



FORSVARET

Målbilde for Forsvarets datasentriske arkitektur



Metadata

KORTTITTEL:	FDSA
GRADERING:	UGRADERT
UTGIVER:	Sjef Forsvarsstaben
SAKSBEHANDLENDE AVD.:	FST Teknologi, Cyber og IKT
GJELDER FOR:	Forsvaret
HJEMMEL:	Instruks til forsvarssjefens undergitte sjef 2026-01-01 punkt 4.1.c
IKRAFTTREDELSE:	2026-10-05
FORRIGE VERSJON:	

Sammendrag

Forsvarets datasentriske arkitektur (FDSA) er et strategisk målbilde som beskriver en ønsket slutttilstand for hvordan Forsvaret forvalter, deler og utnytter data. Digital reguleringsplan (DRP) gir de styrende rammene som FDSA forholder seg til, og FDSA er særlig forankret i innsatsområdene DAT (Datadrevet forsvar og KI) og SIK (Sikkerhet).

For å møte dagens og fremtidens trusselbilde må vi etablere et datadrevet forsvar. På samme måte som vi behandler personell og materiell som strategiske ressurser, må vi også løfte data til kjernen av vår virksomhet, forvaltet uavhengig av applikasjonene som skaper eller konsumerer dem.

Målbildet defineres av tre grunnpilarer:

- 1. Nasjonal suverenitet og kontroll:** Forsvaret skal kunne operere uavhengig av enkeltleverandører eller tredjeparter for kritiske kapasiteter. Dette innebærer eierskap til data og deres mening, teknologisk handlefrihet for å skifte løsninger ved behov og nasjonal kontroll over krypteringsnøkler og kritiske kontrollmekanismer. Sikkerhet og personvern skal bygges inn fra start fremfor som en ettertanke.
- 2. Datastyring og utnyttelse:** Ansvar for data skal distribueres til domeneene som kjenner konteksten best, fra operative søyler til virksomhetsbærende funksjoner. Informasjon tilgjengeliggjøres som kvalitetssikrede dataprodukter optimalisert for automatisert utnyttelse, gjenbruk og selvbetjening. Felles regler sikrer at desentralisert eierskap ikke fører til silotenkning.
- 3. Samvirke og robusthet:** Informasjon skal struktureres etter felles begrepsapparat og ontologier og baseres på NATO-standarder for å sikre entydig forståelse og sømløs informasjonsflyt, i alt fra effektiv virksomhetsstyring til samvirke med allierte i operasjoner. Arkitekturen skal understøtte autonome operasjoner selv ved brutt eller degradert samband.

Målbildet gir retning for realiseringen av FDSA gjennom en konseptuell arkitektur organisert i ti kapabilitetsområder. Disse beskriver til sammen hvilke kapabiliteter som er nødvendige for å realisere et datadrevet forsvar, uten å binde seg til konkrete teknologivalg eller enkeltløsninger. Et etterfølgende teknisk målbilde vil konkretisere arkitekturen gjennom å beskrive de tekniske tjenestene som realiserer kapabilitetene.

Forsvarets distribuerte dataplattform (FDDP) er kjernen i realiseringen av FDSA. FDDP binder produsenter og konsumenter av data sammen på tvers av domener, applikasjoner og lokasjoner; domeneene får verktøy og tjenester for å hente inn, transformere og berike data til dataprodukter, mens konsumenter gis tilgang gjennom et standardisert delingslag. FDDP er konseptuelt én plattform med distribuerte egenskaper, som strekker seg fra allmenn sky og Forsvarets egne datasentre til taktiske enheter i felt.

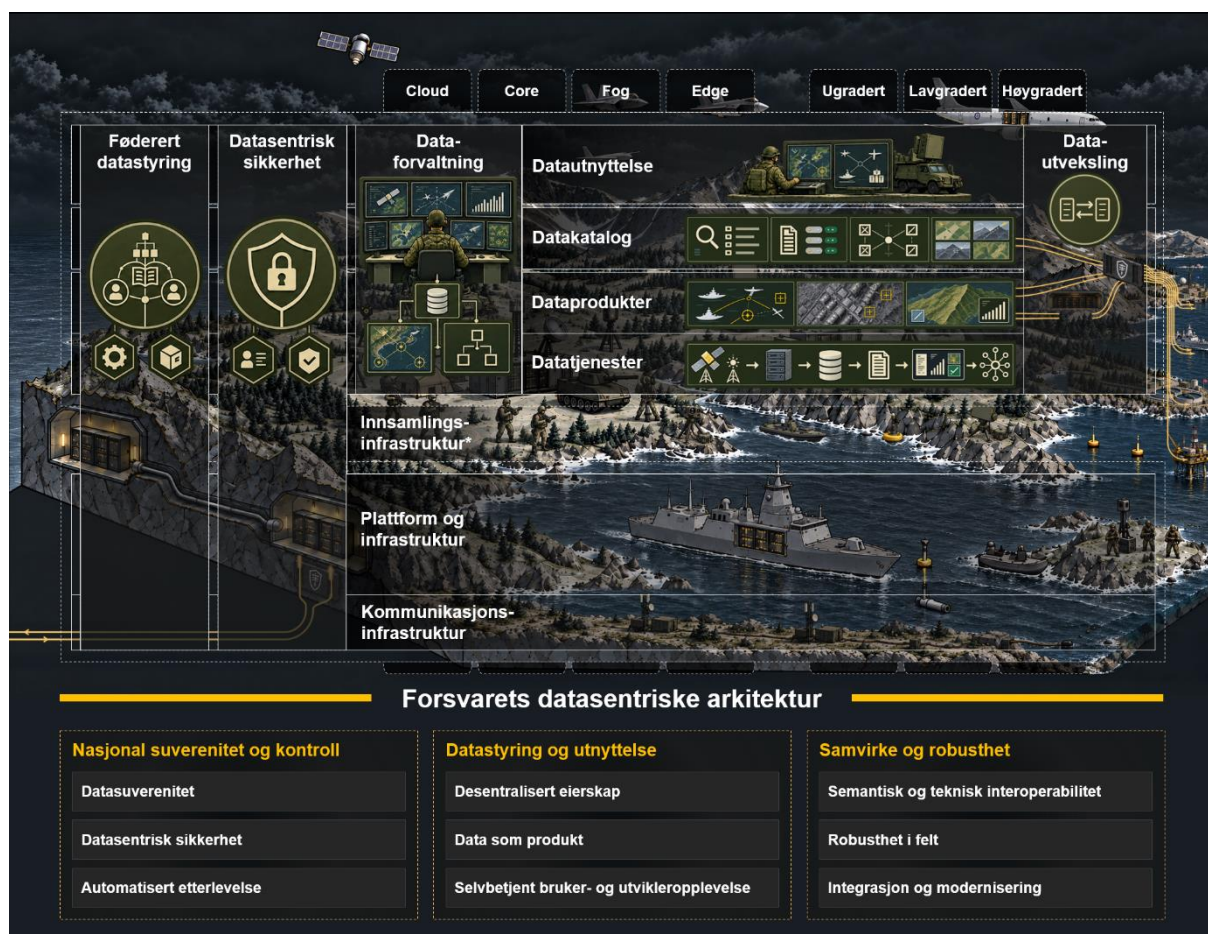
Innhold

Sammendrag	3
Innhold	4
1 Innledning	5
Bakgrunn	5
Formål	6
Avhengighet til styrende dokumenter og IKT-styringsmodell	6
Virkeområde	7
Forvaltning	7
Leseveiledning	7
2 Strategisk kontekst	8
Erfaringer fra moderne krigføring	8
Forpliktelser fra NATO	8
Det digitale leverandørlandskapet	9
3 Det datasentriske fundamentet	10
1. Datasuverenitet	11
2. Datasentrisk sikkerhet	12
3. Automatisert etterlevelse	13
4. Desentralisert eierskap	14
5. Data som produkt	15
6. Selvbetjent bruker- og utvikleropplevelse	17
7. Semantisk og teknisk interoperabilitet	18
8. Robusthet i felt	19
9. Integrasjon og modernisering	20
4 Konseptuell arkitektur	21
Føderert datastyring	22
Datasentrisk sikkerhet	22
Dataprodukter	22
Datakatalog	22
Datatjenester	23
Dataforvaltning	23
Datautveksling	23
Datautnyttelse	23
Plattform og infrastruktur	24
Kommunikasjonsinfrastruktur	24
Avgrensninger mot øvrige initiativer	25
5 Forsvarets distribuerte dataplattform	26
Konseptuelle noder i FDDP	27
Kjernekapabiliteter i FDDP	28
Scenarier	29
6 Begreper, definisjoner og forkortelser	32
Begrepsliste	32
Forkortelser	35

1 Innledning

Bakgrunn

Forsvaret står i en teknologisk brytningstid hvor evnen til å samle, bearbeide og utnytte data kan bli det avgjørende fortrinnet i en operasjon. Datamengden i det moderne stridsfeltet har eksplodert som følge av flere og mer avanserte sensorer, fra satellitter til droner og små IoT-enheter. Samtidig øker mengden effektorer, og disse skal i økende grad koordineres på tvers av domener for å skape rettidige, koordinerte og synkroniserte effekter. Erfaringer fra moderne krigføring, som i Ukraina, har demonstrert hvordan åpne data, sensor-til-effektor-integrasjon og bruk av kunstig intelligens kan utligne tradisjonelle styrkeforskjeller.



Figur 1 Illustrativ fremstilling av Forsvarets datasentriske arkitektur

Den pågående digitale transformasjonen er Forsvarets svar på dette utfordringsbildet. Gjennom å levere økt evne til situasjonsforståelse, kommando og kontroll, virksomhetsstyring og interoperabilitet skal transformasjonen understøtte målene i Forsvarets målbylde:

- forebygge og avskrekke konflikt
- nasjonal beredskap og evne til kollektivt forsvar
- styrkestrukturens utholdenhet
- militær støtte til Ukraina
- utvikling

Etableringen av en *datasentrisk arkitektur* er essensiell for å realisere denne transformasjonen. Arkitekturen gir Forsvaret et felles fundament for å utnytte data på tvers av operasjoner og virksomhetsstyring; fra situasjonsforståelse og sensor-til-effektor-integrasjon, til styringsinformasjon som understøtter effektiv forvaltning av personell, materiell og andre ressurser i fred, krise og krig. Målbildet bygger på at data er en strategisk ressurs som skal kunne deles og utnyttes innenfor regelverkets rammer, herunder krav til sikkerhet og personvern. Dette krever en grunnleggende endring i hvordan data forvaltes, fra å være en sekundær ressurs låst til spesifikke applikasjoner, til å gjøres tilgjengelig som et selvstendig produkt via standardiserte grensesnitt og protokoller, uavhengig av applikasjonene som skaper eller konsumerer dem.

Realiseringen av den datasentriske arkitekturen krever at vi utvikler en datadreven kultur, investerer i ny teknologi og etablerer en rask og sikker dataflyt på tvers av Forsvaret. Dette målbildet understøtter Forsvarssjefens ambisjon om et data- og etterretningsdrevet forsvar. Fremtidens forsvar er et datadrevet forsvar.

Formål

FDSA beskriver en ønsket slutttilstand for hvordan Forsvaret forvalter, deler og utnytter data. Målbildet skal gi strategisk retning og etablere grunnlaget for sikker og sømløs dataflyt som understøtter Forsvarets målbidde, fra effektiv virksomhetsstyring og forvaltning av personell, materiell og andre ressurser, til situasjonsforståelse, kommando og kontroll og samvirke med allierte og totalforsvaret.

Som målbilde beskriver FDSA verken gap mot dagens situasjon eller hva som kreves for å nå slutttilstanden, eksempelvis å bygge en gjennomgående datakultur og styrke eierskap til data.

Avhengighet til styrende dokumenter og IKT-styringsmodell

Digital reguleringsplan (DRP) gir de styrende rammene for Forsvarets digitale transformasjon og setter de overordnede føringene som FDSA forholder seg til. FDSA utfyller DRP ved å beskrive hvordan dataarkitektur og *datasentrisk sikkerhet* skal utformes for å realisere et datadrevet forsvar, og er særlig forankret i innsatsområdene DAT (Datadrevet forsvar og KI) og SIK (Sikkerhet). FDSA skal legges til grunn i utviklingen av tidsplaner og prioriteringer innenfor handlingsrommet DRP definerer, og forvaltes av IKT-styringsmodellen.

IKT styringsmodell er Forsvarets rammeverk for enhetlig strategisk styring av Forsvarets IKT. Modellen skal styrke gjennomføringsevnen på IKT-området, og dermed øke operativ evne og bidra til ambisjonene i Forsvarets langtidsplan (LTP) og gjennomføringsplan (FGP). IKT styringsmodell er en integrert del av Forsvarets virksomhetsstyring. Forsvarssjefens porteføljestyre (PSM) prioriterer og styrer porteføljen organisert i seks behovsområder. IKT styringsmodell operasjonaliserer porteføljestyringen av Behovsområde Cyber og IKT (fellesfinansiert IKT), og setter samtidig rammer for egenfinansiert IKT i de øvrige fem behovsområdene: Luft, Land, Maritim, Spesialoperasjoner, Cyber/Space og Understøttelse.

FDSA er også forankret i Stortingets vedtak 991 og 992 (2025-2026), jf. Innst. 440 S (2025-2026) og Prop. 68 S (2025-2026), som gir målbildet et tydelig politisk mandat. Stortinget har vedtatt at Forsvarets data skal lagres slik at den nasjonale kontrollen økes, og at den digitale grunnmuren skal underlegges norsk og europeisk jurisdiksjon. Vedtakene understreker viktigheten av FDSA og gir særlig grunnlag for fundament 1 (Datasuverenitet).

Dette dokumentet vil etterfølges av et teknisk målbilde som konkretiserer arkitekturen gjennom å beskrive de tekniske tjenestene som realiserer *kapabilitetene*, og som inngår i det videre arbeidet med Forsvarets digitale transformasjon.

Virkeområde

FDSA er et styringsinstrument for Forsvarets digitale transformasjon, og operasjonaliseres gjennom IKT-styringsmodellen som beskrevet over, inkludert håndtering av avvik fra målbildet. FDSA treffer applikasjoner og plattformer som produserer, behandler eller deler data, og skal inngå i beslutningsunderlaget for anskaffelse, utvikling og forvaltning av disse.

Forvaltning

Forsvarsstaben (FST) har ansvar for utgivelse, revidering, vedlikehold og godkjenning av FDSA.

Leseveiledning

Kapittel 2 beskriver den strategiske konteksten til FDSA, og noen viktige eksterne rammefaktorer som vil påvirke implementeringen av målbildet.

Kapittel 3 beskriver fundamentet for Forsvarets fremtidige informasjonsforvaltning gjennom ni prinsipper som samlet beskriver hva det i praksis innebærer å være et datasentrisk forsvar.

Kapittel 4 organiserer det datasentriske fundamentet i en konseptuell arkitektur, beskrevet gjennom ti kapabilitetsområder. Kapitlet avgrensar også FDSA mot øvrige initiativer som realiserer deler av arkitekturen.

Kapittel 5 beskriver Forsvarets distribuerte *dataplattform* (FDDP), konseptuelle noder og fire scenarier som illustrerer hvordan enkelte eksisterende og fremtidige applikasjoner og plattformer vil forholde seg til FDDP.

Sentrale begreper i teksten er forklart i kapittel 6, og uthevet med *kursiv og farge* første gang de nevnes.

2 Strategisk kontekst

Krigen i Europa, den økende stormaktsrivaliseringen, økt trusselnivå, polarisering, uforutsig-barhet, og global økonomisk usikkerhet bidrar til et ustabilt internasjonalt landskap. Samtidig utfordrer hybride angrep, cyberoperasjoner og påvirkningskampanjer tradisjonelle forsvars- og beredskapsstrukturer for å utnytte samfunnets sårbarheter. For å sikre operativ handlefrihet og nasjonal kontroll i dette komplekse trusselbildet, må Forsvaret omsette lærdommer fra moderne krigføring og innfri NATOs krav til digital interoperabilitet.

Erfaringer fra moderne krigføring

Krigen i Ukraina har vist hvordan moderne teknologi kan transformere nasjonalt totalforsvar. Mest synlig er bruken av ubemannede systemer, men gjennom DELTA har Ukraina på kort tid tatt frem et system som gjennom en *datasentrisk tilnærming* gir betydelig operativ effekt i et komplekst og dynamisk miljø. DELTA samler data fra mange kilder og utnytter dette til å identifisere, prioritere og engasjere mål i stor skala gjennom effektiv deling og økt bruk av kunstig intelligens. Denne samhandlingen understøttes av utstrakt bruk av moderne løsninger innen sikker deling av data. Systemet er nå i bruk i store deler av de væpnede styrkene og er testet mot NATO-standarder for interoperabilitet og sikkerhet.

For Norge gir DELTA et verdifullt innblikk i hvordan en datasentrisk interoperabilitet kan realiseres sammen med industri og understøttet av tilpasset lovgiving. Erfaringene viser at en slik tilnærming gir høyere beslutningshastighet, bedre situasjonsforståelse og økt fleksibilitet.

Forpliktelser fra NATO

NATO har gjennom sin strategi for digital transformasjon fastslått at alliansen skal kunne gjennomføre *multidomeneoperasjoner* (MDO) innen 2030. Dette målet innebærer at nasjonale kapabiliteter må kunne operere i et felles, datadrevet informasjonsmiljø på tvers av land, sjø, luft, cyber og rom.

For å realisere dette har NATO utviklet en datasentrisk referansearkitektur (DCRA) som setter standarden for fremtidens informasjonsutveksling. DCRA adresserer alliansens behov for å gå fra et komplekst, fragmentert datalandskap basert på applikasjonssentrisk utveksling til en enhetlig datasentrisk tilnærming som legger til rette for sanntids, datadrevet beslutningstaking. Denne fødererte modellen støtter nasjonal suverenitet ved å tillate desentralisert styring av dataressurser, samtidig som den følger felles NATO-rammeverk og standarder.

Federated Mission Networking (FMN) er den tekniske og operative rammen for interoperabilitet i alliansen. FMN utvikles gjennom iterative spiraler der hver spiral introduserer økt modenhet og nye tekniske krav. De nyere spiralene (Spiral 5 og utover) representerer et skifte mot datasentrisitet, og identifiserer utviklingen av semantiske modeller, rammeverk for datastyring og mekanismer for sikker datadeling på tvers av domener som kritiske kapabiliteter.

Det digitale leverandørlandskapet

Det globale leverandørlandskapet utgjør både en mulighet og en strategisk utfordring. Hyperskalerbare *skytenester* gir tilgang til kapasitet og funksjonalitet som overstiger det nasjonale aktører realistisk kan utvikle selv. Samtidig har Stortinget gjennom Vedtak 991 og 992 (2025-2026) jf. Innst. 440 S (2025-2026) vedtatt at Forsvarets graderte og ugraderte data skal lagres på en måte som reduserer risiko og øker den nasjonale kontrollen, og at Forsvarets digitale grunnmur skal underlegges norsk og europeisk jurisdiksjon. Innstillingen understreker at «suverenitet over Forsvarets data ikke kan baseres på kontraktsvilkår alene, men må sikres gjennom tilstrekkelig nasjonal kontroll over både den fysiske infrastrukturen og den rettslige rammen den opereres innenfor.»¹

I tillegg til fysisk infrastruktur og rettslig ramme, som vedtaket trekker frem, er teknologiske standarder og formater en tredje forutsetning for suverenitet. Hyperskalerbare skyplattformer kan understøtte både åpne og proprietære løsninger. Benyttes åpne standarder, kan data og arbeidslasten flyttes mellom leverandører og plattformer ved behov, mens proprietære løsninger øker risikoen for teknisk innlåsing, selv innenfor norsk eller europeisk jurisdiksjon. Særlig avgjørende er hvordan data lagres, der åpne formater som for eksempel Parquet og Iceberg gjør det mulig å migrere eller replikere data uavhengig av underliggende plattform.

Dette forsterker viktigheten av og retningen i målbildet, hever terskelen for løsninger som svekker nasjonal kontroll, og stiller krav om at Forsvaret evner å vurdere avveininger mellom funksjonalitet og kontroll på en eksplisitt og dokumentert måte.

¹ Innst. 440 S (2025-2026) s. 9.

3 Det datasentriske fundamentet

Målbildet for Forsvarets datasentriske arkitektur er bygget på tre grunnpilarer som til sammen utgjør fundamentet for vår fremtidige informasjonsforvaltning:

- Nasjonal suverenitet og kontroll
- Datastyring og utnyttelse
- Samvirke og robusthet

De påfølgende sidene detaljerer de ni sentrale områdene som konkretiserer dette fundamentet. Samlet beskriver disse punktene hva det innebærer å være et datasentrisk forsvar i praksis, og setter de nødvendige kravene for å sikre at data løftes frem som en strategisk ressurs for å realisere vårt datadrevne forsvar.



Figur 2 Pilarer og fundamenter i Forsvarets datasentriske arkitektur



1. Datasuverenitet

Forsvaret skal kunne operere uavhengig av enkeltleverandører eller tredjeparter for kritiske kapasiteter. Dette innebærer tilstrekkelig eierskap over egne data, og teknologisk handlefrihet for å sikre operativ evne i fred, krise og krig.

Stortinget har gjennom Innst. 440 S (2025-2026) vedtatt at Forsvarets graderte og ugraderte data skal lagres på en måte som reduserer risiko og øker den nasjonale kontrollen, og at den digitale grunnmuren i Forsvaret skal underlegges norsk og europeisk jurisdiksjon.

Relevante DRP-prinsipper:	DAT1 – Datasuverenitet og strategisk handlefrihet	APP2 – Standardisering
	FSL5 – Kritiske applikasjoner i Forsvarets egne datasentre	

1.1 Eierskap og kontroll

Forsvaret skal ha tilstrekkelig eierskap og kontroll over egne data og deres mening. Det betyr at Forsvaret har evne til å flytte, endre eller skjerme kritiske kapasiteter uten avhengighet til tredjeparter. Nasjonal, sikret infrastruktur skal benyttes for kritiske funksjoner for å ivareta strategisk handlefrihet uavhengig av sikkerhetspolitiske endringer. Lagring av Forsvarets data og forvaltning av den digitale grunnmuren skal skje under norsk og europeisk jurisdiksjon.

1.2 Motvirke teknologisk innlåsing

Forsvaret skal benytte åpne, dokumenterte standarder og grensesnitt som ikke er knyttet til en enkeltleverandør, med en preferanse for å følge valg gjort av NATO og nære allierte. Dette sikrer teknologisk handlefrihet og evne til rask omstilling uten tap av datatilgang i fred, krise og krig.

1.3 Nasjonal egenevne og kompetanse

Forsvaret skal besitte nødvendig teknologisk kompetanse til å forstå, utnytte og endre egne algoritmer, datamodeller og grensesnitt. Denne egenevnen er en forutsetning for datasuverenitet og sikrer at Forsvaret ikke blir låst til enkeltleverandører og tredjeparter for å opprettholde operativ evne.

1.4 Nasjonal kryptokontroll

Sikkerhetsmekanismer for graderte data skal forvaltes under eksklusiv nasjonal kontroll gjennom hele livssyklusen. Krypteringsnøkler skal oppbevares adskilt fra tredjeparts infrastruktur, slik at fremmed lovgivning eller tvangsmidler ikke kan gi innsyn i informasjonen.



2. Datasentrisk sikkerhet

Sikkerhetsarkitekturen skal sikre selve **dataobjektene**, i tillegg til systemene og applikasjonene som forvalter dem. Dette er en forutsetning for kontrollert informasjonsflyt og samvirke på tvers av domener og graderingsnivåer.

Relevante DRP-prinsipper:	SIK3 – Security by Design og Zero Trust	FSL4 – Verifisert og føderert identitet
	PV2 – Dataminimering og formålsbegrensning	

2.1 Sikkerhet følger data

Sikkerhetsmekanismer, inkludert kryptering og rettighetsstyring, skal være knyttet direkte til dataobjektet gjennom hele livssyklusen for å garantere dataens integritet og konfidensialitet, uavhengig av hvor objektet befinner seg.

2.2 Felles autoritativ identitet

Forsvaret skal forvalte en enhetlig og verifiserbar identitet for personell, materiell og informasjonssystemer. Denne identiteten skal utgjøre grunnmuren for datasentrisk sikkerhet, og forankres i autorative kilder for å sikre entydig identifikasjon, muliggjøre sømløs samhandling på tvers av domener og med allierte, samt garantere autonom tilgang til egne systemer under alle forhold, også ved brutt eller degradert samband (DDIL).

2.3 Unike identifikatorer og maskinell merking

Alle informasjonsobjekter og ressurser skal ved opprettelse tildeles en unik og varig global identifikator som fungerer som felles referansenøkkel. Informasjon skal klassifiseres og merkes maskinelt i tråd med internasjonale standarder (f.eks. NATO STANAG 4774). Dette muliggjør automatisert tilgangsstyring der data vil være tilgjengelig for alle autoriserte aktører i sanntid.

2.4 *Attributtbasert tilgang* («ABAC»)

Tilgang til data tildeles dynamisk basert på verifiserbare attributter ved bruker, system, kontekst og tid målt opp mot dataenes skjermings- og delingsbetingelser. Dette styres etter *Zero Trust*-prinsipper, som innebærer at ingen bruker eller enhet har implisitt tillit, og at enhver forespørsel må verifiseres uavhengig av hvor den kommer fra. Denne finmaskede tilgangsstyringen gjør det mulig å dele data tryggere og mer automatisk med dem som oppfyller forhåndsdefinerte sikkerhetskrav, og styrker etterlevelsen av personvern.

2.5 Flyt mellom graderingsnivåer

Arkitekturen skal understøtte sikker utveksling av data mellom ulike graderingsnivåer. Godkjente sikkerhetsbarrierer skal kontrollere og vaske informasjonen i sanntid. Valideringen skal inkludere en vurdering av dataobjektets skjermings- og delingsbetingelser opp mot egenskapene ved den mottakende applikasjonen.



3. Automatisert etterlevelse

Sikkerhetspolicyer og regelverk skal operasjonaliseres gjennom kode («*policy-as-code*») og håndheves automatisk og maskinelt for å sikre etterlevelse, redusere risiko for menneskelig feil og garantere *sporbarhet*. Sikkerhet og personvern skal bygges inn fra start, fremfor som en ettertanke.

Relevante DRP-prinsipper:

SIK3 – Security by Design og Zero Trust

PV1 – Personvern og personopplysningssikkerhet

3.1 Programmatisk policy og «PEP»

Regelverk skal håndheves automatisk ved at tekniske vaktposter («Policy Enforcement Points») validerer enhver transaksjon mot dataobjektets identifikator og merking (ref. 1.2.3) før datautveksling finner sted. Dette sikrer at deling av informasjon alltid skjer innenfor rammene av gjeldende lovverk og sikkerhetsbestemmelser.

3.2 Uavhengig kontroll

Sikkerhetshåndteringen skal flyttes ut av selve applikasjonen. Dette gjør Forsvaret uavhengig av leverandørens innebygde mekanismer og sikrer en helhetlig håndheving på tvers av informasjonssystemer. Dette realiseres gjennom et distribuert arkitekturmønster som fungerer som en uavhengig vaktpost mellom applikasjonen og omverden.

3.3 Autonom håndheving av policy og regelverk

Tekniske vaktposter skal fungere autonomt i tilfeller der brutt eller degradert samband (DDIL) for å sikre kontinuerlig håndheving av policy lokalt. Dette muliggjøres gjennom en lokal, signert kopi av regelverket («Policy Cache») og desentralisert identitetsverifisering, og sikrer operativ handlefrihet og informasjonsflyt uavhengig av sentrale tjenester.

3.4 Innebygd sikkerhet og personvern («Security and privacy by design»)

Applikasjoner skal designes, anskaffes og implementeres med tekniske sikkerhets- og personvernmechanismer («guardrails») som en integrert del av løsningen, slik at sikkerhet og personvern ivaretas fra start fremfor som en ettertanke. Dette sikrer at brukeren overholder sikkerhetskrav og regelverk uten behov for inngående teknisk sikkerhetskompetanse.

3.5 Opphav («data provenance») og sporbarhet («data lineage»)

Det skal etableres en uforanderlig logg over dataenes opphav, transformasjoner og tilgangshistorikk. Mekanismer for *anonymisering*, *pseudonymisering* eller sletting skal benyttes for å sikre at loggdata som omfatter personopplysninger, begrenses til det som er nødvendig for sikkerhet, revisjon og etterlevelse. Loggføring skal skje lokalt, med automatisk synkronisering til sentrale tjenester så snart prioritet og tilgjengelige kommunikasjonsbærere tillater det.



4. Desentralisert eierskap

Desentralisert eierskap representerer en fundamental endring i hvordan Forsvaret forvalter sine data ved at ansvaret skal distribueres til definerte domener med autonomi til å forvalte egne data. Autonomien skal utøves innenfor felles prinsipper og standarder som fastsettes av en sentral autoritet for informasjonsarkitektur med mandat til å stille krav og følge opp etterlevelse.

Relevante DRP-
prinsipper:

DAT2 – Desentralisert eierskap

4.1 Domenebasert ansvar

Definerte *datadomener*, som omfatter både operative søyler (f.eks. hær, sjø, luft) og virksomhetsbærende funksjoner (f.eks. HR, logistikk, økonomi), skal eie og forvalte egne data. Ansvaret innebærer både å sikre datakvalitet for operativ effekt, effektiv forvaltning og korrekt rapportering, og å definere og forvalte domenets *begrepsapparat* slik at informasjonen forstås entydig av alle mottakere. Store domener kan dekomponeres i sub-domener for å ivareta nødvendig granularitet og fleksibilitet; eksempelvis kan logistikk brytes ned i områder som forsyning, lager, transport og vedlikehold.

4.2 Føderert styringsmodell

Lokalt eierskap i domenene skal balanseres med sentrale standarder og styringsmekanismer som sikrer at data og *ontologier* fra ulike domener kan sammenstilles sømløst. Kjørereglene omfatter krav og beste praksis for dokumentasjon av begrepsapparat og datamodeller, tekniske standarder for dataformater og protokoller, og krav til sikkerhet og merking av data. Som et særskilt ansvar skal den sentrale autoriteten fungere som beslutningsmyndighet for harmonisering ved overlapp eller tvil om begrepsbruk på tvers av ulike domener.

4.3 Autorative fellesdata

Utpekte domener skal eie og forvalte autoritative kilder (*grunndata*) for tverrgående entiteter som personell, materiell og geografi, slik at denne informasjonen kan konsumeres som en omforent sannhet av andre domener. Ansvaret er todelt og omfatter forvaltning både av datakildene og eierskap til å definere og forvalte begrepsapparatet for de tverrgående entitetene.



5. Data som produkt

Data skal tilgjengeliggjøres som kvalitetssikrede produkter, optimalisert for et konkret formål, men tilrettelagt for gjenbruk. Dette skiftet fra system- til produktfokus er nødvendig for å understøtte et datadrevet forsvar.

Relevante DRP-prinsipper:

DAT1 – Datasuverenitet og strategisk handlefrihet

DAT2 – Desentralisert eierskap



Et *dataprodukt* er en datasamling som er rettet inn mot et spesifikt brukstilfelle, og som har en eier som er ansvarlig for å forvalte og tilgjengeliggjøre produktet.

5.1 Kvalitetssikring og livssyklus håndtering

Dataprodukteier garanterer for kvalitet og tilgjengelighet, slik at informasjonen kan benyttes direkte i beslutningsprosesser, fra strategisk ledelse til taktisk utførelse. Data forvaltes i henhold til FAKTISK-prinsippene, inkludert arkivlovverk og sikkerhetskrav, og saneres når lovlig/operativt behov opphører.

F	Finnbare: Brukere skal kunne finne Forsvarets dataprodukter og få innsikt i hvem som er ansvarlig for dem, hva de kan forvente av dem, og hvordan de kan få tilgang til dem.
A	Anvendelige: Brukere skal kunne anvende Forsvarets dataprodukter, ved at de er tilgjengelige gjennom dokumenterte standard grensesnitt og via felles plattformer og tjenester.
K	Klare: Brukere skal ha en klar forståelse av meningsinnholdet i Forsvarets dataprodukter, ved at de bruker et felles begrepsapparat og gir tilstrekkelig kontekst.
T	Troverdige: Brukere skal kunne ha tillit til Forsvarets dataprodukter, gjennom at det så langt som mulig gjøres synlig hvordan produktene er produsert og hvilke kilder de tar utgangspunkt i.
I	Interoperable: Brukere skal enkelt kunne integrere Forsvarets dataprodukter med hverandre og med eksterne kilder, gjennom at de bruker felles og standardiserte dataformater, begrepsapparat, og metadatastandarder.
S	Sikre: Brukere skal kunne ha tillit til at Forsvarets dataprodukter behandles på en sikker måte, der tilgang styres automatisk ut fra produktenes skjermings- og delingsbetingelser, der produktenes integritet og tilgjengelighet bevares, og der bruk og tilgang registreres og loggføres.
K	Koblede: Brukere skal se at Forsvarets dataprodukter er koblet sammen slik at sammenhenger og avhengigheter mellom forskjellige produkter er synlige.

5.2 Standardiserte produktbeskrivelser

Ethvert dataprodukt skal ha en entydig identifikator, og følges av *metadata* som gjør det selvforklarende, og som tydelig beskriver produktets opphav, oppdateringsfrekvens, nøyaktighet, distribusjonsregler og levetid.

5.3 Brukerorientert utvikling

Dataprodukter skal designes for gjenbruk. Det skal etableres mekanismer for kontinuerlig tilbakemelding fra bruker til dataforvalter for å videreutvikle produktene.

5.4 Digitale tvillinger

Digitale tvillinger skal etableres som sammensatte dataprodukter basert på autoritative sanntidsdata for å legge til rette for simulering, prediktivt vedlikehold og beslutningsstøtte.



6. Selvbetjent bruker- og utvikleropplevelse

Autoriserte brukere skal ha umiddelbar tilgang til å finne og utnytte Forsvarets dataprodukter gjennom felles selvbetjeningsløsninger.

Relevante DRP-
prinsipper:

DAT2 – Desentralisert eierskap

6.1 Felles *dataproduktkatalog* og -verktøykasse

En føderert og søkbar katalog over organisasjonens autoritative dataprodukter muliggjør gjenfinning og gjenbruk. Allerede utviklede komponenter for prosessering, visualisering og utnyttelse av data gjøres tilgjengelig for gjenbruk.

6.2 Umiddelbar tilgang

Autoriserte brukere skal kunne abonnere på datastrømmer gjennom selvbetjeningsløsninger med umiddelbar effekt, uten forsinkende saksbehandlingsledd.

6.3 Selvbetjent infrastruktur

Plattformen skal tilby verktøy som setter personell med og uten teknisk spisskompetanse i stand til å utnytte data for analyser og beslutningsstøtte, med et fokus på å bygge en god bruker- og utvikleropplevelse.

6.4 Kontrollerte delingssoner

Det etableres sikre soner for datadeling med totalforsvaret, allierte, industri og akademia for å legge til rette for effektivt samvirke uten å eksponere Forsvarets kjernenettverk, og innenfor gjeldende juridiske rammer, herunder personvern.



7. Semantisk og teknisk interoperabilitet

Informasjon skal struktureres etter felles ontologier og baseres på gjeldende NATO-standarder for å sikre entydig forståelse mellom mennesker og maskiner, i alt fra effektiv virksomhetsstyring til samvirke med totalforsvaret og allierte styrker i komplekse operasjoner.

Relevante DRP-prinsipper:	APP5 – Interoperability by design	APP2 – Standardisering
	SAM1 – Integrert samvirke med allierte, totalforsvaret og andre relevante aktører	

7.1 Felles begrepsapparat og ontologi

Et felles begrepsapparat understøttet av ontologier skal etableres for å sikre entydig forståelse. Der begrepsapparatet er en samling av begreper som etablerer et felles fagspråk gjennom standardiserte definisjoner, formaliserer ontologiene de logiske sammenhengene mellom begrepene gjennom relasjoner og regler. Ontologiene som forvaltes i det enkelte datadomene skal kobles til Forsvarets sentralt forvaltede øvre ontologi for å sikre at data kan utnyttes på tvers av domener, med totalforsvaret og allierte.

Eksempel: Begrepsapparatet definerer entydig hva en «trussel» er. Ontologien definerer hvordan trusselen logisk relaterer seg til «posisjon», «kapasitet» og «intensjon».

7.2 Felles formater og modeller

Det skal etableres felles dataformater, informasjonsmodeller og grensesnitt for å sikre evne til sømløs informasjonsflyt og samvirke mellom systemer og avdelinger i Forsvaret. Så langt mulig skal disse baseres på NATO-standarder og referansemodeller for å sikre Forsvarets evne til å inngå i koalisjonsoperasjoner. Der nasjonale behov krever tilpasninger skal vi forvalte en oversettelse mot NATOs modeller slik at våre data kan utveksles med allierte uten tap av mening.

7.3 Maskinlesbarhet og klargjøring for KI

Data skal lagres og distribueres i maskinlesbare formater som er koblet til Forsvarets standardiserte ontologier. Dette gjør at de kan knyttes sammen i *kunnskapsgrafer* for å legge til rette for automatisert sammenstilling av data og bruk av kunstig intelligens til avansert beslutningsstøtte.



8. Robusthet i felt

Arkitekturen skal understøtte operasjoner, databehandling og lagring i degraderte miljøer (DDIL) for å opprettholde motstandsdyktighet i fred, krise og krig. Enheter skal kunne operere og samvirke selvstendig, med automatisk synkronisering mot sentrale systemer når forbindelsen gjenopprettes.

Relevante DRP-prinsipper:	FSL2 – Differensierte plattformtjenester	FSL3 – Autonomi og handlefrihet
	SIK4 – Digital beredskap og cyberoperativ evne	

8.1 Distribuert robusthet og lokal autonomi

Prosessering av dataprodukter skal så langt som mulig skje distribuert og ikke i en sentral infrastruktur. Data og applikasjoner i fog- og edge-miljøer skal kunne operere selvstendig ved begrenset, ustabil eller manglende tilkobling til sentrale systemer. For å opprettholde felles situasjonsforståelse skal systemene automatisk synkroniseres når forbindelsen gjenopprettes. Automatisert *replikering* på tvers av geografiske lokasjoner og plattformer skal proaktivt sikre redundans og tilgjengelighet i tråd med spesifikasjonene i *datakontrakten*, selv ved bortfall av kommunikasjonslinker eller infrastruktur.

8.2 Dataprosessering i felt

Data skal prosesseres der det gir størst effekt, på tvers av *cloud*, *core*, *fog* og *edge*. Der det er mulig skjer dette lokalt på sensorer og plattformer for å korte ned beslutningssløyfer og best mulig utnytte tilgjengelig overføringskapasitet. Tunge analyser og administrative prosesser kjøres typisk sentralt for å utnytte historisk og aggregert informasjon, mens tidskritiske funksjoner kjøres lokalt på sensorer og plattformer for å sikre tempo og autonomi.

8.3 Uavhengighet av bærer

Data skal merkes slik at Forsvarets applikasjoner og plattformenes utvekslingsmekanismer automatisk kan velge best mulig kommunikasjonsbærer (satellitt, 5G, fiber, felt-radio) for overføring, når tilgjengelig båndbredde er begrenset, basert på tilgjengelighet og operativt behov. Denne merkingen gjør infrastrukturen i stand til å rute kritiske dataprodukter via den mest egnede kanalen i tråd med kravene definert i dataproduktet.



9. Integrasjon og modernisering

Løst koblet arkitektur skal sikre robust og sømløs informasjonsflyt mellom moderne kapasiteter og eksisterende systemer.

Relevante DRP-prinsipper:	APP1 – Modulære applikasjoner og løse koblinger	APP2 – Standardisering
	APP4 – Variantbegrensning	APP6 – Livssyklusstyring av applikasjoner

9.1 Skille mellom data og applikasjoner

Data skal forvaltes som en selvstendig ressurs, lagres i åpne formater og frigjøres fra applikasjonene som genererer dem. Applikasjoner skal behandles som utskiftbare konsumenter og produsenter av data som kan ha egen persistering, men som skal avgi informasjon av felles verdi gjennom standardiserte grensesnitt. Dette sikrer at historikk og informasjonsverdi bevares uavhengig av utskiftninger av applikasjonene.

9.2 Løst koblede arkitekturer

Sårbare direktekoblinger («punkt-til-punkt») skal erstattes av løst koblede applikasjoner ved bruk av standardiserte API-er og hendelsesbaserte strømmer for å sikre fleksibilitet og skalerbarhet.

9.3 Håndtering av eldre systemer

Eldre systemer, inkludert *digitalisert materiell*, («legacy») skal innkapsles gjennom tekniske abstraksjonslag som eksponerer data via standardiserte grensesnitt, og erstattes når en helhetlig kost-nytte-vurdering tilsier det. Dette sikrer at teknisk gjeld ikke hindrer innovasjon eller operativ utnyttelse av data.

9.4 Ende-til-ende *observerbarhet*

Arkitekturen skal overvåke dataflyten, innad i og på tvers av datadomener, i sanntid. Kontinuerlig måling av data- og leveransequalität, inkludert forsinkelser, volum og feilrater, garanterer operativ presisjon og evne til proaktiv feilretting.

4 Konseptuell arkitektur

Det datasentriske fundamentet beskriver hva det innebærer å være et datasentrisk forsvar. Dette kapittelet organiserer fundamentet i en konseptuell arkitektur, i tråd med prinsipper fra DCRA og FMN. Arkitekturen beskriver hvilke evner Forsvaret må besitte for å forvalte, dele og utnytte data, internt på tvers av domener og informasjonssystemer, og eksternt med totalforsvaret og allierte.

Disse evnene omtales som kapabiliteter der en kapabilitet er evnen til å levere en bestemt effekt, uavhengig av hvordan den realiseres eller hvilke teknologier som brukes.² Kapabilitetene er derfor relativt stabile over tid selv når teknologien endres.

Arkitekturen er organisert i ti kapabilitetsområder som gir det overordnede bildet av hva en datasentrisk arkitektur må dekke. De åtte første kapabilitetsområdene angår data direkte, mens plattform og infrastruktur og kommunikasjonsinfrastruktur leverer den digitale grunnmuren de øvrige realiseres på.

1. **Føderert datastyring:** Distribuert ansvar innenfor felles kjøreregler
2. **Datasentrisk sikkerhet:** Sikkerheten følger dataene med tilgang styrt av policy
3. **Dataprodukter:** Domenene gjør data forståelig, delbar og gjenbrukbar
4. **Datakatalog:** Oversikt over dataprodukter og begreper
5. **Datatjenester:** Selvbetjent utvikling og drift av dataprodukter
6. **Dataforvaltning:** Metadata, semantikk og kvalitet følger dataproduktet i styrt livssyklus
7. **Datautveksling:** Selvbetjent oppdagelse og standardisert deling av dataprodukter
8. **Datautnyttelse:** Understøttelse av beslutning og handling
9. **Plattform og infrastruktur:** Kjøremiljø på tvers av cloud, core, fog og edge
10. **Kommunikasjonsinfrastruktur:** Uavhengighet av bærer



Figur 3 Kapabilitetsområder i Forsvarets datasentriske arkitektur

² NATO Architecture Framework Version 4.1 (2026) s. 196.

Føderert datastyring

Føderert datastyring fastsetter felles spilleregler for hvordan data forvaltes, deles og sikres på tvers av Forsvaret, med totalforsvaret og med allierte. Domenene forvalter sine egne data med autonomi, mens felles standarder, roller og etterlevelseskraav hindrer at autonomien fører til fragmentering. Regler vedtas og versjoneres sentralt, og håndheves lokalt i hele arkitekturen.

Området brytes videre ned i følgende kapabiliteter:

- Styringsmodell og myndighet
- Prinsipper, policy og standarder
- Roller, ansvar og eierskap
- Maskinell styring og etterlevelse
- Frigivelsesforvaltning

Datasentrisk sikkerhet

Datasentrisk sikkerhet innebærer at beskyttelsen følger dataene, ikke applikasjonene eller nettverket rundt dem. Et dataobjekt bærer sin egen sikkerhetsmerking gjennom hele livssyklusen, uavhengig av hvor det lagres, prosesseres eller deles. Området omsetter sikkerhetskravene fra styringsregimet til kjøretidslogikk og håndhever dem ved enhver datatransaksjon.

Området brytes videre ned i følgende kapabiliteter:

- Føderert identitet- og tilgangsstyring
- Informasjonsflyt og delingskontroll
- Sikkerhetsklassifisering og merking
- Kryptering og nøkkelforvaltning
- Sikkerhetslogging og overvåking

Dataprodukter

Dataprodukter er den bærende enheten i arkitekturen, og de er kapabiliteter i seg selv. Det er gjennom dataprodukter at Forsvarets data blir delbare, forståelige og gjenbrukbare, og de øvrige kapabilitetsområdene er bygget for å understøtte dem. Dataproduktene eies og forvaltes av datadomenene, som omfatter både operative søyler (f.eks. hær, sjø, luft) og virksomhetsbærende funksjoner (f.eks. HR, logistikk, økonomi).

Dataprodukter grupperes gjerne i operasjonelle og analytiske dataprodukter. Operasjonelle dataprodukter støtter pågående operasjoner, som sensor-til-effektor-sløyfen og eksekvering av KI-modeller, med vekt på nær-sanntidsinformasjon og rask beslutningstaking. Analytiske dataprodukter støtter analyse, rapportering og trening av KI-modeller, med vekt på historikk, trender og innsikt.

Datakatalog

Datakatalogen er en føderert katalog over Forsvarets begreper og dataprodukter. Dataproduktkatalogen, som er en sentral del av kapabiliteten, gjør dataprodukter tilgjengelige for å oppdages, abonneres på og gjenbrukes i henhold til dataproduktets kontrakt. I tillegg gir datakatalogen oversikt over begreper og metadata, som gjør både dataprodukter og data forståelige. Sistnevnte omfatter blant annet data som bearbeides og transformeres mot et dataprodukt, uten selv å bli publisert.

Datatjenester

Datatjenester er kapabilitetene som henter inn, bearbeider og analyserer data. Kapabilitetene tilbys som selvbetjente tjenester, slik at et domene kan etablere og foredle et dataprodukt uten å bygge egen infrastruktur, med selvbetjening fremfor bestilling.

Området brytes videre ned i følgende kapabiliteter:

- Innhenting og integrasjon
- Behandling og transformasjon
- Analyse-, KI- og annoteringstjenester
- Datadistribusjon og føderert deling

Dataforvaltning

Dataforvaltning fastsetter hva et dataprodukt er og hva det betyr, gjennom felles begreper og ontologier, og sikrer at det har tydelig eierskap, en kontrakt som beskriver betingelsene for tilgang og bruk, definert kvalitet og en styrt livssyklus. Området er kjernen i realiseringen av FAKTISK-prinsippene. Området forvalter også Forsvarets grunn- og referansedata, som autoritative kilder for tverrgående entiteter.

Området brytes videre ned i følgende kapabiliteter:

- Begreps-, ontologi- og modellforvaltning
- Dataoppdagelse og metadataforvaltning
- Grunn- og referansedataforvaltning
- Datakvalitetsstyring
- Livssyklusforvaltning

Datautveksling

Datautveksling er evnen til å dele data på tvers av Forsvaret, med totalforsvaret, allierte, industri og akademia, uten tap av mening og kontroll.

Området brytes videre ned i følgende kapabiliteter:

- Grensesnitt- og profilforvaltning
- Semantisk samordning
- Samvirketesting

Datautnyttelse

Datautnyttelse er der data omsettes til operativ verdi. Området beskriver anvendelsesområder arkitekturen understøtter, fremfor kapabiliteter arkitekturen leverer. Konsumentene spenner fra applikasjoner og informasjonssystemer til digitalisert materiell og taktiske plattformer i felt, som alle konsumerer dataprodukter fremfor å integrere direkte mot kildene.

Området omfatter følgende anvendelsesområder:

- Situasjonsforståelse
- Kommando og kontroll

- Virksomhetsstyring
- Samvirke og interoperabilitet

Plattform og infrastruktur

Plattform og infrastruktur leverer kjøremiljøet som gjør de øvrige kapabilitetsområdene operative, fra sentrale datasentre til sensorer og plattformer i felt. Kjøremiljøet strekker seg over fire lag med ulik kapasitet og rolle: *cloud* gir skalerbar og føderert kapasitet, *core* er den redundante kjernen, *fog* er desentraliserte og fremskutte noder, og *edge* er de taktiske enhetene ytterst. Det som er pakket for cloud skal kunne flyttes til en taktisk plattform uten kodeendringer, og lagene er derfor samme plattform i ulik størrelse.

Området brytes videre ned i følgende kapabiliteter:

- Fysisk infrastruktur
- Virtuell infrastruktur
- Applikasjonskjøremiljø og orkestrering
- Plattformnære datatjenester
- Utviklingsstøtte
- Kontrollplan og driftsstøtte

Kommunikasjonsinfrastruktur

Kommunikasjonsinfrastrukturen binder instansene av plattformen sammen, fra datasentre til taktiske noder i felt. Dataprodukter merkes slik at utvekslingsmekanismene automatisk kan velge best egnet bærer når båndbredden er begrenset, basert på tilgjengelighet og operativt behov.

Området omfatter blant annet følgende bærere og beskyttelsesmekanismer:

- Fiber
- Radio
- 5G
- Satcom
- Krypto

Avgrensninger mot øvrige initiativer

Flere av kapabilitetsområdene realiseres gjennom initiativer med egne målbilder og egen eier. Under beskrives hvilke kapabiliteter utvalgte strategiske initiativ realiserer, og hvor grensene mellom dem går.



Figur 4 Avgrensning av FDDP, MilSky, Datasenter, FKI og ERP mot kapabilitetsområdene i FDSA

Forsvarets distribuerte dataplattform (FDDP) realiserer kjernen i FDSA, og binder sammen produsenter og konsumenter av data på tvers av domener, applikasjoner og lokasjoner. FDDP realiserer teknisk kapabilitetene innenfor Dataforvaltning, Datakatalog, Datatjenester, Datautveksling og publisering av Dataprodukter. FDDP beskrives nærmere i kapittel 5.

MilSky og Datasenter realiserer sammen kapabilitetsområdet Plattform og infrastruktur. Datasenter bygger og drifter de fysiske lokasjonene, med redundans på tvers av landet. MilSky leverer kjøremiljøet som driftes i disse lokasjonene, på tvers av cloud, core, fog og edge. FDSA stiller krav til at kjøremiljøet er likt på tvers av lagene og kan operere autonomt ved brutt samband, mens målbildet for plattformen og de fysiske lokasjonene forvaltes i egne styringsdokumenter.

Forsvarets kommunikasjonsinfrastruktur (FKI) realiserer Kommunikasjonsinfrastruktur. FKI leverer bærerene og den kryptografiske beskyttelsen av sambandet mellom dem. FDSA stiller krav til at dataprodukter kan rutes over den mest egnede bæreren, mens valg og utbygging av bærere forvaltes av Forsvarets digitale grunnmur.

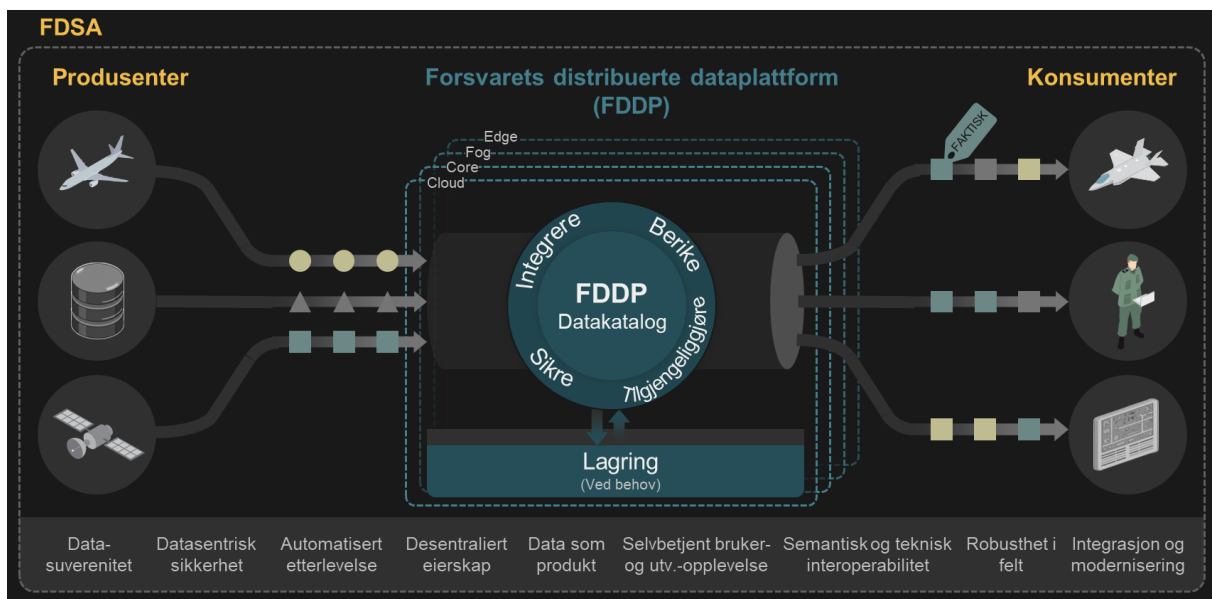
ERP er en applikasjon i Datautnyttelse, og understøtter Virksomhetsstyring. ERP er samtidig en sentral produsent av autoritative data om personell, materiell og organisasjon, som tilgjengeliggjøres som dataprodukter gjennom FDDP. Løsningen har egen persistering og egne integrasjoner, og er etter arkitekturens regler en utskiftbar konsument og produsent av data.

5 Forsvarets distribuerte dataplattform

Forsvarets distribuerte dataplattform (FDDP) er kjernen i realiseringen av FDSA. FDDP binder produsenter og konsumenter av data sammen på tvers av domener, applikasjoner og lokasjoner, og gjør data søkbare, tilgjengelige og klare for bruk.

Fra produsentsiden gir FDDP domenene verktøy og tjenester for å hente inn, transformere og berike data til dataprodukter gjennom Datatjenester, med eierskap, kontrakt og kvalitet ivaretatt gjennom Dataforvaltning. Fra konsumentensiden gir FDDP et felles innslagspunkt for å oppdage dataprodukter gjennom Datakatalogen, med standardiserte grensesnitt for å ta dem i bruk, i tråd med kapabilitetene i Datautveksling. Data gjøres tilgjengelige enten der de oppstår, gjennom *virtuell dataatilgang*, eller ved at dataene lagres i FDDP. Sistnevnte er særlig aktuelt ved sammenstilling av flere kilder eller for å bevare historiske data. FDDP realiserer på denne måten teknisk kapabilitetene innenfor Dataforvaltning, Datakatalog, Datatjenester, Datautveksling og publisering av Dataprodukter, som beskrevet i kapittel 4.

FDDP er konseptuelt én plattform med distribuerte egenskaper, som realiseres teknisk som noder på tvers av cloud, core, fog og edge, derav navnet Forsvarets *distribuerte* dataplattform.



Figur 5 Illustrativ fremstilling av FDDP og forskjellen mellom FDDP og FDSA

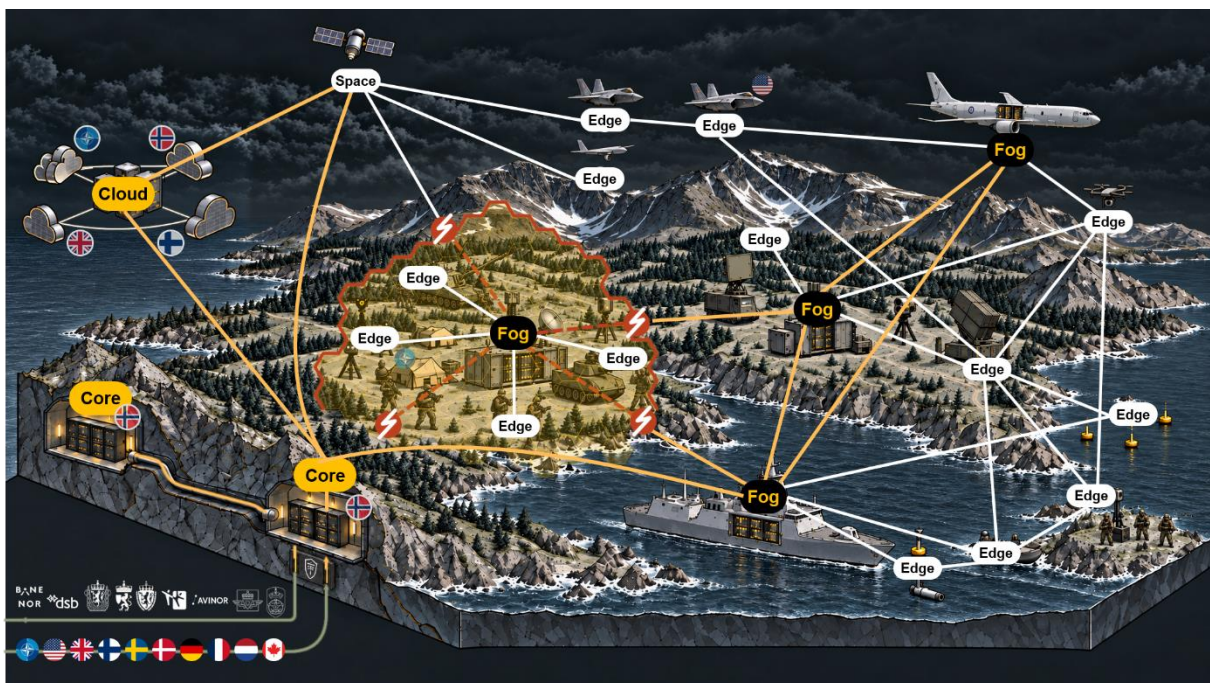
Konseptuelle noder i FDDP

FDDP realiseres som noder der en node er en instans av FDDP, med det utvalget av kapabiliteter ressursene på nodens lokasjon tillater. Noder kan eies og driftes både sentralt og av det enkelte domene. Teknologivalg kan avvike, for eksempel ved at tunge analyseverktøy erstattes med lettvekts, innebygde løsninger i begrensede miljøer. Sammen muliggjør nodene dataflyt på tvers av Forsvaret, og hver node skal kunne fortsette å virke ved degradert eller bortfalt samband.

Sentrale noder, i cloud og core, har det bredeste utvalget av kapabiliteter og størst kapasitet for lagring, prosessering, analyse og KI. Core bygger en georedundant kjerne i Forsvarets sentrale og regionale datasentre, der tunge analytiske prosesser kjøres, KI-modeller trenes før de deployeres, og tverrgående dataprodukter forvaltes og utveksles, som personell- og materielldata, med store historiske datamengder. Cloud benyttes for ikke-kritiske og godkjente arbeidslaster med elastisk kapasitet.

Fremskutte noder, i fog, har begrenset prosesseringskraft, lagringskapasitet og båndbredde og et utvalg kapabiliteter tilpasset lokal produksjon og konsum. Sensordata fra tilknyttede kilder fusjoneres lokalt til et situasjonsbilde, og det er ofte det bearbejdede resultatet og ikke rådataene, som sendes videre til sentrale noder når forbindelsen tillater det. Et datarom på en fregatt er et eksempel på en fremskutt node som opererer på denne måten.

Taktiske noder, på edge, er de minste og mest begrensede, fordi de opererer i miljøer som setter strenge begrensninger på størrelse, vekt og effekt. Analyse og KI-modeller kjører frittstående, uten avhengighet til nettverk. Kommunikasjon med andre noder skjer gjennom komprimerte, hendelsesbaserte protokoller, ofte uten en sentral megler som koordinerer utvekslingen. En enhet på en CV90 er et eksempel på en taktisk node som inneholder bare de kapabilitetene som er nødvendige for lokal produksjon, lagring og policyhåndheving, forhåndspopolert med det den trenger for planlagte operasjoner.



Figur 6 Illustrativ fremstilling av FDDP-noder og dataflyten mellom dem

Kjernekapabiliteter i FDDP

Kapabilitetene FDDP realiserer er beskrevet i kapittel 4. Fire av dem forklares nærmere her, for å tydeliggjøre hva FDDP er i praksis.

Innhenting og integrasjon (Datatjenester): Forsvarets produsenter av data dekker et bredt spekter av kilder, fra sensorer til forvaltningssystemer, med hver sine protokoller, formater og sikkerhetsregimer. Denne kapabiliteten kapsler inn kompleksiteten gjennom et felles mønster, der hver klasse av kilder får en dedikert inngang som oversetter kildedataene til standardiserte dataformater.

Behandling og transformasjon (Datatjenester): Gjennom automatiserte prosesser økes verdien og brukbarheten av data. Rådata knyttes til felles begrepsapparat, ontologier og informasjonsmodeller, metadata påføres og valideres, sikkerhetsmerking settes i henhold til definerte standarder, og data kvalitetssikres og aggregeres. For analytiske dataprodukter som må bearbeides før de kan deles brukes en bronse-sølv-gull-prosess. Rådata fra kilde eller sensor bevares uendret i bronse, valideres og kontekstualiseres i sølv og bearbeides til produkter klare for deling i gull.

Datakatalog, og datadistribusjon og føderert deling (Datatjenester): Dataprodukter registreres i dataproduktkatalogen ved publisering, med et standardisert grensesnitt og en datakontrakt som beskriver tjenestenivå og betingelser for tilgang og bruk. Konsumenter oppdager og abonnerer på dataprodukter gjennom katalogen, og gis tilgang i henhold til datakontrakten. Dataprodukter tilgjengeliggjøres enten gjennom virtuell datatilgang, der data blir liggende i kilden, eller ved at dataproduktet lagres i FDDP. Det siste vil ofte være nødvendig ved sammenstilling av flere kilder med ulik granularitet eller lagring av historiske versjoner av data, oppgaver som normalt ikke kan realiseres gjennom virtuell tilgang alene. Virtuell tilgang og datalagring i FDDP utfyller dermed hverandre som komplementære mekanismer.

Scenarier

Scenariene under viser kapabilitetene fra kapittel 4 i praksis, og illustrerer hvordan FDDP lar data skape verdi for andre enn den som produserer dem. Hvert scenario tar utgangspunkt i en konkret kilde eller applikasjon, og peker på hvilke kapabiliteter i FDDP som tas i bruk.

1 Link 16/Link 22 - Gateway-integrasjon mot taktisk nettverk

Scenario 1: Taktiske datalink-nettverk er optimalisert for nær sanntidsutveksling av data mellom militære plattformer og inngår ikke i FDDP. Scenarioet illustrerer hvordan FDDP kan samvirke med slike nettverk via et gateway-mønster for å hente ut data for utnyttelse.

Taktiske datalink (TDL)-nettverk, som Link 16 og Link 22, er standardiserte, sikre og krypterte kommunikasjonsnettverk der militære enheter på tvers av domener kan dele sitt taktiske bilde i nær sanntid. TDL-nettverk inngår ikke direkte i FDDP, men samvirker med dataplattformen gjennom definerte gatewayer som lytter på meldingene og oversetter dem til standardiserte dataprodukter i FDDPs dataproduktkatalog.

Disse produktene erstatter ikke sanntidsdataene som utveksles i TDL-nettverket, men gjør det mulig å bevare og videreformidle innholdet i TDL-meldinger til andre konsumenter i FDDP. Et typisk brukstilfelle er historisk rekonstruksjon av hendelsesforløp, for eksempel som grunnlag for en battle damage assessment (BDA) etter at operasjonen er gjennomført.

Gatewayen kan også konfigureres i motsatt retning, for eksempel for å utveksle utvalgt målinformasjon som har blitt tilgjengeliggjort i FDDP med TDL-nettverket.

Kapabiliteter:

- **Innhenting og integrasjon:** gatewayen som lytter på TDL-meldingene og oversetter dem
- **Dataoppdagelse og metadataforvaltning:** TDL-innholdet registreres som dataprodukt
- **Datadistribusjon og føderert deling:** historiske TDL-meldinger bevares i FDDP

Anvendelsesområde:

- **Situasjonsforståelse:** BDA-analysen understøtter vurderingen av gjennomført operasjon

2 P-8 - Historisk lagring av sensordata

Scenario 2: Sensorplattformer produserer store datamengder som slettes lokalt etter bruk. Scenarioet illustrerer hvordan FDDP sikrer lagring av historikk og hvordan rådata og analytiske produkter forvaltes som separate dataprodukter med sporbarhet mellom dem.

En P-8 Poseidon samler store datamengder, typisk av størrelsesorden terabytes, på hvert tokt. Sensordataene slettes typisk fra plattformens lokale lagring etter at toktet er avsluttet og data er avlevert.

Radar-, bilde- og sporingsdata fra P-8 registreres som dataprodukter med metadata om toktets parametere, sensoroppsett og geografiske dekningsområde, og lagres i FDDP.

Analytiske produkter avledes basert på sensordataene med eksplisitt referanse tilbake til det opprinnelige dataproduktet. Denne sporbarheten gjør det mulig å etterprøve konklusjoner og rekonstruere beslutningsgrunnlaget ved behov.

Kapabiliteter:

- **Dataoppdagelse og metadataforvaltning:** radar-, bilde- og sporingsdata registreres som dataprodukt
- **Behandling og transformasjon:** analytiske dataprodukter avledes fra sensordataene
- **Datadistribusjon og føderert deling:** sensordataene bevares i FDDP etter at de er slettet fra plattformens egen lagring

Anvendelsesområde:

- **Situasjonsforståelse:** de analytiske produktene understøtter maritim situasjonsforståelse

3 Skipskontrollsystem - Integrasjon av eldre applikasjoner og OT-data

Scenario 3: Forsvaret har mye teknologi og digitalisert materiell som har blitt anskaffet uten å stille krav til datautveksling. Dette scenarioet illustrerer hvordan FDDP kan integrere med eldre applikasjoner gjennom et abstraksjonslag.

Skipskontrollsystemet på en korvett i Skjold-klassen logger løpende data om tilstanden på maskineriet i fartøyet (OT-data): temperaturer og vibrasjoner på maskindeler, turbinstarter og -stopper, og drivstofforbruk. Systemet er isolert fra øvrig teknologi ombord. I tråd med FDSA skal det stilles krav til leverandøren om å eksponere disse dataene i åpne, standardiserte formater som FDDP deployert ombord kan konsumere direkte. Alternativt utvikles en adapter som fungerer som et abstraksjonslag og oversetter dataene til et standardisert format som kan konsumeres av FDDP.

Råhistorikken fra fartøyet registreres som et dataprodukt i Forsvarets dataproduktkatalog og bevares i FDDP i henhold til dataproduktets kontrakt. Analytikere bruker denne historikken til å trene modeller for prediktivt vedlikehold. Modellene kjøres løpende på nye data fra fartøyet og genererer vedlikeholdsrekvisisjoner i SAP når modellen predikerer at det er behov for det.

For de fleste konsumenter har råhistorikken for høy oppløsning til å være nyttig. Det avledes derfor et aggregert driftssammendrag som et analytisk dataprodukt gjennom en bronse-sølv-gull-prosess i FDDP. Det analytiske produktet konsumeres av SAP for vedlikeholdslogging og logistikk.

Kapabiliteter:

- **Innhenting og integrasjon:** adapteren mot skipskontrollsystemet
- **Dataoppdagelse og metadataforvaltning:** råhistorikken registreres som dataprodukt
- **Livssyklusforvaltning:** historikken bevares i FDDP i henhold til dataproduktets kontrakt
- **Behandling og transformasjon:** bronse-sølv-gull-prosessen som produserer driftssammendraget
- **Analyse-, KI- og annoteringstjenester:** modellene for prediktivt vedlikehold
- **Datadistribusjon og føderert deling:** det analytiske dataproduktet konsumeres av SAP

Anvendelsesområde:

- **Virksomhetsstyring:** driftssammendraget understøtter vedlikeholdsstyring

4 Arctic Eye – Fusjon av analytisk og operasjonell data

Scenario 4: Arctic Eye er et dashboard som gir Forsvarets øverste ledelse ett felles situasjonsbilde på tvers av operasjoner og virksomhetsstyring slik at de i samme bilde ser sanntidsbildet for operasjoner og tilstanden på strukturelementene som understøtter dem. Scenarioet beskriver ikke hvordan Arctic Eye er bygget i dag, men slutttilstanden som målbildet legger til rette for.

Arctic Eye er en analytisk applikasjon som utelukkende konsumerer dataprodukter fra FDDP og krever at to datastrømmer fusjoneres: Virksomhetsstyringsdata, som primært produseres i SAP, og situasjonsbilder, som primært produseres i NORCCIS. For å gjennomføre denne fusjonen må det finnes en felles identifikator på tvers av applikasjoner der et fartøy i SAP må entydig knyttes til samme fartøy i NORCCIS.

Virksomhetsstyringsdataene, som teknisk tilgjengelighet på materiell og tilgang på kompetent personell, forvaltes av de ansvarlige domene og tilgjengeliggjøres som dataprodukter i FDDPs dataproduktkatalog. Uttrekk fra SAP går gjennom en bronse-sølv-gull-prosess i FDDP der data valideres, transformeres og berikes med kontekstuelle metadata før de publiseres som analytiske dataprodukter.

NORCCIS tilgjengeliggjør sine situasjonsbilder som dataprodukter i FDDPs dataproduktkatalog. Autoriserte brukere kan abonnere på disse produktene direkte gjennom katalogen. Det er disse dataproduktene som utgjør datastrømmen fra operasjoner, publisert i nær sanntid gjennom åpne grensesnitt.

Kapabiliteter:

- **Behandling og transformasjon:** bronse-sølv-gull-prosessen for virksomhetsstyringsdataene fra SAP
- **Grunn- og referansedataforvaltning:** felles identifikator på tvers av SAP og NORCCIS
- **Dataoppdagelse og metadataforvaltning:** begge datastrømmene publiseres i dataproduktkatalogen
- **Datadistribusjon og føderert deling:** Arctic Eye abonnerer på og henter ut dataproduktene

Anvendelsesområde:

- **Situasjonsforståelse og Virksomhetsstyring:** Arctic Eye fusjonerer operasjonelt og virksomhetsstyrt bilde til ett situasjonsbilde for Forsvarsledelsen

6 Begreper, definisjoner og forkortelser

I tilfeller der begreper er hentet fra et annet dokument er dette indikert sist i definisjonen, for eksempel betyr [DRP] at begrepets definisjon er hentet fra Digital reguleringsplan.

Begrepsliste

Begrep	Definisjon
Anonymisering	Å gjøre personopplysninger anonyme, slik at det ikke lenger er mulig å avdekke hvem opplysningene gjelder. Anonymiserte opplysninger regnes ikke som personopplysninger.
Attributtbasert tilgangsstyring («ABAC»)	En modell for tilgangsstyring der tilgangsrettigheter tildeles dynamisk basert på en kombinasjon av egenskaper (attributter) ved brukeren, ressursen og den aktuelle konteksten (f.eks. tid og sted). [DRP]
Begrepsapparat	Hvordan en virksomhet definerer og bruker begreper. Det består gjerne av definisjoner, avgrensninger, forklaringer og eksempler. Et begrepsapparat er primært laget for mennesker for å sikre en felles forståelse, bedre kommunikasjon og forhindre begrepsforvirring. [DRP]
Cloud	Samlebegrep for allmenn sky, nasjonal sky og alliert sky. Slike skyplattformer gir høy elastisitet, der kapasitet kan skaleres raskt opp og ned etter behov. Cloud er ett av fire lag i Forsvarets skyløsning, sammen med core, fog og edge. [DRP]
Core	Sentralt lag i en distribuert IT-struktur – typisk tilsvarende sentralisert cloud computing. Dette kjennetegnes av store databehandlingsressurser, f.eks. datasentre eller store skyregioner, høy kapasitet og skalerbarhet, optimalt for tung databehandling, langtidslagring og avansert analyse. Ikke lokasjonsnært, noe som innebærer større avhengighet av nettverksforbindelser og potensielt høyere latenstid. [DRP]
Datadomene	En logisk gruppering av relaterte data tilpasset et spesifikt forretningsområde eller funksjon. Administrert av eksperter med spesialisert funksjonell ekspertise, gir den et rammeverk for organisering, styring og produksjon av dataprodukter. Dette sikrer konsistens, klarhet og overholdelse av regulatoriske krav og standarder, samtidig som det legger til rette for effektiv informasjonsdeling.
Datakontrakt	En formell beskrivelse av betingelsene for tilgang til og bruk av et dataprodukt, utarbeidet og forvaltet av dataproduktets eier. Kontrakten beskriver tekniske krav, skjermings- og delingsbetingelser, kvalitetskrav og livssyklusinformasjon.
Dataobjekt	Enhver data, uansett format. Dette kan være en enkelt verdi, et datasett eller en analyserapport.
Dataplattform	Et integrert miljø som gjør det mulig å dele og bruke data på tvers av organisasjonen ved å gjøre dem søkbare, tilgjengelige og klare for bruk, og som sikrer at data kan forvaltes gjennom hele livssyklusen.

Dataprodukt	En samling dataobjekter, pakket med essensielle metadata, som er designet for å være gjenbrukbare, oppdagelige og interoperable på tvers av ulike miljøer. [DRP]
Dataproduktkatalog	En søkbar oversikt over dataprodukter som gjør det mulig for konsumenter å oppdage, abonnere på og få tilgang til dataprodukter gjennom standardiserte grensesnitt.
Datasentrisk arkitektur	Teknisk realisering der data er det primære organiserende elementet, strukturert som delbare, styrte og standardiserte dataprodukter innenfor en føderert modell som sikrer interoperabilitet, kvalitet og sikkerhet på tvers av informasjonssystemer og organisasjoner. (Data Centric Reference Architecture (NATO 2024a)). [DRP]
Datasentrisk tilnærming	Overordnet tilnærming, som omhandler en felles intensjon om å behandle data som en delt ressurs som kan utnyttes av alle til å gjennomføre operasjoner. Intensjonen omfatter deling, utveksling, verdsettelse og utnyttelse av data. [DRP]
Datasentrisk sikkerhet	Sikkerhetsmekanismer der beskyttelsesmekanismene legges direkte på dataene uavhengig av hvor dataene befinner seg, slik at konfidensialitet, integritet og tilgjengelighet opprettholdes gjennom hele livssyklusen. [DRP]
Digitalisert materiell	Materiellsystemer der IKT utgjør en integrert del av systemets funksjon. Interoperabilitet, samvirke og dataflyt utgjør en dimensjonerende delmengde av det digitaliserte materiellets operative evne. [DRP]
Edge	Noder plassert ytterst i Forsvarets skyløsning, der data genereres, behandles og brukes nær operasjonen. De muliggjør lokal databehandling tett på sensorer, plattformer og brukere, og bidrar til økt robusthet gjennom autonomi, redusert nettverkstrafikk og lavere forsinkelse. [DRP]
Fog	Et distribuert mellomlag mellom cloudkjernen (core) og edge noder. Fog-laget ligger nærmere operasjonsområdet for å redusere latenstid. Behandler data lokalt før de eventuelt sendes videre til sentral sky. Avlaster core-laget ved å filtrere, analysere og reagere på data hurtigere. Består av mange noder, typisk små datasentre, rutere, aksesspunkter eller taktiske IT-noder. [DRP]
Grunndata	Autorative data om kjerneentiteter (som personell, materiell og geografi) som forvaltes som en felles sannhet og gjenbrukes på tvers av hele organisasjonen for å sikre konsistens. Kalles også masterdata eller stamdata. [DRP]
Kapabilitet	Evnen til at et system eller en organisasjon kan utføre en funksjon på et gitt prestasjonsnivå for å oppnå strategiske eller operative mål. Den realiseres gjennom kombinasjoner av mennesker, prosesser, organisasjon, informasjon og teknologi. (NATO, 2020). For Forsvarets IKT vil elementer som mennesker, prosess, kompetanse, applikasjoner, data, informasjonssystemer og kommunikasjonsinfrastruktur inngå. [DRP]

Kunnskapsgraf	En strukturert representasjon av entiteter og relasjonene mellom dem.
Metadata	Data som beskriver andre data (f.eks. opprinnelse, struktur og format). [DRP]
Multidomene-operasjoner	Orkestrering av militære aktiviteter på tvers av alle domener og miljøer, synkronisert med ikke-militære aktiviteter, for å gjøre alliansen i stand til å levere konvergerende effekter til rett tid (NATO, 2022a). [DRP]
Observerbarhet («observability»)	Evnen til å overvåke dataflyt og måle data- og leveranse kvalitet, inkludert forsinkelser, volum og feilrater, for å sikre operativ presisjon og proaktiv feilretting.
Ontologi	Et felles og delt, maskinlesbart vokabular for en virksomhet eller kunnskapsområde. En ontologi er mer enn et begrepsapparat, og beskriver både hvilke begreper som finnes, hvordan de henger sammen og hvilke relasjoner og regler som gjelder mellom dem. Dette gjør sammenhenger logiske og entydige, slik at både mennesker og maskiner kan forstå, dele og gjenbruke data på samme måte. Der begrepsapparat forklarer hva et begrep betyr, viser en ontologi også hvordan begrepet er koblet til andre begreper – f.eks. hvordan «avdeling» relaterer til enhet, styrke, oppdrag og lokasjon – og hvilke regler som gjelder. [DRP]
Opphav («data provenance»)	Informasjon om et dataprodukts kilder, produksjonsprosess og transformasjoner, som gjør det mulig å forstå og etterprøve hvordan produktet er fremstilt.
Policy-as-code	Tilnærming til å administrere og håndheve sikkerhetspolicyer ved å uttrykke dem ved hjelp av programmerings- eller konfigurasjonsspråk.
Pseudonymisering	Behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger, forutsatt at tilleggsopplysningene lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar fysisk person. (GDPR art. 4 nr. 5)
Replikering	Opprettelse og vedlikehold av flere kopier av data på tvers av geografisk adskilte noder eller applikasjoner for å sikre tilgjengelighet, redundans og konsistens.
Skytjeneste	En IKT-tjeneste levert fra en skyplattform ved hjelp av skyteknologi. Ifølge NIST gir skytjenester praktisk, on-demand nettverkstilgang til en delt pool av konfigurerbare dataressurser som raskt og effektivt leverer IKT-tjenester til virksomheten. Bruk av skytjenester muliggjør kostnadsmodeller basert på faktisk forbruk i motsetning til tradisjonelle tjenestemodeller. Mer formelt definerer NIST skytjenester som bestående av fem essensielle egenskaper, tre tjenestemodeller og fire leveransemodeller. [DRP]
Sporbarhet («data lineage»)	Evnen til å følge et dataprodukts reise fra kilde til konsument, inkludert alle transformasjoner, tilganger og endringer gjennom livssyklusen.

Virtuell datatilgang	Tilgang til data og dataprodukter direkte fra kildesystemene uten at data fysisk flyttes eller kopieres, slik at data fremstår som tilgjengelig fra ett sted for konsumenten uavhengig av hvor de faktisk befinner seg.
Zero Trust	Sikkerhetsrammeverk basert på prinsippet om at ingen bruker, enhet eller applikasjon har implisitt tillit, uansett om de befinner seg innenfor eller utenfor organisasjonens nettverk. All tilgang må verifiseres eksplisitt, basert på identitet, kontekst og enhetens tilstand, og gis kun med minste privilegium. Zero trust antar at brudd kan skje og krever kontinuerlig autentisering, autorisasjon og overvåking av alle forespørsler. Zero trust realiseres gjennom pilarene: bruker, enhet, nettverk, applikasjon, data, automatisering/orkestrering samt synlighet/analyse. [DRP]

Forkortelser

ABAC	Attribute-based Access Control
API	Application Programming Interface
DCRA	Data Centric Reference Architecture for the Alliance
DDIL	Disconnected/Disrupted, Degraded, Intermittent and Limited/Low-Bandwidth (kommunikasjonsmiljøer)
DRP	Digital Reguleringsplan
FAKTISK	Finnbare, Anvendelige, Klare, Troverdige, Interoperable, Sikre og Koblede
FDDP	Forsvarets distribuerte dataplattform
FDSA	Forsvarets datasentriske arkitektur
FGP	Forsvarets gjennomføringsplan
FMN	Federated Mission Networking
IoT	Internet of Things
KI	Kunstig intelligens
LTP	Langtidsplan for Forsvaret
MDO	Multidomeneoperasjoner
PEP	Policy Enforcement Point
PSM	Forsvarssjefens porteføljestyre
STANAG	Standardization Agreement