Forsvarets strategi for digital transformation

Kort version

Reference: Forsvarets strategi for digital transformation v0.2.3, sag 2022/008984, dok. 1887013.

Dette er en forkortet version af ref. Formålet med dette dokument er et give et hurtigt overblik over strategien for digital transformation af Forsvaret. Der er således en lang række detaljer, som er udeladt. For en mere indgående forståelse af strategien, anbefales det at læse ref. i sin helhed.

1. INDLEDNING

NATO og vores primære samarbejdspartnere implementerer Multi-Domain Operationer (MDO) omfattende air, land, sea, space, cyber. De transformerer deres forsvar til at være digitale og data-centriske, hvor der anvendes data og maskinlæring til understøttelse af operative og styringsmæssige beslutningsprocesser. Vores potentielle modstandere, både de ligeværdige modstandere og de simple terrororganisationer, forstår at drage nytte af denne udvikling med innovativ kreativitet og potentiel stor effekt. Det er derfor afgørende, at Forsvaret følger med denne udvikling, så vores enheder kan forsvare sig mod de nye kampformer i alle spektre og domæner.

2. FORMÅL

Dette dokument fastlægger visionen og strategien for den digitale transformation af Forsvarsministeriets koncern og for implementering af Danish Common Operation Information Environment (DA-COIE) over de næste 10 år. Målsætninger fremsættes for den digitale transformation for den først kommende forsvarsaftale. Den digitale transformation af koncernen og implementeringen af DA-COIE er et strategisk udviklingsprogram, der skal godkendes og finansieres politisk.

3. VISION OG MÅLSÆTNINGER

Moderne teknologi giver mulighed for at øge hastigheden i vores beslutninger og forbedre vores billede af kampladsen, hvilket er afgørende, for at imødegå nuværende og fremtidige trusler i alle domæner. Vi skal omfavne teknologien, modernisere, cyberbeskytte og udnytte mulighederne i de nye teknologier. Vores arv af digitale netværk er kommet til ved knobskydning gennem årene. Mange af koncernens it-netværk er fragmenterede, siloopdelte, underdimensionerede, skrøbelige og er ikke cybersikrede til moderne standarder.

Vores modstandere moderniserer og digitaliserer deres militære kapaciteter, og deres militære effektivitet styrkes i disse år. For fortsat at kunne levere på Forsvarets opgaver og forsvare Danmark og Kongeriget må vi tilpasse os de nye tider og transformere Forsvaret.

3.1. Danish Common Operational Information Environment (DA-COIE)

DA-COIE som koncept er en betegnelse for den samlede integration, interoperabilitet og sammenhæng i Forsvarets informations- og kommunikationsteknologi (IKT). Ambitionen for DA-COIE er et informationsmiljø, hvor den rette information er tilgængelig, for den rette modtager, i det rette format, på det rette tidspunkt. Sigtet er at forbedre Forsvarets og koncernens kommunikationsinfrastruktur og evne til at behandle data og informationer for derigennem at understøtte funktionerne understand, decide, act. Denne strategi for digital transformation vil implementere DA-COIE.

3.2. Digital transformation af Forsvaret

Forsvarsministeriets koncern skal igennem en transformation og udvikle sig til et digitalt, driftssikkert, redundant, cybersikret, datadrevet forsvar, der fungerer nationalt og internationalt i fred, krise og krig. Forandringen forudsætter en teknologisk modernisering og en kulturel transformation af vores organisation og vores personel til den digitaliserede tidsalder, understøttet af en vilje til forandringsledelse og opbygning af styrket governance. Vi skaber et datadrevet forsvar med digitalt kompetente chefer, ledere og medarbejdere.

I Fremtidens Forsvar er data værdsat som en strategisk ressource, og i det digitaliserede Forsvar kobles sensorer, beslutningstagere og effektorer. Digitalt integrerede kapaciteter fra Forsvaret og Hjemmeværnet kobles med Beredskabsstyrelsen og Politiet.
Forsvaret analyserer data ved anvendelse af maskinlærings- og analyseservices for at skabe et bedre beslutningsgrundlag og situationsforståelse med henblik på at kunne træffe effektive beslutninger og handle hurtigt operativt såvel som virksomhedsmæssigt. Forsvaret integreres digitalt med støttestrukturen og skaber et styrket logistisk planlægnings- og styringsgrundlag. Forsvaret skal være integreret med NATO og skal fleksibelt kunne integrere med vores samarbejdspartnere, når behovet opstår. Forsvaret skal sikre, at øget digitalisering ikke medfører øgede sårbarheder i cyberdomænet. Derfor vil vi udvikle løsninger med en robust og sammenhængende arkitektur på tværs af koncernen, hvor centrale principper som Secure by Design har prioritet.

3.3. Forsvarets vision for digitalisering (Ends)

Pejlemærkerne for Forsvarets digitale transformation for det næste årti lyder således:

- Forsvarsministeriets koncern er en digitaliseret datadrevet organisation, hvor data er den strategiske kapacitet, der integrerer Forsvaret nationalt og internationalt på tværs af alle operative domæner samt på tværs af styringsområder.

- Gennem standardisering og interoperabilitet udveksles data sikkert, pålideligt, gnidningsfrit og kontrolleret imellem sensorer, beslutningstagere og effektorer. Dette i og mellem alle værn og kommandoer samt på tværs af koncernen, Totalforsvaret, Kongeriget og med vo-res internationale partnere.
- Koncernens digitale kapacitet er cybersikret, skalerbar, integreret, let anvendelig og leveret til alle godkendte brugere til rette tid og i rette mængde.

3.4. Strategiske målsætninger for 2029

Vores plan for implementering af DA-COIE er at iværksætte en langsigtet integreret iterativ udviklingsproces, hvor vi arbejder parallelt i flere spor. Vi iværksætter en udviklingsproces med syv primære fokusområder inden for digitalisering; (1) mennesker, (2) processer, (3) data, (4) teknologi, (5) cybersikkerhed, (6) exploitation og (7) integration. For hvert fokusområde udvikles en delstrategi.

Vores strategiske målsætninger for 2029 er følgende:

- Forsvarsministeriets koncern har en driftssikker, redundant, sikret, cybersikker, akkrediteret, skalerbar, moderne digital kapacitet, bestående af en digital infrastruktur, herunder en distribueret datacenterstruktur og kommunikationssystemer, der med en datacentrisk[1] arkitektur forbinder sensorer, effektorer[2] og beslutningstagere på tværs af de militære domæner, styringsområder og med vores partnere nationalt og internationalt. Centralt er integration og interoperabilitet på tværs af domæner og platforme.
- Den moderniserede datacentriske arkitektur giver adgang til data og muliggør anvendelsen af maskinlærings- og analyse services, der vil effektivisere de militære operationer og styrke styringen af Forsvaret på tværs af koncernen.
- Koncernens medarbejdere kan tilgå information gennem DA-COIE og varetage deres faglige funktioner og administrative opgaver via deres mobile enheder.
- Digitalt kompetente, innovative og bemyndigede soldater, medarbejdere, ledere og chefer agerer smidigt i en digitalt tranformeret koncern, der løbende udvikler sig og udnytter nye muligheder.
- Forsvarets kapaciteter kan, hvis det er nødvendigt, operere digitalt sammen også uden at være forbundet til DA-COIE.

4. FOKUSOMRÅDER (WAYS)

---

[1] Datacentrisk referer til en arkitektur, hvor data er det primære, den permenente ressource, og hvor alt andet kan forandre sig. Hvor "datadrevet" handler om kultur og mennesker, handler datacentrisk om arkitektur

[2] Effektorer defineres som de teknologier, der ændrer tilstanden på et "objekt".

'ngen skal skabe en række forandringer i forhold til kultur, pro- og implementere en række nye teknologier. Følgende fokusområ- er gennemgående temaer, som vil ramme ind i alt hvad vi gør i for- til transformationen.

1. **Mennesker**. Forsvaret og koncernen skal have rådighed over en digitalt veluddannet arbejdsstyrke med de rette kompetencer. Vi vil skabe en attraktiv arbejdsplads med fleksibel løndannelse, tilbyde gode karrieremuligheder og investere i videreuddannelse.
2. **Processer**. Der udvikles relevante og effektive koncernfælles processer, der kan understøtte Forsvarets operationer og behov for styring af koncernen.
3. **Data.** Forsvarsministeriets koncern skal tranformeres til en datadrevet organisation. Vi vil samle og kuratere data fra alle kilder og muliggøre exploitering af data på tværs af koncernen ved anvendelse af maskinlærings- og analyseservices.
4. **Teknologi**. Vi vil skabe en moderne og sikker teknologisk platform for hele koncernen. Vi vil erstatte vores nuværende silobaserede tilgang med et robust koncernfælles arkitektur og infrastruktur, designet til brug for hele koncernen.
5. Cyber. Bevidstheden om cybersikkerhed hos den enkelte medarbejder skal styrkes. Vi skal cybersikre alle gateways, monitere al digital trafik på netværkene, og anvende de mest moderne krypteringsmetoder. Vi skal engagere sig i de kommende krypteringsteknologier, som blockchain og Quantum computing, så vi er rede til at implementere dem, når teknologierne er modne.
6. **Exploitering af data**. Vi skal styrke og accellerere exploiteringen af data i Forsvaret. Opgaven for koncernens samlede digitale funktion er gennem DA-COIE at stille dataanalyse og machine learning til rådighed som services for operative kommandoer og beslutningstagere.
7. **Integration af operative kapaciteter og virksomhedsstyringen på netværket**. De operative kapaciteter og de styringsmæssige områder skal integreres med netværket. Sensordata fra de operative kapaciteter skal sendes til de centrale computere for dataanalyse og beslutningstagning. Den viden og situationsforståelse vi opbygger centralt gennem dataanalyse, skal deles med de operative kapaciteter. Tilsvarende skal data fra styringsområderne kunne fusioneres af centrale dataanlyseredskaber for at danne grundlag for tværgående beslutningstagning.

5. MIDLER TIL AT NÅ MÅLSÆTNINGEN

Den digitale transformation af Forsvarsministeriets koncern er et strategisk udviklingsprogram, der skal godkendes og finansieres politisk som en del af den kommende forsvarsaftale. Implementeringen af DA-COIE og den digitale transformation vil involvere alle styrelser i koncernen. Vores eksisterende driftsplaner, udviklingsplaner, anlægsplaner, program-

mer og finansieringsplaner vil skulle tilpasses eller integreres med Program DA-COIE. Derfor anbefales programmet forankret højt i koncernen under ledelse af en programbestyrelse med alle styrelseschefer.

Under programbestyrelsen etableres en programstyregruppe indledningsvis på oberst- eller vicechefsniveau med deltagelse af de støttende styrelser samt NIV II myndighederne i Forsvarskommandoen. Formanden for programstyregruppen anbefales at være chefen for Forsvarskommandoens Udviklings- og Planlægningsstab. Der anbefales udpeget en programleder indledningsvis på oberstniveau (M402), der referer til formanden for programstyregruppen. Programorganisationen forankres i Udviklings- og Planlægningsstaben i Forsvarskommandoen. Programsektionerne vil blive bemandet med personel med faglig baggrund fra Forsvaret, Forsvarsministeriets Materiel- og Indkøbsstyrelse, Forsvarsministeriets Ejendomsstyrelse samt Forsvarsministeriets Personalestyrelse.

Etableringen af DIC med software definerede datacentre, software definerede netværk, virtuelle computere, datamanagement og dataanalyse vil tilvejebringe et fundamentalt nyt digitalt agilt operativt miljø, der giver nye operative muligheder i form af deling af information og bedre beslutningsgrundlag. Det betyder, at styringen af netværkene, styringen af data og dataanalyse skal integreres med Forsvarets operative virksomhed, så agiliteten i den digitale kapacitet og styrkerne ved dataanalyse kan anvendes operativt. Til det formål etableres Forsvarets Datakommando som en niveau II myndighed med ansvaret for at drifte, udvikle og styrkeindsætte Forsvarets kapaciteter inden for CIS, cyberbeskyttelse, data og dataanalyse tæt integreret med Forsvarsministeriets Materiel- og Indkøbsstyrelse. Forsvarets Datakommando støtter Operationsstaben, værn og kommandoer med dens kompetencer i både styrkeproduktion og styrkeindsættelse.

6. OVERVEJELSER I FORHOLD TIL, HVORDAN STRATEGIEN IMPLEMENTERES

Den digitale transformation skal understøtte Forsvarets operationer og koncernens styringsbehov, og de fremtidige teknologier skal have operationer og brugeren i centrum. Derfor udvikler vi brugerbehov og Information Exchange Requirements iterativt i takt med implementeringen af en datacentrisk arkitektur, der sikrer sammenhængen mellem kapaciteter, kommando og kontrol, netværk, datacentre, infrastruktur, kommunikationssystemer, applikationer og computere. Cyberbeskyttelsen, som i Secure-by-Design, skal tænkes ind i arkitekturen fra starten.

Vi vil styrke sammenhængen mellem vores operative og styringsmæssige applikationer samt imellem ERP applikationerne. DA-COIE's tværgående arkitektur og data-centriske tilgang skal sikre, at vi kan udnytte ERP data i de operative applikationer og omvendt hvor der er behov.

Program DA-COIE skal koordineres og integreres med eksisterende programmer og projekter. Særligt tænkes der her på Program IT-Konsolidering (PIT), F-35 programmet og de mange it- og materielkapacitetsprojekter, der køres i Forsvarsministeriets Materiel- og Indkøbsstyrelse. På samme måde skal de dele af infrastrukturprojekterne, som kræver bygning af bygninger, planlægges og koordineres med Forsvarsministeriets Ejendomsstyrelse.

Vi vil iværksætte et arbejde, der skal give os et overblik over de data vi har i koncernen. Dette overblik skal skabe grundlaget for udviklingen af den data-centriske arkitektur, overførslen af data fra de eksiterende systemer til Defence Information Cloud[3] (DIC) samt udvikling af vores evne til at anvende kunstig intelligens.

Etableringen af DA-COIE er en opgave, der vil tage flere år, og teknologien vil i perioden løbende udvikle sig. Derfor vil vi gennemføre programmet iterativt. Vi vil starte med at etablere infrastrukturen, arkitekturen og datamanagement, mens vi fortsat drifter vores eksisterende systemer. Når kerneinfrastrukturen er klar, vil vi iterativt overføre services fra de eksisterende netværk, og derefter nedlægge dem.

[3] Generisk ord der ikke refererer til en bestemt løsning. Det er forventeligt en hyperskalerbar cloud bestående af flere clouds.

Standarderne i NATO Federated Mission Networking bliver centrale for vores udvikling af DA-COIE. Vi sikre os, at vi har interoperabilitet med vores strategiske samarbejdspartnere. Det må forudses, at store dele af Forsvarets operative kapaciteter skal integreres. De teknisk ansvarlige for disse kapaciteter inddrages tidligt for at sikre, at de tekniske udviklingsplaner for kapaciteten overholder de fælles standarder, og at tilslutningen af kapaciteten til netværket indarbejdes i kapacitetens vedligeholdelsesplan. Vi vil prioritere, i hvilken rækkefølge vi integrerer kapaciteterne.

Et af de helt centrale fokusområder er uddannelse. Forsvarets skoler får en hovedrolle i dette. Vi starter med at definere transformationen og udvikle de digitale uddannelser. Vi vil inkludere digital uddannelse i de eksisterende uddannelsestilbud og lave nye uddannelser. Vi vil skabe nye karriereveje, hvor it-kompetencer i er i centrum. Helt centralt bliver udviklingen af kompetencer indenfor data, maskinlæring og dataanalyse, netværksmanagement og cyberbeskyttelse.

Det må forudses, at det vil tage tid at rekruttere it-kyndigt personel samt at videreuddanne vores allerede ansatte personel, så de er kompetente til at designe, udvikle og drive DA-COIE. Vi kan ikke vente med at gå i gang, til vores eget personel er klar. Vi vil derfor styrke vores kompetencer med konsulenter efter behov, indtil vores eget personel er klar til at overtage opgaven.

Vores indkøbsprocesser er for lange og for bureaukratiske til at kunne levere i takt med den digitale udvikling. Vi vil derfor effektivisere og optimere vores indkøbsprocesser, så de understøtter behovet for effektive og hurtige anskaffelser.

I samarbejde med Hjemmeværnet, Politiet og Beredskabet vil vi udvikle en strategi for, hvorledes digitaliseringen spænder på tværs af totalforsvaret i fred, krise og krig.

Et digitaliseret datadrevet multi-domæne forsvar er ikke en hyldevare, der kan anskaffes færdiglavet. Det er en udvikling Forsvaret selv må tage ansvaret for. DA-COIE vil blive en kompleks samling af teknologier, der skal kunne virke sammen sikkert, robust og redundant i en fælles arkitektur. Selv små ændringer i systemet, som eksempelvis softwareopdateringer, vil kunne påvirke de øvrige komponenter i systemet. Derfor skal vi afprøve og kvalitetssikre vores opdateringer, inden de slippes løs på det operative netværk. Til det formål etableres et Forsvarets BattleLab, der tillige skal stå for udvikling af innovative løsninger og samspillet mellem Forsvaret, universiteterne og industrien i et nyt Center for Militær Teknologi under Forsvarskommandoen.