

Digital sikkerhed, tillid og dataetik

Introduktion: Vision, mål og effekter

Vi vil ruste Danmark som leverandørland i det digitale kapløb med fokus på Danmarks styrkeposition som garant for etik, cybersikkerhed, ansvarlighed, brugerinddragelse og kvalitet i digitale løsninger og dermed bringe Danmark i front som digital teknologileverandør baseret på ansvarlighed. Dette vil støtte op om både EU's og Danmarks strategier om digitale løsninger baseret på europæiske, skandinaviske og danske værdier som tillid, åbenhed og etisk ansvarlighed. Mangel på tillid kan stå i vejen for udnyttelse af digitale teknologiers potentialer [\[1\]](#)[\[2\]](#).

Vi anvender i denne beskrivelse *ansvarlighed/ansvarlige løsninger* som fælles begreb for etiske, cybersikre, privacy-venlige, ikke-biased, tillids- og tryghedsskabende løsninger.

Det er indsatsens mål at udvikle og modne digitale teknologier inden for områderne *Advanced AI and Analytics*, *Cybersecurity* og *Digital og kritisk infrastruktur* for at skabe og opretholde tilliden til teknologi-anvendelse. Dette vil ske ved at udvikle en dansk test-, demonstrations- og udviklingsfacilitet (TDU) og sikre danske og europæiske initiativer for ansvarlig brug af teknologier [\[3\]](#)[\[4\]](#)[\[5\]](#)[\[6\]](#)[\[7\]](#)[\[8\]](#)[\[9\]](#).

Denne TDU vil være tilgængelig for alle landets virksomheder og offentlige institutioner, hvor der gennem den fireårige periode har været gennemført pilot-cases med min. 20 virksomheder. Den vil sikre adgang til test og certificering, standardiseringsarbejde inden for digitale teknologier, demonstration og udvikling af cutting edge AI og cybersikkerhed. Vi vurderer, at vi med en sådan facilitet kan øge aktørernes viden om mulighederne inden for cybersikkerhed, ansvarlig udnyttelse af AI og digitale teknologier. TDU'en etableres i samarbejde med FORCE Technology og Nordic IoT Centre.

Markeds- og samfundsbehov

Tillid er vigtig for digitalisering i danske virksomheder. 69% af de adspurgte virksomheder i en [undersøgelse fra IDA](#) svarer, at kundernes (digitale) tillid i høj eller meget høj grad er vigtig, alligevel er tilliden til digitale tjenester faldende både i Danmark[\[10\]](#) og internationalt[\[11\]](#)[\[12\]](#).

For virksomheder, som ønsker øget vækst og fremtidssikring via digitalisering, ligger der et enormt potentiale i at anvende AI i deres produkter, tjenester og drift. I regeringens nationale strategi for kunstig intelligens[\[8\]](#) beskrives Danmarks styrkeposition, når det kommer til at udvikle ansvarlig AI. Disse styrkepositioner er vores stærkeste kort i den internationale konkurrence. Der er dog et stykke vej til anvendelsen af denne (forskningsbaserede) viden i virksomhederne.

Der kommer flere og flere krav omkring cybersikkerhed – både danske [\[4\]](#)[\[5\]](#), fra EU[\[3\]](#)[\[6\]](#) og andre eksportmarkeder – hvis danske virksomheder vil levere produkter, komponenter og services til kritisk infrastruktur, og danske og udenlandske kunder begynder at stille cybersikkerhedskrav til deres IT-, IoT-, OT¹-leverandører.

De fremtidige behov hos målgruppen er blevet afdækket gennem en række interviews med virksomheder samt dialog med relevante branche- og interesseorganisationer, bl.a. DI, IT-Branchen, Dansk Erhverv,

¹ OT: Operational Technology, kontrol af fx produktionssystemer

Dansk Energi, Energinet og SMV:Digital, foruden et større afdækningsarbejde af undersøgelser på området. Resultaterne har samlet sig om manglende kompetencer, nem tilgang til teknologier, neutral og objektiv rådgivning samt usikkerhed om certificering, standarder og lovgivning.

En manglende indsats inden for ansvarlig anvendelse af digital teknologi vil hindre danske virksomheder i fortsat at udnytte digitalisering og derved svække deres konkurrenceevne internationalt.

Gennemførlighed

Alexandra Instituttet har stærke forskningsbaserede kompetencer inden for cybersikkerhed, privacy, AI og digitalisering generelt. Både stærke tekniske kompetencer og stærke kompetencer inden for brugerinvolvering og forretningsudvikling. Kombinationen af viden om teknologi og menneskers og organisationers brug af teknologi er vigtig for at få innovative løsninger baseret på forskning på området ud i virksomhederne.

En af de største udfordringer i forhold til at gennemføre AI-projekter i industrien er at komme fra *proof of concept* til produktion. Mange virksomheder efterspørger redskaber, retningslinjer, standarder og benchmarks for at kunne sætte moderne løsninger i drift. I tillæg er der udfordringer i forhold til adgang til tilstrækkelige mængder data. Data er altafgørende for AI-projekter, og særligt i forhold til sprogteknologi (NLP) er der behov for at kunne stille data til rådighed for udvikling af modeller. Da data kan være følsomme, er det altafgørende med modeller med fokus på ansvarlighed. Det er vigtigt med nem adgang til uvidelig rådgivning inden for tillid og digital sikkerhed, hvilket er en central GTS-rolle.

Dette initiativ bygger videre på en lang række forskningsprojekter, Alexandra Instituttet har deltaget i, og vil medvirke til at få teknologierne fra disse projekter stillet til rådighed som ydelser for danske virksomheder.

For at sikre at vi beskæftiger os med relevante ydelser, og at indsatsen forholder sig fornuftigt til private aktører, vil vi inddrage virksomheder og andre aktører gennem netværk, klyngeorganisationer, brancheorganisationer, arrangementer og workshops.

Potentielle aktiviteter

Standarder, test og certificering (*videnspredning, rådgivning, standardisering*): Denne aktivitet vil fortsætte og udvide vores involvering i standardisering af nye digitale teknologier, bl.a. AI og cybersikkerhed. Det er vigtigt, at Danmark kan spille ind i dette arbejde, og at danske SMV'er er repræsenteret. Både Alexandra Instituttet og FORCE Technology er allerede involveret i standardiseringsarbejde, hvilket vil blive intensiveret i denne aktivitet.

Vi vil udbygge og udvikle test- og certificeringsfaciliteter. På IoT-området vil dette ske i samarbejde med FORCE Technology gennem Nordic IoT Centre. Der vil være et samarbejde med den nye [Mærkningsordning for It-sikkerhed og Ansvarlig Dataanvendelse](#), hvor vi samtidig kan tilbyde udvidelser til virksomheder, der har brug for at gå skridtet videre og vise, at de lever op til yderligere standarder, herunder nyudviklede [standarder for AI](#). Ligeledes vil aktiviteten være knyttet til cybersikkerhedsforordningen[6], hvor vi både vil formidle viden og på sigt certificere produkter.

Sikring af kritiske systemer og kritisk infrastruktur (*forskning, udvikling, videnspredning*): Når vi digitaliserer vores kritiske systemer og kritiske infrastruktur og forbinder dem til internettet, er det vigtigt, at vi som samfund kan have tillid til disse systemer. Det kræver fokus på cybersikkerhed og håndtering af nye engineering-udfordringer inden for AI og IoT. Det omfatter dels sikker udvikling af produkter samt test af produkter og systemer dels avancerede løsninger til at undgå og til at opdage angreb – bl.a. baseret på AI-løsninger. Endvidere omfatter det metoder og teknologi for at håndtere nye typer teknisk gæld som IoT- og AI-systemer kan oparbejde. Aktiviteten vil indeholde teknologi- og rådgivningsudvikling.

Dataadgang og anonymisering (*forskning, udvikling, videnspredning*): For at kunne udnytte potentialet i AI er det vigtigt med adgang til testdata – data der kan være følsomt og med behov for beskyttelse. Der findes en lang række teknologiske muligheder, som vi i denne aktivitet vil udvikle og stille til rådighed i form af ydelser: Både teknologiudvikling i form af softwarekomponenter (fx [FRESCO](#)) og rådgivningsydelser om brug af teknologierne, samt hjælp til valg af teknologi. Eksempler på teknologier: Federated learning, Edge Computing, brugercentriske løsninger, Anonymisering, Syntetiske data, Multi-party Computation (MPC), Blockchain og smarte kontrakter.

Ansvarlig anvendelse af kunstig intelligens (AI) (*forskning, udvikling, videnspredning*): Vi vil udarbejde og tilpasse eksisterende metoder og værktøjer til udvikling af gennemsigtig, forklarlig og sikker AI med udgangspunkt i en tværfaglig tilgang med øje for organisation og kontekst. Disse værktøjer vil udvikles på baggrund af viden og kompetencer, der er indsamlet og oparbejdet i bl.a. forrige RK-periode, hvor vi har arbejdet med at forstå de udfordringer, virksomheder står overfor, når de skal udvikle og implementere ansvarlig AI. Udvikling af prototyper, der demonstrerer mulighederne, både i forhold til kommunikation og databenyttelse samt gennemsigtige og forklaringsbaserede kunstig intelligens-løsninger (XAI), langs de fire akser: *Fairness*, *Explainability*, *Auditability* og *Safety*. Herunder også en kvalificering af teknologiernes potentiale for at skabe reel *impact*.

Samarbejdspartnere og snitflader til innovationssystemet

Der forventes samarbejde med blandt andre:

- **Universiteter:** AU, DTU, AAU, ITU, KU o.a. samt udenlandske universiteter.
- **GTS-institutter:** FORCE Technology deltager omkring IoT og Nordic IoT Centre. DBI (case-samarbejde om IT resiliens).
- **Organisationer:** DI, [Mærkningsordningen for It-sikkerhed og Ansvarlig Dataanvendelse](#), Dansk Standard, CenSec, Danish Hub for Cyber Security, Rådet for Digital Sikkerhed, ECSO (European Cyber Security Organisation) og IoT Security Foundation.
- **Innovationsnetværk og klynger:** Nye netværk og klynger inden for digitale teknologier og sikkerhed.
- **Private fonde:** Industriens Fond.
- **DIREC:** DTU, KU, ITU, CBS, SDU, AU, AAU og Alexandra Instituttet søger pt. om midler til et nationalt center for forskning i digitale teknologier som beskrevet i [regeringens mål for forskning og innovation](#) fra 2017

Alexandra Instituttet har et tæt samarbejde med de ovennævnte: Forskningssamarbejde med de nævnte universiteter inden for cybersikkerhed, AI og [dansk NLP](#); et stærkt samarbejde med FORCE Technology gennem nuværende aktiviteter; medlem af CenSec, ECSO og IoT Security Foundation; repræsenteret i bestyrelsen for Danish Hub for Cyber Security og Rådet for Digital Sikkerhed og sidder i flere udvalg i Dansk Standard, herunder med formandskab i udvalget for AI. Vi har flere projekter med bevillinger fra Industriens Fond og Innovationsfonden.