluttbruker.

Felles for alle tre typene av distribuerte skytjenester er at de benytter mekanismer som gir sky-egenskaper (som forklart i kapittel 2.1 og 2.2), og de har som mål å flytte skytjenestene nærmere sluttbrukeren. En viktig driver for dette arbeidet er behovet for å redusere forsinkelser som kan oppstå, eksempelvis på grunn av flaskehalser i nettverket, når sentrale skytjenester benyttes. Så langt har *cloudlets* og *fog* fått mest oppmerksomhet i forsknings- og utviklings-miljøer, mens MEC drives frem av et industrikonsortium og er tett assosiert med 5G. Det er også verdt å legge merke til at Gartner trekker frem distribuert sky som en viktig strategisk teknologitrend (Gartner, 2020).

For denne rapporten er ikke forskjellene mellom de ulike typene av distribuert sky så viktig. Selve konseptet distribuert sky synes imidlertid å være svært relevant for bruk i forsvars-sammenheng, fordi det gir mulighet for autonomi og redundans. Dette kommer vi tilbake til i kapittel 4.2.2.

3 Status for bruk av skytjenester i Forsvaret

Som en stor (i norsk målestokk) organisasjon er det naturlig at også Forsvaret, og generelt hele forsvarssektoren, vurderer bruk av skytjenester. Det er imidlertid en del forhold innen sektoren generelt, men særlig i Forsvaret, som gjør at nytteverdien og anvendeligheten av slike tjenester ikke nødvendigvis er like klar som for sivil sektor. I dette kapittelet ser vi på hva Forsvaret anvender av skytjenester i dag og hva de planlegger for fremover. Forhold som gjør at Forsvaret skiller seg ut med tanke på bruk av sky blir drøftet i kapittel 4.

Så langt forfatterne av denne rapporten kjenner til, er det kun én etablert anvendelse av sky-tjenester i Forsvaret i dag, og det er Forsvarssektorens Office 365 (FO365), tatt frem gjennom prosjektet «Etablering av ugraderte skytjenester» (Forsvarsdepartementet, 2018). Prosjektet er ikke ferdig, og løsningen er fortsatt under utrulling.

Office 365 (og dermed FO365) er som nevnt tidligere et eksempel på SaaS og et verktøy for samhandling, kontorstøtte, dokumentutveksling, -lagring og -distribusjon. Det er med andre ord snakk om svært utbredt programvare, hvor bruken ikke skiller seg særlig fra tilsvarende anvendelser i andre sektorer. Mer spesifikt dreier det seg om Microsoft sine verktøy Teams, Outlook (e-post), kalender, OneDrive-lagring og Office-pakken, og alle tjenestene leveres fra Microsoft Azure. FO365 er kun tillatt brukt med ugraderte data.

I tillegg har FMA IKT-kapasiteter, i forbindelse med koronapandemien, etablert en ugradert utviklingsplattform som dels kjører i Azure, og dels hos FMA. Dette er en felles plattform for personell i FMA IKT-KAP og industri, som skal benyttes for videre utvikling av applikasjoner og plattformer i Forsvaret (Forsvarsmateriell, 2020).

Utover disse to anvendelsene er det ingen bruk av skytjenester i produksjonssystemer i Forsvaret i dag. Det er imidlertid planer om en kraftig økning i bruk av skytjenester både i Forsvaret og forsvarssektoren gjennom investeringsprogrammet MAST. Programmet omfatter både sikre plattformer og en rekke tjenesteområder, og målet er «å oppnå mer effektiv informasjonsdeling, samhandling og gjennomgående tjenester for nasjonale styrker i operasjoner, samt med aktører i totalforsvaret og allierte» (Forsvarsmateriell, 2020).

Derimot er virtualisering i utstrakt bruk i Forsvaret, eksempelvis på FISBasis[5]-plattformene og på TYR. Sistnevnte, som utgjør dagens IKT-plattform i en kommandoplass i Hæren[6], består typisk av 2–3 fysiske tjenere, som så kjører et antall virtuelle tjenere (såkalte *serverroller*). Disse serverrollene leverer generell funksjonalitet som Active Directory[7], lagringstjeneste, e-post, karttjenester og så videre, samt mer spesialisert programvare som NORCCIS[8] og

[5] Forsvarets Informasjonssystem Basiskonfigurasjon. Dette er Forsvarets felles IT-plattformer.
[6] TYR er referanseløsningen. Faktiske installasjoner kalles NOR-TI-<gradering>, f.eks. NOR-TI-B for en BEGRENSET-installasjon. Merk også at TYR er et egennavn, og ikke en forkortelse.
[7] Katalogtjenesten Microsoft benytter for håndtering av brukere, brukerrettigheter og kontroll av ressurser.
[8] NORwegian Command and Control Information System. Forsvarets primære kommando- og kontrollsystem.

NORBMS[9]. Virtualisering gjør at maskinvareressursene (prosessorkraft, minne og lagring) kan fordeles etter behov mellom de ulike serverrollene, og man får en bedre utnyttelse av disse ressursene.

Som klienter benyttes normalt PC (såkalte «tykke klienter»), som dels kjører programvare lokalt (eksempelvis Microsoft Office), og dels klientprogramvare som for eksempel NORCCIS-klient som igjen kommuniserer med NORCCIS tjenerprogramvare som kjører på en virtuell tjener. Det er også grunn til å regne med at det vil komme støtte for såkalte nullklienter i TYR. Dette innebærer at selve klientmaskinen, som tidligere var en fysisk PC, nå kjører som en virtuell maskin, mens maskinvaren er redusert til skjerm, tastatur, mus og et minimum av maskinvare som kommuniserer med den virtuelle klienten. Dermed lagres ingen data i den fysiske klientmaskinen, som kan forenkle sikkerhetsregimet noe. Det er likevel fortsatt snakk om ren virtualisering, og ikke ekte skytjenester.

Klientmaskinene i kommandoplassen er normalt koplet til tjenerne gjennom nettverkskabel med god kapasitet. Overføringshastigheten er derfor ikke noe tema innad i en kommandoplass. Kommandoplassen har imidlertid radioforbindelser til kjøretøy som kjører mer selvstendige TYR-klienter, såkalte taktiske terminaler. Disse tykke klientene kan fungere isolert, men når det er forbindelse utveksler de data med tjeneren i kommandoplassen.

I tillegg har kommandoplassen forbindelser til kommandoplasser på høyere nivå. Sistnevnte kan gå over satellittkommunikasjon, noe som typisk gir vesentlig høyere overføringshastighet enn radioforbindelsen ut til kjøretøy og enkeltmann.

Om vi ser på de essensielle egenskapene ved skytjenester som vi presenterte i kapittel 2.1, og holder disse opp mot dagens TYR-løsning i en kommandoplass, så finner vi at TYR i liten grad kan sies å representere en skyløsning:

- *Generell tilgang via nettverk*: Datasenteret i kommandoplassen er primært tilgjengelig for brukerne gjennom lokalnettet innad på kommandoplassen. I tillegg er det en viss tilgjengelighet over radionett, for brukerne av taktiske terminaler ute i felt. Utover dette er datasenteret ikke tilgjengelig via nettverk.

- *Selvbetjent oppsett*: I en kommandoplass har man i dag ikke noe skille mellom leverandør og kunde. Konseptet selvbetjent oppsett gir derfor ikke mening i denne sammenhengen. Det meste av oppsettet skjer automatisk, ved å kjøre et installasjonsprogram, og tjenere, tjenester og klienter er konfigurert og satt i drift før operasjonen starter.

- *Samling av ressurser*: Fordi et datasenter i en kommandoplass kun har én bruker, mister man muligheten til å kunne fordele maskinvareressursene over flere kunder (flerbruk).

[9] NORwegian Battle Management System. Forsvarets hovedsystem for kommando og kontroll på taktisk nivå og lavere.

Dermed må også maskinvaren dimensjoneres etter den ene «kundens» maksimale behov.

- *Fleksibel og transparent dekning av ressursbehov*: Virtualisering gir en viss grad av rask skalerbarhet, fordi maskinvareressursene kan fordeles på de virtuelle maskinene etter behov. Det vil likevel være en relativt begrenset form for skalerbarhet, ettersom man har en ganske begrenset mengde maskinvare til disposisjon, og i tillegg få virtuelle maskiner å flytte ressursene mellom.

- *Ressursbruk måles*: I en kommandoplass vil ressursbruken måles, men da primært med tanke på å ivareta sikkerhet og fordele ressurser. Ressursmåling med tanke på å ta betalt etter forbruk gir ikke mening i denne sammenhengen.

Generelt vil også et datasenter i en kommandoplass være langt unna den massive skalaen man ser i datasentre som leverer skytjenester.

4 Avveininger for bruk av skytjenester i Forsvaret

I kapittel 2 introduserte vi de egenskapene som er nødvendig for at en IKT-basert tjeneste skal kunne kalles en skytjeneste, og i kapittel 3 ble status for bruk av skytjenester (i motsetning til nettbaserte tjenester generelt) i Forsvaret diskutert. I dette kapittelet ser vi på hva som karakteriserer Forsvaret, og som kan gjøre at man ikke nødvendigvis kan nyttiggjøre seg alle de fordelene som loves ved bruk av skytjenester.

Grovt sett kan man si at IKT-bruken i Forsvaret kan deles inn i en administrativ/forvaltningsdel og en operativ/skarp del.[10] I McKinsey-rapporten «Modernisering og effektivisering av stabs-, støtte- og forvaltningsfunksjoner i forsvarssektoren» (McKinsey, 2015) gjør man et tilsvarende skille, og kaller det henholdsvis støtte-IKT og operativ IKT. På administrativ side har Forsvaret mange fellestrekk med øvrig offentlig sektor og store organisasjoner i Norge[11], og burde derfor i prinsippet kunne benytte samme type IKT-systemer. Dette støttes også av McKinsey-rapporten, som sier at «støtte-IKT i større grad egner seg for sammenligninger med IKT-virksomhet i andre organisasjoner» (McKinsey, 2015). Eksempler kan være systemer for regnskap, personalforvaltning, kontorstøtte og samhandling.

På operativ side er derimot Forsvaret til dels svært forskjellig fra den sivile verden, med en rekke IKT-systemer som i liten grad brukes noe annet sted enn innenfor militær virksomhet. Eksempler er systemer for ildledning, kommando og kontroll (K2) og kampledelse (*battle*

[10] Dette skillet er ikke skarpt, og det er økende oppmerksomhet i Forsvaret rundt behovet for tilgang til administrative systemer i forbindelse med operasjoner.
[11] Dog er det nok et større innslag av gradert informasjon som må håndteres i Forsvaret enn i øvrig offentlig sektor.

management). I dag benyttes en blanding av skreddersydde systemer, norske industriutviklede systemer og internasjonale/Nato-systemer. Stadig flere av disse systemene kjører på moderne operativsystemer og maskinvare, men det er fortsatt et antall systemer som krever eldre, eller spesialisert operativsystem og maskinvare.

Når vi i resten av dette kapittelet ser på hva som er viktig for Forsvaret med tanke på bruk av skytjenester, vil det derfor naturlig handle mest om operativ side. Vi har så tatt utgangspunkt i løsningsegenskapene som ble introdusert i kapittel 1.2. Disse er informasjonssystemsikkerhet, tilgjengelighet, funksjonalitet, robusthet, opprettholdelse, interoperabilitet og fleksibilitet.

4.1 Informasjonssystemsikkerhet

Forsvaret har behov for IKT-systemer som kan håndtere gradert informasjon, og da på alle graderingsnivåer. Vi ser imidlertid at mye av det administrative arbeidet, eksempelvis logistikk, regnskap og personalforvaltning holdes på lavgradert eller ugradert nivå. Utrullingen av FO365, beskrevet i kapittel 3, skal brukes til ugradert informasjon og indikerer dermed en økt satsing på arbeid på ugradert nivå. Dette betyr ikke at informasjonssystemsikkerhet ikke vil være viktig også for ugradert informasjon, men med tanke på sikkerhetsgodkjenning av skytjenester har ugraderte systemer færre utfordringer enn systemer som skal håndtere gradert informasjon. Som nevnt i kapittel 1.3 er det også gjort mye arbeid innen skytjeneste i offentlig sektor, også innenfor området sikkerhet (Norges Offentlige Utredninger, 2015) (Norges Offentlige Utredninger, 2017).

Leverandører av skytjenester satser gjerne tungt på sikkerhet (Sensei Enterprises, 2018), og disse er sannsynligvis vel så godt, om ikke bedre, rustet til å møte trusler i cyberdomenet enn mange organisasjoner med egne datasentre. Etablerte leverandører sørger for at de har nye, sofistikerte og oppdaterte sikkerhetssystemer, og et eksempel på dette er de tidligere sårbarhetene som ble avdekket i Intel sine prosessorer (CPU-er) (Graz University of Technology, 2018). Store skyleverandører var raskt ute med å håndtere disse sårbarhetene i sine maskinparker, og samtidig opplyse kundene om hva de eventuelt måtte gjøre selv i tillegg.

Selv om sikkerheten i skyen generelt er god og pålitelig, får en likevel en del nye mulige angrepsvektorer, i tillegg til de tradisjonelle truslene mot programvare. Noen eksempler er:

- Funksjonelle trusler fra skykomponenter: Verktøy for å understøtte de essensielle egenskapene ved sky (f.eks. panel for selvbetjening) kan alle inneholde feil og være sårbare for angrep. Et eksempel her er programvaren som sørger for virtualisering.

- Angrep på en klient: Skyleverandører satser mye på sikkerhet, og en innfallsport en angriper kan bruke er å forsøke å kompromittere klientprogramvare, for så å komme inn i tjenester utenfra.

- Selve kompleksiteten i skyen: Jo mer komplekst et system er, desto vanskeligere er det å sikre det.

Ugraderte virksomhetsprosesser som kun trenger «standard» tjenester (eksempelvis kontorstøttetjenester) er enklest og billigst å flytte til skyen. Skytjenester handler i stor grad om storskala, og innen slike standardiserte tjenester er det et bredt tilbud fra skyleverandørene. Det er derfor naturlig nok her Forsvaret har startet, med introduksjonen av FO365.

En utfordring for Forsvaret er imidlertid at informasjonselementer som enkeltvis er ugraderte, kanskje burde vært gradert dersom de aggregeres (Nasjonal sikkerhetsmyndighet, 2020). Dette blir stadig mer aktuelt ettersom mulighetene for maskinbasert dataanalyse av store datamengder øker kraftig. Denne utfordringen blir også trukket frem i (Kommunal- og moderniseringsdepartementet, 2016):

> *«Det er verdt å nemne at informasjon som i utgangspunktet ikkje er skjermingsverdig, kan bli betrakta som skjermingsverdig om han blir lagra i eit felles datasenter eller ei skyteneste der informasjonen til fleire samfunnsfunksjonar er samla. Då vil skadepotensialet ved tap av den samla informasjonen kunne få innverknad på den nasjonale tryggleiken. Dette kan gjere risikovurderingar meir kompliserte, ettersom ein risikerer å måtte vurdere ikkje berre sine eigne data, men òg summen av data som er lagra på same stad.»*

På operativ side vil mye informasjon være gradert. Dette kan for eksempel være planverk, ordre, sensorinformasjon, etterretningsinformasjon og måldata. Det er derfor grunn til å anta at behovet for å håndtere (høy)gradert informasjon er større på operativ side. Samtidig eksisterer mye av denne graderte informasjonen i form av dokumenter, regneark og presentasjoner, og kontorstøtteverktøy er dermed høyst nødvendig også på operativ side. Samhandlingsverktøy er også svært mye brukt her, eksempelvis Skype for business og andre videokonferanseløsninger.

Utfordringen er at selv om skytjenester og datasentrene som leverer dem er svært sikre, er det fortsatt mange uavklarte spørsmål rundt skytjenester og gradert informasjon, og regelverket rundt graderte informasjonssystemer er på etterskudd når det gjelder skytjenester. NSM har gjort noe arbeid innenfor virtualisering og flerbruk, gjennom veilederen «G-07 Partitioned Mode of Operation for VS» (Nasjonal Sikkerhetsmyndighet, 2017), men denne veilederen omhandler ikke skytjenester i særlig grad. Den har noe relevans for IaaS, men PaaS og SaaS blir ikke berørt. Det synes derimot klart at det å samle virtualiserte systemer med ulik gradering på samme fysiske servere er svært utfordrende. Eksempelvis har Forskrift om informasjonssikkerhet (Forsvarsdepartementet, 2001) en del krav til systemeierskap, roller og ansvar for graderte IKT-systemer, som er utfordrende å møte hvis disse systemene kjører virtuelt i et flerbruksmiljø.

Selv om alle gjestesystemene som kjører på en fysisk infrastruktur er eid av Forsvaret, betraktes de normalt som separate informasjonssystemer (Nasjonal Sikkerhetsmyndighet, 2017), og det kan dermed bli utfordrende å la disse dele samme fysiske infrastruktur dersom de har ulik gradering. Dette reduserer mulighetene for samling av ressurser, som er en essensiell egenskap ved sky. Noen av stordriftsfordelene ved bruk av sky kan dermed bli redusert eller gå tapt.

Ser vi på TYR-installasjoner er dette uproblematisk, da det kun er ett informasjonssystem som kjører på tjenermaskinene, og dermed kun én systemeier.

4.2 Tilgjengelighet

Med tilgjengelighet menes her at nettverk, tjenester og informasjon er tilgjengelig ved behov, og i militære operasjoner kan dette innebære tilgjengelighet i et miljø med mobile styrker, krevende topologi og en motstander som gjør aktiv bruk av det elektromagnetiske spekter til å lokalisere og/eller forstyrre radiosendere. Når vi vurderer tilgjengelighet i sammenheng med skytjenester innebærer dette at de nødvendige skytjenestene er tilgjengelige for bruk når brukeren trenger dem og der brukeren er.

En essensiell egenskap ved skytjenester er generell tilgang via nettverk, som beskrevet i kapittel 2.1. Fordi maskinvaren som leverer tjenestene ikke er lokalisert på samme sted som brukerne, er nettverkstilgang nødvendig. I prinsippet kan en dermed være på jobb hvor som helst så lenge organisasjonen benytter skytjenester. Imidlertid betyr dette også at skytjenesten kan være sårbar overfor avbrudd i nettforbindelsen. Når internettforbindelsen eller nettverket er nede, er skytjenestene utilgjengelige. Hvis forbindelsen er treg, vil tjenestene også oppleves som trege, og hele systemet eller operasjonene kan bli inaktive om man mangler redundante tjenester eller alternative nettforbindelser.

Ser vi på skytjenester levert over Internett, som for eksempel FO365, har Forsvaret en ekstra utfordring i noen tilfeller da det per i dag ikke nødvendigvis er Internett tilgjengelig over alt hvor Forsvarets brukere befinner seg.

For graderte og/eller operative tjenester i felt blir utfordringen enda større. Som vi var inne på i kapittel 3 er Forsvarets graderte systemer lukkede, og kan i utgangspunktet kun nås fra det (lukkede) nettet de er koplet til, f.eks. FISBasis HEMMELIG (FISBasis H). Eventuelle skytjenester på FISBasis H vil være tilgjengelige over nettverk, men kun på steder hvor selve FISBasis H er tilgjengelig.

Ute i felt oppstår det ytterligere en utfordring, nemlig manglende nettverkstilgang. Dette kan være ufrivillig og skyldes manglende kapasitet i nettverket eller jamming fra en motstander, eller det kan være frivillig, fordi man ikke ønsker å røpe egen posisjon gjennom bruk av radiosendere.

4.2.1 Geografisk distribusjon

To av egenskapene diskutert i kapittel 2.1 og 2.2 som kjennetegner skytjenester – *geografisk distribusjon av ressurser/data* og *samling av ressurser* (muliggjort via Internett) – betyr at geografisk nærhet til databehandlingsressurser ikke er nødvendig for å benytte disse. Det betyr også at det kan være vanskelig å vite i hvilket land kundens data blir oppbevart og/eller behandlet. Data kan flyttes rundt mellom datasentre av forskjellige grunner, for eksempel hvis en bestemt type ressurs ikke finnes i alle datasentre vil dataene sendes dit hvor ressursen er,

avhengig av behov. Slike dataoverføringer kan skje uten at brukeren av tjenesten merker noe. Vanligvis skjer dette også uten at brukeren blir forespurt eller varslet, men flyttingen vil typisk måtte følge den avtalen man har med leverandøren. Oppførselen varierer altså med leverandør og avtaler om tjenestekvalitet (SLA, *Service Level Agreement*).

Denne geografiske dataflyten kan skape juridiske utfordringer med sikkerhetsmessige eller operative implikasjoner. EU-domstolen har for eksempel nylig besluttet at overføring av data som dekkes av EUs personvernlovgivning (*General Data Protection Act*, GDPR) ikke kan overføres til USA fordi de da ikke beskyttes av EUs regler for personvern (Datatilsynet, 2020). Dette er positivt for personvernet, men betyr at noen skytjenester ikke kan benyttes i EØS-land uten at kunden bryter loven. Dette kan også representere et potensielt problem for Forsvaret, eksempelvis om det besluttes å ta offentlige skytjenester i utstrakt bruk. Kanskje man finner at det er mulig å benytte slike skytjenester for ugradert og lavgradert informasjon etter en nøye verdivurdering. Denne vurderingen kan imidlertid stille seg annerledes dersom det viser seg at tjenester og data man forventer befinner seg i Norge (eller i det minste i et Natoland), plutselig migreres til annet land utenfor alliansen.

I tillegg vil et land ha jurisdiksjon over data som oppbevares innenfor landets grenser. Russland har for eksempel forlangt at alle sosiale medier og lignende oppbevarer data på maskinvare som befinner seg i Russland (Brombach, 2014). Når data flyttes rundt kan det bety at disse dataene dekkes av et annet lands lover og regler, og muligens kan tappes av landets etterretning. Som et eksempel gir USAs «Foreign Intelligence Surveillance Act (FISA) Section 702» vide fullmakter for å samle inn data fra blant annet leverandører av skytjenester. Her er det dessuten en utfordring at USA kan kreve tilgang også til data lagret utenfor landet, så lenge firmaet som leverer skytjenesten er amerikansk. Implikasjonene i FISA Section 702 er oppsummert her (Nojeim, 2017). Dette kan i seg selv være en motivasjon for at Russland (og senere også andre nasjoner) i større grad ønsker å beholde data innenfor landets grenser (J. Sherman, 2020).

Her kan også initiativet Gaia-X (GAIA-X, u.d.) nevnes. Dette er et europeisk initiativ ledet av Frankrike og Tyskland, som har som mål å utvikle felles krav for en europeisk datainfrastruktur. Bakgrunnen for initiativet er at de fleste av dagens store leverandører av skytjenester er ikke-europeiske, samtidig som man ser et økt behov for suverenitet over og tilgjengelighet til egne data.

En annen mulig fallgruve er relatert til det faktum at mange skytjenester gjerne er bygget med flere lag oppå hverandre, med ulike leverandører av de forskjellige lagene. Det er ekstremt kostbart å bygge ut en storskala infrastruktur for skytjenester. Dette har ført til at selv svært store firmaer som tilbyr skytjenester ikke nødvendigvis eier sine egne datasentre. Dropbox benyttet utelukkende Amazon AWS i mange år, frem til 2018 da de endret modell til å benytte flere ulike leverandører i parallell i tillegg til AWS, for å redusere sine løpende kostnader (Kidd, 2018). I skrivende stund brukes AWS eksempelvis av Zoom (som benyttes av mange for videokonferanser) og Apples iCloud (Statt, 2019).

En slik modell senker terskelen for nye aktører, ettersom man ikke trenger å investere i store serverparker for å starte salg av en tjeneste, men samtidig gjør det bildet mer uoversiktlig for

kunden, ettersom det blir vanskeligere å vite hvor dataene faktisk befinner seg. Dette er en høyst relevant problemstilling for Forsvaret i de tilfellene det er krav om at informasjon som behandles skal befinne seg i Norge.

4.2.2 Skytjenester i en taktisk kommandoplass

I utgangspunktet består anvendelser av skytjenester av et antall klienter (PC, mobil, nettbrett og så videre) som via et nettverk bruker tjenester som kjører i ett eller flere store datasentre. Overført til bruk i felt vil det si brukere (soldater i teig, på fartøy eller i kommandoplasser) med PC, nettbrett eller mobil som bruker skytjenester som leveres fra sikrede, sentrale datasentre. En slik løsning vil være sårbar, fordi klienter som mister forbindelsen til skytjenestene vil kunne utføre svært lite.

I tillegg vil rekkevidde ofte kunne være en begrensende faktor. Taktiske radioer har ofte så kort rekkevidde at forbindelsen må gå over flere hopp, for å kunne bruke tjenester i et sentralt datasenter. Mange typer av taktiske radioer har dessuten svært begrenset, og til dels variabel kapasitet. Satellittforbindelser vil kunne tilby tilstrekkelig rekkevidde, men de kan være kostbare og noen systemer har begrenset dekning i deler av Norge.

Dersom Forsvaret på sikt tar i bruk mobilkommunikasjon (4G og 5G) i felt vil bildet være noe annerledes, ettersom slik kommunikasjon har både stor kapasitet, og god dekning gjennom et stort antall basestasjoner med svært god forbindelse inn til sentral infrastruktur (Jørgenrud, 2015) (Farsund & Hegland, 2020).

I en krise/krigssituasjon vil man imidlertid måtte regne med at en motstander aktivt vil prøve å sette kommunikasjonen ut av spill ved hjelp av jamming og å ta ut basestasjoner, og da er mobilkommunikasjon minst like sårbart som militær radiobasert datakommunikasjon. I tillegg kan det, uavhengig av hvilken kommunikasjonstype som benyttes, i noen tilfeller være nødvendig å avstå fra all bruk av radiosendere, for ikke å røpe egen posisjon.

Dette betyr at en «tradisjonell» skyløsning hvor sentrale skytjenester brukes fra klienter med radiokommunikasjon ute i felt er sårbar og lite egnet for operativ bruk. Som beskrevet i kapittel 2.5 ser vi imidlertid en trend med distribuerte skyløsninger, hvor små datasentre trekkes helt ut til sluttbrukeren. Denne trenden er særlig hjulpet frem av 5G, hvor såkalt *edge computing* er sentralt (C. Mouradian, 2017), nærmere bestemt det som kalles *Multi-Access Edge Computing* (MEC). Hensikten er å skaffe regnekraft til kanten (*edge*) av mobile nettverk og slike MEC-noder er da gjerne samlokalisert med 5G basestasjoner.

En slik distribuert skyløsning vil kunne passe bedre inn i en militær kontekst, ved at kommandoplasser eller fartøy utstyres med et lite datasenter[12] som enten kan fungere autonomt, eller som en node i en større, distribuert skyløsning, avhengig av om det har forbindelse ut eller ikke. Lokalt i kommandoplassen eller ombord på fartøyet vil brukerne være tilknyttet sitt datasenter

[12] Et datasenter i denne sammenhengen kan være noen få servere, det vil si utstyr som får plass i et lite rack eller i en koffert.

med kablede klienter. Kjøretøy og enkeltsoldater kan benytte skytjenestene fra sin lokale kommandoplass så lenge radiokommunikasjon er mulig. Tilsvarende kan fartøy i en fartøygruppe benytte skytjenester fra fartøyet med det lokale datasenteret ombord.

Videre vil MEC og SaaS i kombinasjon gi mulighet for lokasjonsuavhengighet, ved at man ikke vet, og trenger heller ikke vite, om tjenesten man benytter kjører lokalt i kommandoplassen eller i en bakenforliggende sentralisert sky. Dette gir mulighet for tilgang til et langt større sett av tjenester, fordi man ikke lenger er bundet til det settet av tjenester som tilbys av tjenerne i den lokale kommandoplassen. I tillegg kan man møte det samme brukergrensesnittet og de samme tjenestene, enten man sitter ved en kontorplass, for eksempel i en garnison, eller i et kjøretøy ute i felt.

4.3 Funksjonalitet

Denne løsningsegenskapen ble opprinnelig definert som evne til å utføre en oppgave eller funksjon. Når vi her ser på funksjonalitet i forbindelse med skytjenester er det på bakgrunn av at standardisering og storskala er viktige faktorer for å oppnå noen av fordelene med sky. Samtidig er Forsvaret avhengig av en del spesialisert funksjonalitet i form av programvare og systemer som ikke brukes så mange andre steder.

Mens mange organisasjoner kan klare seg med forholdsvis generell (standardisert) programvare, eksempelvis for kontorstøtte, økonomi og personalforvaltning, har Forsvaret en stor porteføljе av spesialisert programvare, som gjerne også krever spesiell maskinvare for å kjøre. Mye av denne arven er planlagt faset ut i årene fremover, men man vil likevel være bundet til en del spesialisert program- og maskinvare eksempelvis på fly, fartøy og til dels kjøretøy.

Når organisasjoner går over til å bruke skytjenester og det ikke finnes SaaS-programvare som kan benyttes, er ofte *lift and shift* det første steget. Dette er beskrevet i kapittel 2.4.1 og innebærer at eksisterende informasjonssystemer migreres over til en felles plattform, normalt i form av IaaS. De eksisterende informasjonssystemene fortsetter da å kjøre som virtuelle systemer, men funksjonaliteten er den samme, og brukerne vil i liten grad merke forskjell. Forsvaret selv bruker gjerne begrepet systemkonsolidering om denne prosessen (Forsvarsdepartementet, 2020).

Dersom vi ser på IKT på taktisk nivå, er TYR, som beskrevet i kapittel 3, basert på utstrakt bruk av virtualisering og i prinsippet har man dermed allerede gjennomført en form for *lift and shift* av de ulike applikasjonene som benyttes i TYR. Informasjonssystemet TYR som helhet er imidlertid fortsatt et «fysisk» informasjonssystem, i den forstand at de virtuelle maskinene kjører på dedikert maskinvare og som inngår som en del av informasjonssystemet.

Ulempen med *lift and shift* er at eksisterende programvare som bare er løftet over på en skyplattform ikke oppnår alle fordelene som SaaS-basert programvare, eksempelvis skalering. I tillegg kan man, som alltid med virtualiserte systemer, få en mer uklar eierskapsmodell, som vi var inne på i kapittel 4.1, og driftsmodellen kan bli mer kompleks.

Oppsummert er *lift and shift* svært aktuelt for Forsvaret, med sin store portefølje av spesialisert programvare, og dette blir også utredet gjennom MAST-programmet. Det er da viktig å gjøre en vurdering av hver enkelt applikasjon, hvorvidt den skal løftes over til en skyplattform eller om den skal beholdes som den er, i påvente av en SaaS-versjon av den samme eller tilsvarende applikasjon.

4.4 Robusthet

Denne løsningsegenskapen innebærer evne til å tåle endringer og påkjenninger, samt motstandsdyktighet mot fiendepåførte trusler, klima og værrelaterte påkjenninger, i tillegg til brukerfeil og plutselige feil i maskin- eller programvare.

Det er først og fremst gjennom redundans at skytjenester kan bidra til økt robusthet sammenliknet med tjenester levert av tradisjonelle applikasjoner. De store skyleverandørene disponerer som regel flere store datasentre som er geografisk spredt. Dermed kan leveransen skytjenester raskt flyttes til et annet datasenter dersom et datasenter skulle bli overbelastet eller satt ut av spill. Dette gjenspeiles også i at de store skyleverandørene gjerne garanterer svært høy oppetid (Channel Futures, 2011). Eksempelvis garanterer Microsoft 99,9 % oppetid for Office 365 (Microsoft, u.d.), som tilsvarer under 9 timer nedetid per år. I tillegg kan forsinkelse reduseres for brukerne, fordi tjenester kan flyttes eller dupliseres og kjøres geografisk nærmere brukeren.

I forsvarssammenheng må det imidlertid skilles mellom fiendepåførte og øvrige trusler, samt om samfunnet befinner seg i fredstilstand eller i krise/krig. For ikke-fiendepåførte påkjenninger er trusselbildet antakelig noenlunde likt i fred, krise og krig.

Når det gjelder fiendepåførte trusler, er det i fredstid primært snakk om ulike former for cyberangrep. Erfaringen viser at slike aktiviteter pågår kontinuerlig, og er å regne som en «normaltilstand» (Nasjonal Sikkerhetsmyndighet, 2020). Man kan derfor forvente at både Forsvaret og eksterne skyleverandører er godt forberedt på, og kan håndtere slike aktiviteter. I en eventuell opptrapping mot krise og krig kan det imidlertid være grunn til å forvente både økt mengde cyberangrep, og kanskje også sabotasjehandlinger og regulære kinetiske angrep mot datasentre og kommunikasjonslinjer.

En annen faktor som er knyttet til løsningsegenskapen robusthet er begrepet *train as you fight*. Hvis man i fredstid gjør seg avhengig av en effektiv, men sårbar IKT infrastruktur som leverer gode skytjenester kan det gi store utfordringer i en krisesituasjon, dersom denne infrastrukturen angripes og skytjenestene ikke lenger er tilgjengelige. Generelt er det gjerne slik at jo mer avhengig man er av en gitt tjeneste, jo viktigere er det at denne tjenesten er robust og tilgjengelig i en krise eller krig. Dersom man til daglig arbeider og trener i et miljø med god tilgang til nødvendige tjenester, bør det legges mye ressurser i å sikre at de samme tjenestene er tilgjengelige, også hvis en motstander aktivt forsøker å hindre det.

De sistnevnte aktivitetene reiser spørsmål innenfor en rekke områder, eksempelvis innenfor temaet folkerett, når det kommer til bruk av eksterne leverandører av skytjenester. Slike

spørsmål ligger utenfor det denne rapporten skal se på, men er viktige å ta stilling til ved vurdering av eksterne leverandører for leveranse av skytjenester.

Dersom krav til graderte informasjonssystemer innebærer at Forsvaret må ha egne datasentre for graderte skytjenester vil antallet slike datasentre påvirke hvor mye redundans det er mulig å oppnå, og dette vil i sin tur påvirke robustheten til skytjenestene. Det er grunn til å regne med at forsvarseide datasentre for graderte skytjenester vil kunne bli plassert i fjellhaller, som gir en viss beskyttelse mot kinetiske angrep, men dette er ikke noe annerledes enn tradisjonelle datasentre plassert i fjellhaller.

Det som derimot kan bidra til økt robusthet er en løsning for skytjenester basert på mange distribuerte datasentre med gode og redundante innbyrdes kommunikasjonslinjer. Dersom man i stor grad baserer seg på SaaS, og at det enkelte datasenter også kan fungere autonomt, har man et godt utgangspunkt for robuste tjenester. Små mobile (*edge*) datasentre i taktiske kommando-plasser vil også kunne inngå i en slik struktur og bidra til redundans og dermed robusthet. Som nevnt i kapittel 2.5 er distribuert sky trukket frem som en viktig teknologitrend, og gitt Forsvarets behov for robuste tjenester, synes dette å være en teknologi som bør undersøkes nærmere.

4.5 Opprettholdelse

Opprettholdelse (*sustainment*) innebærer evne til å bevare et ytelsesnivå og sikre tjenestens eksistens over en ubestemt tidsperiode. Dette innebærer at tjenesten opprettholdes i alle faser; fred, krise og krig, og som for løsningsegenskapen robusthet kan det være nyttig å skille mellom opprettholdelse i fredstid og i krise/krig.

Det er tilsynelatende en viss overlapp mellom løsningsegenskapene *opprettholdelse* og *robusthet* som vi så på i kapittel 4.4. Når vi i denne rapporten benytter løsningsegenskapene for å vurdere skytjenester, skiller vi mellom dem på følgende måte: Løsningsegenskapen robusthet bruker vi om evnen til å motstå (plutselige) angrep og hendelser, det vil si kinetiske-, cyber- og innsideangrep, eller utilsiktede hendelser som ras, strømbrudd eller alvorlige brukerfeil. Løsningsegenskapen opprettholdelse handler derimot forhold som kan påvirke tilgjengeligheten av skytjenestene over tid. Eksempler kan være politiske eller juridiske forhold, langvarige operasjoner, brukerstøtte og administrasjon.

Merk at vi her kun ser på opprettholdelse i forbindelse med eksterne skyleverandører eller eksternt driftsansvar. Der hvor Forsvaret eier og selv drifter egne datasentre blir forskjellen liten fra dagens situasjon.

Brukerstøtte kan være en utfordring i forbindelse med bruk av skytjenester fra eksterne leverandører. Bruker man programvare i henhold til SaaS-modellen, der alt ansvar ligger hos leverandøren, er det i utgangspunktet leverandøren som har ansvaret for brukerstøtte. Som nevnt i

kapittel 2.4.3 er imidlertid ikke dette alltid tilfelle, da store kunder gjerne sitter med førstelinje-støtten selv. Det er derfor viktig at ansvaret er tydeliggjort, for å hjelpe brukerne med å finne frem til rette instans.

Dersom man benytter en IaaS- eller PaaS-modell, der ansvaret deles mellom flere aktører, kan det eksempelvis være vanskelig å feilsøke skytjenesten, og dermed på en enkel og utvetydig måte identifisere hvem som har ansvaret for en gitt feil. Et eksempel her kan være bruk av offentlig sky i undervisningen i enkelte universitetsemner, der studenter støter på problemer når de skal bruke ulike leverandørers IaaS/PaaS sammen med egenutviklede tjenester. Disse tjenestene er gjerne avhengige av en *open source* applikasjonstjener som skal puttes i skyen, men som ikke støttes av skyleverandøren. Denne kombinasjonen av tjenester og programvare fra ulike leverandører, gjør feilsøking vanskelig og man ender i praksis ofte opp med ikke å få støtte fra noen part for å løse problemer som oppstår i skjæringspunktet mellom bruken av disse løsningene.

I krise eller krig er det imidlertid flere faktorer som kan påvirke evnen til opprettholdelse. Dersom skytjenestene leveres fra utlandet, eller fra Norge, men av en utenlandsk leverandør, kan man risikere at myndighetene i leverandørens hjemland av ulike årsaker ikke lenger tillater leveranse av tjenester til Norge.

Selv med datasentre lokalisert i Norge, og drevet av et norsk firma, må det sørges for at det finnes personell tilgjengelig for å holde tjenesteleveransene i gang også i krise og krig. Det samme er tilfelle om Forsvaret har egne datasentre som driftes av et eksternt firma. I begge tilfeller er det gjerne også underleverandører involvert, slik at det oppstår hele verdikjeder som må opprettholdes.

I forbindelse med bruk av eksterne firma oppstår det også interessante problemstillinger rundt drift av datasentre i taktisk sammenheng. Fordi slike datasentre må kunne operere autonomt, og dermed ikke alltid kan driftes fra et sentralt sted, er det et spørsmål om driftspersonell må være med ut i felt. I alle tilfeller er det en del folkerettslige og etiske problemstillinger som det er viktig å avklare.

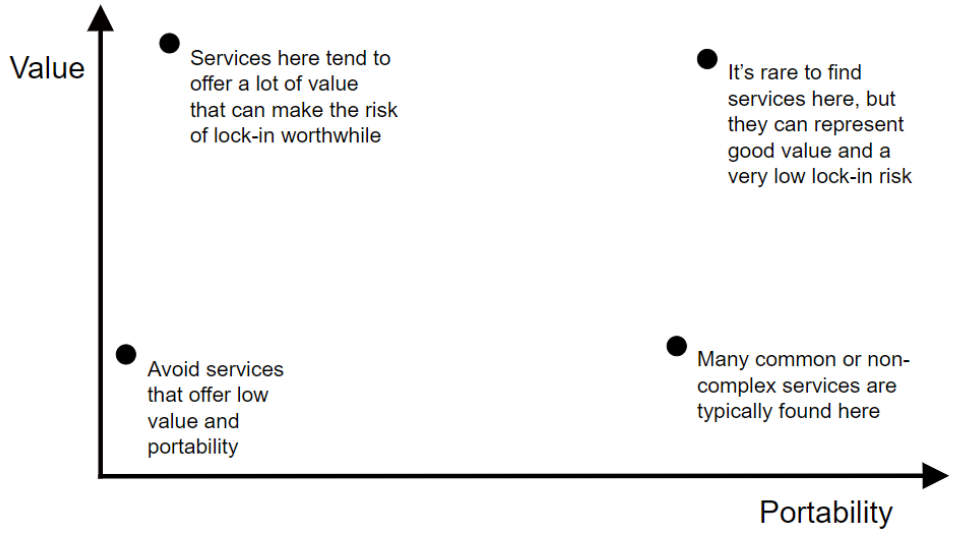
4.6 Interoperabilitet

Med interoperabilitet menes evnen til å samhandle med andre for å nå et mål. I definisjonen fra (Forsvarsdepartementet, 2017) ble det lagt vekt på at dette også inkluderte prosesser og personell. Når vi her benytter denne løsningsegenskapen for å evaluere bruk av skytjenester, så ser vi primært på teknologisk interoperabilitet. Dog utvider vi begrepet til også å omfatte interoperabilitet mellom leverandører av skytjenester.

Som vi har vært inne på er én av fordelene med bruk av skytjenester fra ekstern leverandør at behovet for investeringer blir kraftig redusert. I stedet kjøper man tjenester, og betaler for bruken. Dette betyr også at terskelen for å bytte leverandør av skytjenester er, eller burde være,

relativt lav. Ideelt sett burde «interoperabiliteten» mellom leverandører være god, slik at det er mulig å flytte data og tjenester fra en leverandør til en annen uten alt for store problemer.

I praksis viser det seg imidlertid at man gjerne må gjøre avveininger mellom leverandørbinding på den ene side og funksjonalitet på den andre. Eksempelvis har britiske myndigheter utarbeidet en guide (Government Digital Service, 2019) for hvordan slike avveininger kan gjøres. Figur 4.1 illustrerer et overordnet bilde av noen slike avveininger, hvor X-aksen indikerer graden av portabilitet (jo høyere portabilitet jo lavere grad av leverandørbinding), mens Y-aksen indikerer verdien av tjenesten.



Figur 4.1 Avveining mellom tjenesters verdi og grad av innelåsing (Government Digital Service, 2019).

For en organisasjon av Forsvarets størrelse vil bytte av leverandør av skytjenester uansett ikke være noen triviell operasjon, men bruk av åpne og standardiserte løsninger bør likevel prioriteres. Spesialtilpasninger og bruk av leverandørspesifikke løsninger må også avveies mot kostnad og tekniske vanskeligheter ved et eventuelt bytte av leverandør. Dette må også sees i sammenheng med forrige løsningsegenskap (opprettholdelse): Dersom man velger en utenlandsk leverandør av skytjenester leverandøren blir kjøpt opp av et utenlandsk firma eller får utenlandske underleverandører, kan politiske endringer over tid gjøre det nødvendig å bytte leverandør.

En annen side ved egenskapen interoperabilitet gjelder samvirke mellom skytjenester og «tradisjonelle» tjenester og applikasjoner. I overskuelig fremtid vil Forsvaret sannsynligvis ikke gå fullstendig over til skytjenester – det vil alltid finnes systemer og applikasjoner som må kjøre på egen, dedikert maskinvare, eksempelvis sensorer og effektorer på kampplattformer. Det er derfor viktig å sikre at skybaserte tjenester kan samvirke med slike spesialiserte systemer og utveksle informasjon med dem. Relatert til dette er også muligheten for å løfte eksisterende systemer over på en skyplattform (*lift and shift*). Slike systemer kan ha ulike krav til maskinvare og operativsystem, og skyplattformen må kunne møte disse kravene.

Til slutt må det også tas hensyn til at en del av Forsvarets skytjenester må kunne samvirke med kommende skytjenester levert av Nato. Nato har flere store prosjekter i gang som skal bidra til en overgang til skytjenester. Det mest kjente av disse er IT Modernization (ITM)-prosjektet, hvor General Dynamics IT ble tildelt hovedkontrakten i mars 2017 (NCI Agency, 2017). ITM inngår som en del av et større initiativ for modernisering av Natos IT-infrastruktur gjennom programmet Polaris (Dron, 2019).

Nato leverer også en rekke forskjellige applikasjoner, kalt FAS-er (*Functional Area Services*), (NCI Agency, u.d.). I den grad Forsvaret velger å benytte slike FAS-er i egen virksomhet vil det være nødvendig at disse kan kjøres i Forsvarets løsning for skytjenester, enten gjennom *lift and shift* eller ved at FAS-ene kan kjøres som SaaS (dersom de blir forberedt for dette).

I internasjonale operasjoner vil det trolig være krav om kompatibilitet med Federated Mission Networking (FMN)-spesifikasjonene (NATO ACT, u.d.). FMN har i dag ingen elementer av skytjenester i seg, og vil heller ikke få dette de nærmeste årene. Elementer av teknologien som ligger bak skytjenester har imidlertid dukket opp i forbindelse med spesifikasjoner av fremtidige FMN-versjoner, og det er derfor grunn til å holde et øye med på arbeidet som gjøres på slike fremtidige spiraler.

4.7 Fleksibilitet

Med fleksibilitet menes evne til å tilpasse tjenesten eller systemet til ulike situasjoner, brukere, miljøer og konsepter. Det innebærer også evne til å dimensjonere, skalere, konfigurere og videreutvikle tjenesten eller systemet.

Én av de essensielle egenskapene ved skytjenester, som ble listet i kapittel 2.1, er fleksibel og transparent dekning av ressursbehov. Store datasentre som betjener et stort antall kunder gjør at den enkelte kunde kan skalere ressursbruken svært raskt, og tilsynelatende ubegrenset. Dette innebærer at løsningsegenskapen fleksibilitet tilsvarer en helt grunnleggende egenskap ved skytjenester, nemlig evnen til å dimensjonere og skalere raskt.

Samtidig har Forsvaret behov for å håndtere graderte data, og kan bli nødt til å benytte dedikert maskinvare for dette. Det vil normalt innebære en privat (dedikert) sky uten andre kunder enn Forsvaret selv. Dermed vil evnen til skalering måtte bli et valg man gjør, i en avveining mellom kostnader til maskinvare og utnyttelsen av denne. Med et datasenter som er dimensjonert etter de maksimale behovene er risikoen at mye av denne kapasiteten blir stående ubenyttet mye av tiden[13]. Så fleksibilitet, i form av rask skalering og dimensjonering, er fortsatt mulig, men til en høyere pris enn for offentlige skytjenester som leveres til mange kunder.

Det er fortsatt ikke klart om det vil bli mulig med flerbruksmiljøer som kombinerer ulike graderinger (for eksempel lavgraderte og ugraderte systemer) på samme maskinvare, så hvor mye denne evnen til skalering vil lide er ikke klart. Dersom systemer med ulik gradering kan

[13] Dette er nærmere forklart i vedlegg C.

dele datasenterressurser vil dette gi noe større fleksibilitet og mulighet til å fordele ressurser etter hvor det er behov.

En annen side av løsningsegenskapen fleksibilitet går på muligheten til å konfigurere et informasjonssystem til ulike bruksområder. Innenfor systemutvikling finnes det en rekke teknologier for «programmerte» konfigurasjoner, ofte kalt «*Infrastructure as Code*» (IBM Cloud Education, 2019). Dette betyr at systemkonfigurasjoner kan defineres i form av kode, og så lenge ressursene som konfigureres er virtuelle betyr dette at et ferdig konfigurert system kan settes opp svært raskt. Forsvaret benytter et lignende konsept i TYR i dag, ved at en kommando-plassinstallasjon for en stor del kan settes opp automatisk ved å kjøre et script som sørger for konfigureringen.

Dersom Forsvaret på sikt får en løsning med distribuerte skytjenester på taktisk nivå kan man i større grad se for seg bruk av oppsett definert i form av kode. Da kan i tillegg hele oppsettet kjøres opp i et sentralt datasenter på forhånd, og så migreres over til det taktiske datasenteret rett før operasjonen starter.

5 Oppsummering og konklusjon

I løpet av de siste 10 til 15 årene har bruken av skytjenester fått en betydelig utbredelse, og svært mange organisasjoner har allerede tatt i bruk slike tjenester eller vurderer å gjøre det. Samtidig er det mange ulike oppfatninger av hva sky innebærer, og det kan være utfordrende å forstå hva teknologien bak egentlig innebærer. I tillegg er det noen forhold ved Forsvaret som kan ha innvirkning på bruk av skytjenester.

Denne rapporten har hatt to formål. For det første har vi ønsket å gi en innføring i skytjenester generelt, forklare hva det er og innebærer. For det andre har vi sett på hvordan Forsvaret skiller seg fra sivile organisasjoner med tanke på bruk av sky, og drøftet faktorer som må tas i betraktning ved innføring av slike tjenester. For det sistnevnte har vi konsentrert oss om den operative delen av Forsvaret IKT-bruk, da det er her de store forskjellene fra sivil IKT-bruk ligger.

I introduksjonen til rapporten stilte vi tre spørsmål:

- Hva er egentlig skytjenester, og hvorfor er det nyttig i mange sammenhenger?
- Hvilke egenskaper og behov preger Forsvarets bruk av IKT?
- Hvilke avveininger bør gjøres i forbindelse med bruk av sky i Forsvaret?

Vi har beskrevet hvordan man kan se på skytjenester både fra et forretningsmessig og fra et teknologisk ståsted. Forretningsmessig handler skytjenester primært om å sette ut ansvaret for drift og vedlikehold av IKT-tjenester, og for noen organisasjoner kan dette være den primære motivasjonen for å gå over til å bruke skytjenester.

Fra et teknologisk synspunkt finnes det ikke én entydig definisjon av hva skytjenester er, og vi har derfor i stedet forklart skytjenester gjennom å liste et sett med essensielle egenskaper som slike tjenester må ha, samt et sett med egenskaper som er vanlig å se hos skytjenester: generell tilgang via nettverk, selvbetjent oppsett, samling av ressurser, fleksibel og transparent dekning av ressursbehov og måling av ressursbruk. Til sammen gir disse egenskapene et godt bilde av hva skytjenester innebærer.

Disse egenskapene representerer også de viktigste årsakene til at skytjenester har fått så stor utbredelse: Skytjenester har normalt svært god tilgjengelighet over datanettverk og man har tilsynelatende ubegrenset med ressurser tilgjengelig. Videre tilbyr de store leverandørene en høy grad av sikkerhet og man betaler heller for ressursforbruk enn å måtte investere i eget utstyr.

Kartlegging av Forsvarets behov og krav til egenskaper i IKT-systemer kan gjøres på en rekke ulike måter. Vi har valgt å ta utgangspunkt i et eksisterende rammeverk bestående av syv løsningsegenskaper: informasjonssystemsikkerhet, tilgjengelighet, funksjonalitet, robusthet, opprettholdelse, interoperabilitet og fleksibilitet.

Disse løsningsegenskapene ble først introdusert i arbeidet med konseptuell løsning for taktisk ledelsessystem for landdomenet (Forsvarsdepartementet, 2017). Bakgrunnen for vårt valg er at disse løsningsegenskapene utgjør et rammeverk som er utarbeidet og kjent i Forsvaret. De representerer én av mange mulige måter å beskrive Forsvarets behov og særpreg på når vi skal vurdere bruk av skytjenester, men det er vår vurdering at disse gir et representativt bilde av egenskaper og behov som er viktig for Forsvaret.

Dette rammeverket har vi så sammenholdt med egenskapene ved skytjenester og sett på hvordan de fordelene man normalt oppnår ved bruk av skytjenester slår ut når man legger løsnings-egenskapene til grunn. Det vi da ser er at det er en del forhold rundt Forsvarets virksomhet som gjør at flere av de vanlige fordelene rundt bruk av sky ikke nødvendigvis gjelder, eller er like store som for en sivil organisasjon.

Nedenfor oppsummerer vi de observasjonene og forholdene vi har kommet frem til ved å holde egenskapene ved skytjenester opp mot de syv løsningsegenskapene, og som vi mener det er viktig å ta hensyn til når bruk av skytjenester i operativ sammenheng vurderes:

- Sikkerhet tas svært alvorlig hos de store leverandørene av skytjenester, og disse er sannsynligvis vel så godt, om ikke bedre, rustet til å møte trusler i cyberdomenet enn mange organisasjoner med egne datasentre. Når det kommer til håndtering av gradert informasjon er det imidlertid mye uavklart, og mye arbeid gjenstår, rundt regelverk og hvordan sikkerhetsvurdering og -godkjenning av slike systemer skal gjøres.

- Bruk av skytjenester i sammenheng med (høy)graderte informasjonssystemer i Forsvaret er ikke utelukket, men avhengig av hvordan regelverket til slutt blir, kan mulighetene være mer begrenset enn for ugraderte anvendelser og noen av stordrifts-fordelene ved skytjenester bli redusert eller gå tapt.

- Også ugraderte skytjenester kan representere en utfordring, fordi informasjonselementer som enkeltvis er ugraderte, til sammen kan utgjøre gradert informasjon. Nye muligheter for maskinbasert dataanalyse av store datamengder bidrar til å øke dette problemet. Derfor blir risikovurdering viktig når man skal vurdere hva som kan lagres av ugradert informasjon hos en offentlig leverandør av skytjenester.

- Skytjenester er basert på generell tilgang via nettverk, men taktiske radionett har som regel begrenset kapasitet og nettverket kan være utilgjengelig i perioder, enten fordi motstanderen aktivt forsøker å hindre kommunikasjon, eller fordi man ikke ønsker å røpe egen posisjon. Distribuerte løsninger hvor skytjenester kan leveres fra små datasentre som også kan fungere autonomt kan være en vei å gå for operativ/taktisk bruk av skytjenester.

- Skytjenestenes lokasjonsuavhengighet kan gjøre det utfordrende å vite hvor egne data faktisk befinner seg, noe som i sin tur kan skape juridiske utfordringer. Det faktum at mange skytjenester er bygget med flere lag oppå hverandre, levert av ulike tjeneste-leverandører, bidrar til å gjøre dette enda mer komplekst.

- Forsvaret har en stor portefølje av spesialisert programvare og informasjonssystemer som i beste fall kan gjøres skybasert gjennom *lift and shift*. Det gjør potensialet for kostnadsreduksjon gjennom bruk av skytjenester noe mindre, inntil disse eventuelt erstattes av SaaS-baserte tjenester.

- Når det kommer til evne til å stå imot kinetiske angrep er det ikke grunn til å tro at det er noen forskjell på datasentre som leverer skytjenester og tradisjonelle datasentre. Den viktigste beskyttelsen mot slike angrep (i tillegg til fysisk sikring) er uansett redundans, både i datasentre og kommunikasjonslinjer. Imidlertid har skytjenester, og særlig SaaS, større mulighet for å dra nytte av slik redundans, fordi leveranse av tjenester er lokasjonsuavhengig.

- Det er nødvending med tilgjengelige ressurser for brukerstøtte og drift for at sky-tjenester skal være tilgjengelige. En rekke faktorer kan bidra til å redusere tilgjengelig-heten av skytjenester, eksempelvis uklare ansvarsforhold mellom leverandører, endrede politiske forhold i leverandørers hjemland og vilje og evne hos sivilt driftspersonell til å opprettholde tjenestekvaliteten i en krise- eller krigssituasjon.

- Selv om bytte av leverandør av skytjenester alltid vil være en svært omfattende og krevende operasjon for en organisasjon av Forsvarets størrelse, er det viktig å unngå proprietære løsninger som bidrar til ytterligere leverandørlåsing. I tillegg er det viktig å ta hensyn til utviklingen med hensyn til bruk av skytjenester i øvrig offentlig sektor og i

Nato, for å sikre at samvirke er mulig med disse. Det må også legges til rette for samvirke mellom skytjenester og tradisjonelle applikasjoner som ikke kan flyttes ut i skyen.

Gitt den sterke veksten i bruk av skytjenester, også i offentlig sektor, samt Digitaliseringsrundskrivets pålegg om å vurdere slike tjenester ved nyetablering eller oppgradering av digitale tjenester, er det grunn til å forvente at også Forsvaret vil bli en stor bruker av skytjenester, i hvert fall innen forvaltning og administrasjon. Når det gjelder bruk av skytjenester i Forsvarets operative oppgaver er dette også mulig, men som vi har diskutert i denne rapporten er det en del faktorer som innebærer at enkelte av fordelene ved bruk av skytjenester kan blir noe redusert.

Samtidig kan utnyttelse av distribusjon og redundans i skytjenester bidra til å gi Forsvaret svært robuste IKT-tjenester, også på taktisk nivå, men sannsynligvis til en høyere kostnad enn man vanligvis ser for skytjenester. En distribuert skyløsning kan også gi mulighet for et større sett av tjenester ute på kommandoplassen enn i dag, fordi man ikke lenger er bundet til det settet av tjenester som tilbys av tjenerne i den lokale kommandoplassen.

Dersom Forsvaret ønsker å benytte skytjenester operativt, og spesielt stridsnært, anbefaler vi at det først gjøres en grundig evaluering av hva som er mulig og realistisk å få til innenfor tekniske, juridiske, økonomiske og sikkerhetsmessige rammer.

Referanser

Birje, M. N. (2017). Cloud computing review: Concepts, technology, challenges and security. *International Journal of Cloud Computing, 6*(1), 32-57.

Brombach, H. (2014, 07 24). *Digi.no*. Hentet fra Alle persondata må lagres i Russland - Putin undertegner omstridt lov: https://www.digi.no/artikler/alle-persondata-ma-lagres-i-russland/289500

C. Mouradian, D. N. (2017). A Comprehensive Survey on Fog Computing: State-of-the-art and Research Challenges. *IEEE Communications Surveys & Tutorials.*

Canalys. (2020, 07 30). *Global cloud services market Q2 2020*. Hentet 10 2020 fra canalys: https://www.canalys.com/newsroom/worldwide-cloud-infrastructure-services-Q2-2020?time=1602835241

Channel Futures. (2011, 1 20). *Microsoft and Google: Is 99.9% Cloud Uptime Good Enough for Partners*. Hentet 10 2020 fra Channel Futures: https://www.channelfutures.com/cloud-2/microsoft-and-google-is-99-9-cloud-uptime-good-enough-for-partners

Datatilsynet. (2020, 10 22). *Spørsmål og svar om nye regler for overføring av personopplysninger til land utenfor EØS*. Hentet fra Datatilsynet: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/sos-om-nye-regler-for-overforing/

Digitaliseringsdirektoratet. (2020). *Overordnede arkitekturprinsipper for digitalisering av offentlig sektor*. Hentet fra https://www.digdir.no/digitalisering-og-samordning/overordnede-arkitekturprinsipper/1065

Donnely, C. (2016, 2 12). *Netflix is now 100% all-in on the AWS cloud*. Hentet 10 2020 fra ComputerWeekly.com: https://www.computerweekly.com/news/4500273047/Netflix-is-now-100-all-in-on-the-AWS-cloud

Dron, A. (2019, 5). Polaris - transforming NATO’s digital presence. *NITECH - NATO Innovation and Technology*(1), ss. 63-66. Hentet fra https://issuu.com/globalmediapartners/docs/nitech_issue_01_may_2019/67

Farsund, B., & Hegland, A. (2020). *5G i Forsvaret - Muligheter og sikkerhetsutfordringer, Eksternnotat 20/01206.* FFI. FFI.

Forsvarsdepartementet. (2001). *Forskrift om informasjonssikkerhet.*

Forsvarsdepartementet. (2017). *Konseptuell løsning (KL) for taktisk ledelsessystem for landdomenet, (BEGRENSET).* Usignert KL.

Forsvarsdepartementet. (2018). *Gjennomføringsoppdrag (GO) for Prosjekt 8185 Etablering av ugraderte skytjenester (BEGRENSET).* Gjennomføringsoppdrag.

Forsvarsdepartementet. (2020). *P8171 FSP Neste Generasjon - høygradert, Vedlegg I - Plan for Systemkonsolidering og Tjenestemigrering (BEGRENSET).* Usignert FL.

Forsvarsmateriell. (2020, 11 9). *MAST*. Hentet 11 2020 fra Forsvarsmateriell: https://www.fma.no/anskaffelser/virksomhetsprogrammet-mast

Forsvarsmateriell. (2020). Nyhetsbrev FUP U / FUP@Home. Sikker plattformavdeling.

GAIA-X. (u.d.). *GAIA-X: A Federated Infrastructure for Europe*. Hentet 11 2020 fra GAIA-X: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

Gartner. (2020, 7 23). *Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020*. Hentet 09 2020 fra Gartner: https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020

Gartner. (2020, 10 19). *Gartner Top Strategic Technology Trends for 2021*. Hentet 11 2020 fra Smarter With Gartner: https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021/

Government Digital Service. (2019, 12 17). *Managing technical lock-in in the cloud*. Hentet fra Gov.uk: https://www.gov.uk/guidance/managing-technical-lock-in-in-the-cloud

Graz University of Technology. (2018). *Meltdown and Spectre*. Hentet 9 2020 fra Meltdown and Spectre: https://meltdownattack.com/

Gundelsby, J. H. (2014, 11 4). *Erfaringer fra 150 mikrotjenester fordeler og ulemper*. Hentet fra Difi: https://www.difi.no/sites/difino/files/arkitektur_oslo_kommune_jan_henrik_gundelsby_kort_copy.pdf

IBM. (2019, 12 10). *Lift and Shift*. Hentet 11 2020 fra IBM Cloud Learn Hub: https://www.ibm.com/cloud/learn/lift-and-shift

IBM Cloud Education. (2019, 12 2). *Infrastructure as Code (IaC)*. Hentet 11 2020 fra IBM Cloud Learn Hub: https://www.ibm.com/cloud/learn/infrastructure-as-code

J. Sherman, S. B. (2020, 1 13). *Russia's 'Data Localization' Efforts May Guide Other Governments*. Hentet fra Defense One: https://www.defenseone.com/ideas/2020/01/russias-data-localization-push-may-guide-other-governments/162380/

Jørgenrud, M. B. (2015, 12 3). *Forsvaret vil bli mobiloperatør. Militært samband på nettene til Telenor, Netcom og Ice*. Hentet 10 2020 fra Digi.no:

https://www.digi.no/artikler/forsvaret-vil-bli-mobiloperator-militaert-samband-pa-nettene-til-telenor-netcom-og-ice/320016

Kidd, C. (2018, 9 21). *How Dropbox Reduced OpEx by Moving to a Multi-Cloud*. Hentet 10 2020 fra bmcblogs: https://www.bmc.com/blogs/dropbox-aws/

Kommunal- og moderniseringsdepartementet. (2016). *Nasjonal strategi for bruk av skytenester.* Strategi. Hentet fra https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-bruk-av-skytenester/id2484403/

Kommunal- og moderniseringsdepartementet. (2019). *Digitaliseringsrundskrivet.* Rundskriv. Hentet fra https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2683652/

Kommunal-og moderniseringsdepartementet. (2015). *Kartlegging av hindringer i regelverk for bruk av skytjenester.* Arbeidsgrupperapport. Hentet fra https://www.regjeringen.no/no/dokumenter/kartlegging-av-hindringer-i-regelverk-for-bruk-av-skytjenester/id2425260/

McKinsey. (2015, 3 17). *Modernisering og effektivisering av stabs-, støtte- og forvaltningsfunksjoner i forsvarssektoren.*

Microsoft. (u.d.). *Microsoft 365 Support*. Hentet 10 2020 fra Microsoft 365: https://www.microsoft.com/nb-no/microsoft-365/business/microsoft-365-for-business-support-options

Nasjonal Sikkerhetsmyndighet. (2017). *G-07 Partitioned Mode of Operation for VS (ikke utgitt ennå).* General IT Security Requirements no. 7 (G-07).

Nasjonal Sikkerhetsmyndighet. (2020). *Helhetlig digitalt risikobilde 2020.* Hentet fra https://nsm.no/getfile.php/134267-1601027852/Demo/Dokumenter/Rapporter/NSM_IKT-risikobilde_2020_1609_LR.pdf

Nasjonal sikkerhetsmyndighet. (2020). *Risiko 2020.* Hentet fra https://nsm.no/getfile.php/133684-1592833706/Demo/Dokumenter/Rapporter/nsm-risiko-2020.pdf

NATO ACT. (u.d.). *FEDERATED MISSION NETWORKING*. Hentet 11 2020 fra FEDERATED MISSION NETWORKING: https://act.nato.int/activities/fmn

NCI Agency. (2017, 3 30). *NATO signs milestone contract for IT modernization*. Hentet 11 2020 fra NATO Communications and Information Agency: https://www.ncia.nato.int/about-us/newsroom/nato-signs-milestone-contract-for-it-modernization.html

NCI Agency. (u.d.). *NATO Software Tools List*. Hentet 11 2020 fra COI Cooperation Portal: https://dnbl.ncia.nato.int/nciaservicecatalogue/Lists/NATO%20Software%20Tools%20List/AllItems.aspx

NIST. (2011). *The NIST Definition of Cloud Computing.* NIST Special Publication. Hentet fra https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Nojeim, G. (2017, 2 15). *Section 702: What It Is & How It Works*. Hentet fra Center for Democracy $ Technology: https://cdt.org/insights/section-702-what-it-is-how-it-works/

Norges Offentlige Utredninger. (2015, 11 30). *Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden.* Hentet fra NOU-er: https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

Norges Offentlige Utredninger. (2017, 9 15). *IKT-sikkerhet i alle ledd — Organisering og regulering av nasjonal IKT-sikkerhet.* Hentet fra NOU-er: https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/

OASIS. (2012, 12 04). Reference Architecture Foundation for Service Oriented Architecture Version 1.0. Hentet fra https://docs.oasis-open.org/soa-rm/soa-ra/v1.0/cs01/soa-ra-v1.0-cs01.pdf

Prot, A. (2017, 8 11). *Is SaaS the Future of WordPress?* Hentet 9 2020 fra Torque: https://torquemag.io/2017/08/saas-future-wordpress/

Robinson, M. (2020, 11 12). *DevSecOps: A Complete Guide to What, Why, and How*. Hentet 11 2020 fra Plutora: https://www.plutora.com/blog/devsecops-guide

Seglsten, P. (2020, 10 13). *DFØ skal handle inn skytjenester – har ikke peiling på hva prisen blir*. Hentet 10 2020 fra Digi.no: https://www.digi.no/artikler/dfo-skal-handle-inn-skytjenester-har-ikke-peiling-pa-hva-prisen-blir/500734

Sensei Enterprises. (2018, 8 28). *GOOGLE CLOUD'S DEFENSE IN DEPTH INCLUDES PHYSICAL SECURITY*. Hentet fra Sensei Enterprises: https://senseient.com/ridethelightning/google-clouds-defense-in-depth-includes-physical-security/

Statt, N. (2019, 4 22). *Apple's cloud business is hugely dependent on Amazon*. Hentet 10 2020 fra The Verge: https://www.theverge.com/2019/4/22/18511148/apple-icloud-cloud-services-amazon-aws-30-million-per-month

T. Taleb, K. S. (2017). On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration. *IEEE Communications Surveys & Tutorials, 19*(3), 1657-1681.

ValueBlue. (u.d.). *IaaS, PaaS & SaaS, what was that all about again?* Hentet 09 2020 fra ValueBlue: https://valueblue.com/iaas-paas-saas-what-was-that-all-about-again/

Vaughan, N. (2019). *JD EDWARDS SESSIONS | ORACLE OPENWORLD 2019*. Hentet 11 2020 fra Redfaire: https://www.redfaire.com/blog/jdedwards-oracleopenworld-2019

Vedlegg

A Norsk-engelsk ordliste

Automasjon	Automation
Deling	Sharing
Egenkapital/forhåndsinvestering	Capital expenditure (CAPEX)
Flerbruk	Multi-tenancy
Forretningsprosess som en tjeneste	Business Process as a Service (BPaaS)
Gruppesky	Community cloud
Hybride skyer	Hybrid cloud
Hype-syklusen	Hype cycle
Infrastruktur som en tjeneste	Infrastructure as a Service (IaaS)
Kampledelse	Battle management
Kanten	Edge
Klynge	Cluster
Løpende kostnader	Operational expenditure (OPEX)
Mikrotjenester	Microservices
Nektelsesangrep	Denial of service attacks
Nettsky	Cloud/cloud computing
Offentlig sky	Public cloud
Operativ smidighet	Operative agility
Opprettholdelse	Sustainment
Plattform som en tjeneste	Platform as a Service (PaaS)
Privat sky	Private cloud
Programvare som en tjeneste	Software as a Service (SaaS)
Programvaredefinert infrastruktur	Infrastructure as Code (IaC)
Programvareutvikling	Software development
Ressurssamling	Resource pooling
Sikkerhet	Security
Skrivebord som en tjeneste	Desktop as a Service (DaaS)
Skytjenester	Cloud services
Systemdrift	Information technology operations
Tingenes internett	Internet of Things (IoT)
Tjener	Server
Tjeneste	Service
Tjenestemodell	Service model

Tjenesteoppdagelse	Service discovery
Tjenesteorientert arkitektur	Service Oriented Architecture (SOA)
Virtuell privat sky	Virtual private cloud
Øyeblikksbilde	Snapshot

B Definisjoner av byggesteinene i en skytjeneste

For å sikre en felles forståelse av ord og uttrykk som brukes gjennomgående i denne rapporten definerer vi her de viktigste uttrykkene. Definisjonene gjelder for dette dokumentet, og enkelte er noe forenklet for å kunne understøtte en ikke-teknisk diskusjon om skytjenester.

Figur B.1 Forenklet illustrasjon som viser forholdet mellom programvare, operativsystem og noen av maskinvare-ressursene en datamaskin tilbyr.

- **PC / smartenhet / tjener**: I dette dokumentet vil PC bli brukt som en generell term som dekker bærbare og stasjonære datamaskiner. PC vil også bli brukt når man diskuterer generell bruk av datamaskiner. Smartenheter er nettbrett og smarttelefoner mens tjenere («*servere*») referer til datamaskiner som håndterer større oppgaver (for eksempel store databaser) og kan benyttes av flere brukere. Der en typisk PC eller smartenhet er brukernær, vil en tjener være noe brukeren interagerer med over et nettverk. Tjeneren er spesialisert maskinvare eller programvare som gjøres tilgjengelig for mer enn én bruker eller én type bruk. I denne rapporten brukes ordet «tjener» om maskinvarevarianten, mens tjenerprogramvare betegner programvare som utfører oppgaver for annen programvare, for eksempel vil en *databasetjener* lagre og hente data mens en netttjener (*webserver*) leverer nettsider til en nettleser.

  Alle disse forskjellige enhetene består av *maskinvare* som styres av *programvare*.

- **Maskinvare** er fysiske objekter, det kan være en datamaskin, smarttelefon, trådløse (WiFi) rutere som brukes på et nettverk, en harddisk for lagring av data eller en datamaskin brukt i en nettsky.

- **Programvare** er det som utfører oppgaver på en PC eller tilbyr tjenester på en tjener. Microsoft Word 2010 er et eksempel på programvare for sluttbrukere som kjører på en PC eller smartenhet. En database for utbetaling av lønninger er et eksempel på programvare som kan kjøres på en tjener.

- Et **(data)nettverk** er betegnelsen på flere datamaskiner som er koblet sammen med nettverksmaskinvare som gjør det mulig å sende data (for eksempel filer, meldinger

eller nettsider) fra en datamaskin til én eller flere andre datamaskiner. I dag er nettverk og kommunikasjonsløsninger sentrale komponenter i realiseringen av IKT-systemer.

- **Cyberspace,** som brukt i Forsvaret og Nato, tilkjennegir datasystemer og informasjons-ressurser som er koblet sammen i et nettverk. Cyberspace har både et rent digitalt kommunikasjonsaspekt (overføring av data mellom maskiner) og et samhandlingsaspekt (utveksling av informasjon mellom mennesker med bruk av digitale verktøy). Datasystemer består av to hoveddeler: programvare og maskinvare.

- **Operativsystemet** er spesiell programvare (for eksempel Windows på PC eller iOS/ Android på en smartenhet) som er ansvarlig for å knytte sammen maskinvare med annen programvare.

- **Plattform** er ofte brukt i Forsvaret for å betegne en base eller grunnleggende komponent som kapabiliteter kan bygges på eller knyttes til. Eksempelvis kan et helikopter som kan bære et våpensystem være en plattform. I IKT-sammenheng utgjøres en plattform av maskinvare, operativsystem og en del grunnleggende programvare (tjenester). FISBasis BEGRENSET er et eksempel på en IKT-plattform.

- **Standarder**: For at forskjellig typer programvare og/eller maskinvare skal kunne samhandle må de kunne kommunisere på en forutsigbar måte. Dette fordrer standarder som implementeres i programvare og maskinvare. Bruken av standarder sikrer interoperabilitet mellom systemer fra ulike leverandører. For eksempel er Internett bygget på en rekke standarder for å sende data.

- **Teknologi**: I dette dokumentet refererer teknologi til programvare, maskinvare, standarder, protokoller og prosesser, individuelt eller kombinert i forskjellige konstellasjoner. Et nettverk, en smarttelefon og tekstbehandlingsprogramvare er eksempler på forskjellige teknologier.

- **Tjeneste** brukes som en generell betegnelse på programvare (med maskinvare) som lar brukere utføre en oppgave eller en type oppgaver. Regnskap er et typisk eksempel på en tjeneste. En tjeneste kan i prinsippet kjøre rett på en PC eller smartenhet, men mer vanlig er at den tilbys fra en tjener. Tjenesten kan så benyttes over et nettverk via et brukergrensesnitt på enten en PC eller smartenhet. Tjenester som ligger i nettskyen, omtaler vi som skytjenester.

- **Skytjenester** er, i dette dokumentet, teknologibaserte funksjoner som vanligvis gjøres tilgjengelig for bruk over Internett etter behov, gratis eller betalt. Webmail er et eksempel på en slik tjeneste. Man kan også lansere skytjenester utenfor Internett, som vi beskriver i denne rapporten.

- **Ressursoppdeling:** Dette uttrykket benyttes for forskjellige tilnærminger som forbedrer utnyttelsen av maskinvare ved å la flere brukere få tilgang til samme maskinvare, men

uten at de forskjellige brukerne kan forstyrre hverandre. De to mest brukte metodene for en slik oppdeling er *virtualisering* og innpakking i *konteinere, se Appendix C.*

- **Flerbruk** (*multi-tenancy*) er maskin- eller programvare tjenere som benyttes av mer enn én organisasjon uten fysisk separasjon. På en flerbrukstjener kan for eksempel Forsvaret, uten å vite det, dele maskinvare med for eksempel utenlandske selskaper.

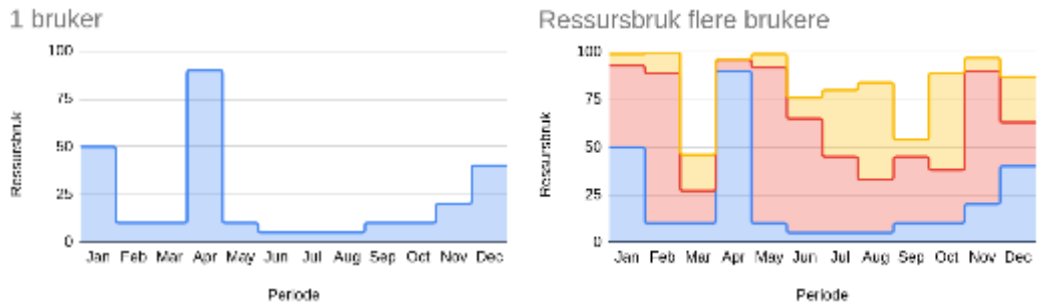
- **Brukere** er mennesker som benytter seg av ett eller flere av de ovenstående elementene. Man kan være en bruker av tjenester, operativsystemer, PC-er og liknende.

- **Kunde** benyttes som et generisk uttrykk for den eller de som har kontraktsforhold til en nettskytilbyder. Eksempelvis kan FLO eller FMA være en kunde hos skytjeneste X, og elevene på Cyberforsvarets våpenskole er brukere av tjenestene som skytjeneste X tilbyr.

C Typer av ressursoppdeling

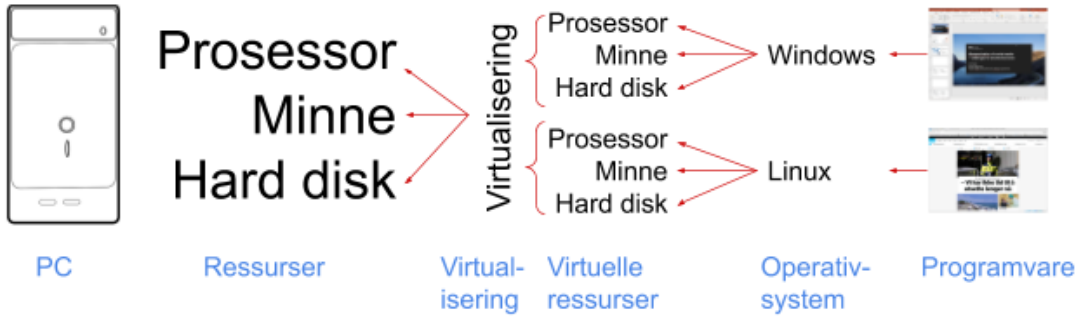
Virtualisering er benevnelsen på teknologier som har som formål å separere maskinvare fra programvare (inkludert operativsystemer). Formålet med denne separasjonen er å dele fysiske ressurser (f.eks. lagringskapasitet eller regnekraft) på mer enn én bruker eller tjeneste for bedre utnyttelse av ressurser og (som regel) kostnadsbesparelser. Virtualisering er blant annet nyttig når man har mer tjenerkapasitet enn det som kreves for den mest krevende enkeltbruken. Sekundært forenkler det også fremtidig drift av systemet, da man enkelt kan utvide med mer maskinvare uten å påvirke eksisterende virtuelle ressurser. Virtualisering letter også sikkerhets-kopiering, da man enkelt kan lage en kopi, et øyeblikksbilde (*snapshot*) av en virtuell maskin (VM). Dette i kontrast til å kjøre «rett på jernet» uten virtualisering, da man får en tett kopling mellom maskin og programvare.

I figur C.1 ser man et tenkt eksempel på forskjellen i ressursutnyttelse med og uten virtualisering. Til venstre i figuren er det illustrert en tjener med én bruker, hvor tjenerens kapasitet er dimensjonert etter brukerens maksimale behov. Vi ser at mye av kapasiteten er ubrukt det meste av tiden. Til høyre i figuren er den samme maskinvaren fordelt på flere brukere, og fordi disse kjører virtuelle maskiner på den fysiske tjeneren kan tjenerens kapasitet fordeles på de ulike brukerne etter behov. Resultatet er en langt bedre utnyttelse av den fysiske tjenerens ressurser.



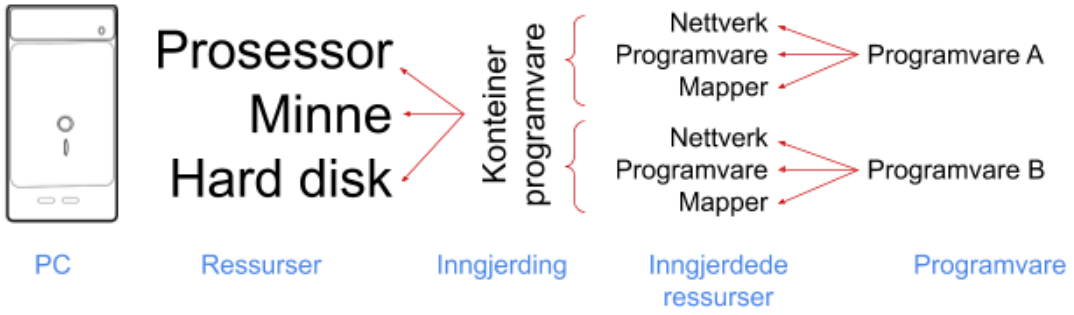
Figur C.1 Eksempel på ressursbruk med og uten virtualisering.

Rent teknisk foregår slik virtualisering ved å simulere maskinvareressurser, for eksempel en harddisk. I figur C.2 ser man forholdet mellom programvare, operativsystem, de virtuelle ressursene opp mot virtualiseringsdelen og den fysiske maskinvaren.



Figur C.2 Forenklet illustrasjon som viser hva virtualisering gjør.

Konteinerisering er en annen måte å fordele maskinvareressurser på. I stedet for å simulere maskinvare for et helt operativsystem, separeres programvaren ved å «gjerde inn» deler av et operativsystem med separate nettverk, mapper og så videre. Når programvare (for eksempel en database) er inne i en konteiner så ser den kun sine filer og nettverk, men deler prosessor, minne og harddisk direkte (se figur C.3). Resultatet er at konteinere tar mindre minne enn virtuelle maskiner og vil generelt kjøre raskere.



Figur C.3 Forenklet illustrasjon av konteinerprinsippet.

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

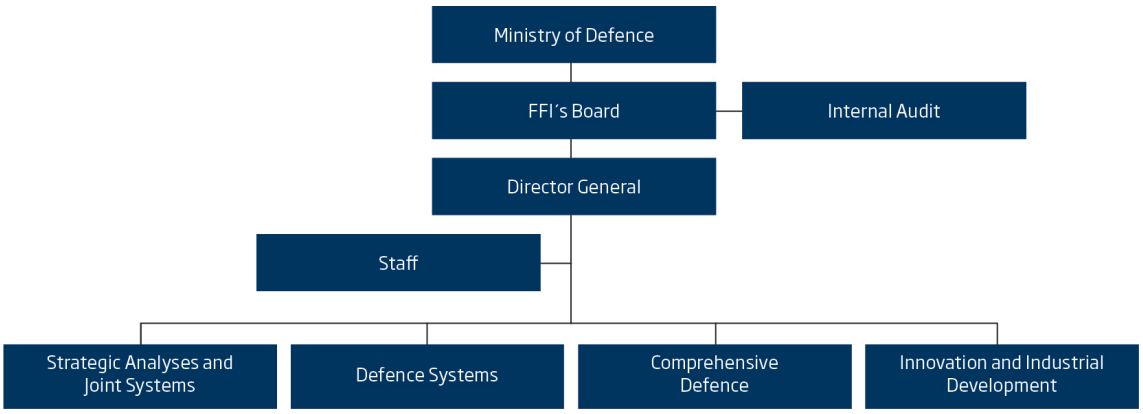
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt