| Indsatsområde | Digital sikkerhed, tillid og dataetik | Evt. nr.: | |
|---|---|---|---|

**Indsatsområde kort (resumé)**

Komplekse teknologier som kunstig intelligens (AI) og avancerede it-sikkerhedsløsninger indeholder kæmpestore forretningsmæssige og -kritiske potentialer for danske virksomheder og forudses ifølge en række rapporter[1] at få en nøglerolle i løsningen af vores største samfundsudfordringer. Dette potentiale kan dog ikke indfris, hvis virksomhederne, deres kunder og brugerne helt generelt ikke har tillid til, hvordan maskinlæringsmodeller virker; tillid til, om et datasæt med persondata er anonymiseret tilstrækkeligt; tillid til, om et givent beslutningsstøtteværktøj er retfærdigt, tillid til, om kritisk infrastruktur er sikret mod fejl eller angreb etc. For hvis ikke vi har tillid til, at et system er sikkert og handler i overensstemmelse med etiske overvejelser og domæneviden, så vil vi ikke udnytte det godt nok. Så er systemet ikke *tillidsværdigt.* Tillid til teknologien er brugs- og forretningskritisk, og hvis ikke vi forstår at koble de avancerede teknologier til brugerne i deres givne kontekster og gøre teknologierne tillidsværdige at bruge, vil gevinsten ved at digitalisere essentielle samfunds- og forretningsfunktioner udeblive.

En Gartner-rapport fra 2019 viser, at op mod 80% af alle AI-projekter ender med aldrig at blive implementeret[2]. Det skyldes ofte manglende forståelse – og i nogle tilfælde direkte frygt – hos brugerne for, hvad AI er og kan. Teknologierne må således udvikles og anvendes på måder, der skaber tillid hos dem, der skal anvende dem. Tillid opnås blandt andet ved, at ejerne og udviklerne af teknologierne kan vise, at teknologien er sikker, og at de udviser ansvarlighed og etik gennem f.eks. transparens, forklarlighed og inddragelse.

Med tanke på, at flere og flere af vores samfundsfunktioner, omgivelser og ting, vi bruger i hverdagen, digitaliseres og kobles på internettet, bør udgangspunktet derfor være, at teknologien *er* sikker, hvilket alt for ofte ikke er tilfældet. Dette er en stor, veldokumenteret[3][4][5] udfordring for danske virksomheder og står i vejen for en endnu stærkere og sikker digitalisering. Særligt certificeringer er en metode til at sikre virksomheders arbejde med cybersikkerhed på en så overskuelig måde som muligt.

Der er et kæmpestort potentiale for Danmark og danske virksomheder i cybersikker, tillidsværdig digital teknologi, men for at indfri det, har vi brug for en tværfaglig indsats til at udvikle standardiserede og målbare metoder til at håndtere tillid, ansvarlighed og sikkerhed i brugen af teknologier. Digital ansvarlighed har potentiale til at blive en vigtig konkurrenceparameter for danske virksomheder, så derfor skal denne indsats sikre, at danske virksomheder føler sig overbeviste om og kan dokumentere over for aftagere, brugere, kunder og medarbejdere, at den teknologi, de anvender og udvikler, faktisk er ansvarlig og sikker. Dette vil ske via:

- Udvikling af testfaciliteter og -kompetencer inden for både certificering på cybersikkerhedsområdet med henblik på certificering af ansvarlige AI-løsninger.
- Udvikling af teknologiske services inden for cybersikkerhed i kritisk infrastruktur, herunder brug af AI som værktøj til at opnå dette.
- Udvikling af teknologiske komponenter og rådgivningsværktøjer til at udvikle ansvarlig AI, herunder brug af følsomme data på en sikker måde.
- Udvikling af tværfaglige metoder og procesværktøjer, der fremmer tillid gennem teknologiforståelse og understøtter den organisatoriske implementering af teknologierne.

**1) Målsætninger, aktiviteter og indikatorer**

Danmark er et af de mest digitaliserede lande i verden og er samtidig kendetegnet ved, at vi har en høj grad af tillid til hinanden. Disse to styrkepositioner skal vi fastholde og udnytte ved systematisk at sikre, at de digitale løsninger, vi udvikler, i højere grad *både* er cybersikre *og* forståelige og etiske. Vi skal også have øjnene åbne for det åbenlyse dilemma i, at høj tillid fra borgere også kan være med til at gøre os mere udsatte i forhold til cybersikkerhed.

Gennem vores arbejde med at sikre digitale løsninger hos danske virksomheder oplever vi, at de efterspørger redskaber, standarder og benchmarkingredskaber til at kunne sætte moderne løsninger og nye produkter i drift. Det gælder især inden for arbejdet med store mængder af data og i endnu højere grad, når det handler om avancerede teknologier som maskinlæring og IoT-sikkerhed. Visionen med denne indsats er at bringe Danmark i front som digital teknologileverandør, der tager udgangspunkt i etik, cybersikkerhed, ansvarlighed, brugerinddragelse og kvalitet i digitale løsninger. Vi ved, at mangel på disser værdier i udviklingen kan stå i vejen for at udnytte mulighederne med de digitale

[1] https://innovationsfonden.dk/sites/default/files/2019-09/an-ai-nation-harnessing-the-opportunity-of-ai-in-denmark.pdf, https://www.danskindustri.dk/brancher/di-digital/analysearkiv/brancheanalyser/2018/4/kunstig-intelligens-i-danmark/
[2] Gartner: *Predicts 2019: Analytics and BI Strategy*
[3] https://innovationsfonden.dk/sites/default/files/2018-07/thefuturemarketforcybersecurityindenmark.pdf
[4] https://erhvervsstyrelsen.dk/sites/default/files/2019-03/it-sikkerhed_og_datahaandtering_i_danske_smver.pdf
[5] https://fe-ddis.dk/cfcs/publikationer/Documents/Cybertruslen-mod-Danmark-2020.pdf

teknologier[6]. Indsatsen udarbejder metoder og værktøjer, der skaber højtspecialiserede rammer for at udvikle gennemsigtig og cybersikker teknologi med udgangspunkt i en tværfaglig tilgang, der integrerer organisationsudvikling, brugerperspektiver og markedsbehov.

Dette vil støtte op om både EU's og Danmarks strategier for digitale løsninger baseret på europæiske, skandinaviske og danske værdier som tillid, åbenhed og etisk ansvarlighed, ligesom det vil understøtte flere af FN's verdensmål, særligt dem, der arbejder for ansvarlige og gennemsigtige institutioner[7].

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

Det er indsatsens målsætning at udvikle og modne digitale teknologier inden for områderne *AI and Data Analytics*, *Cybersikkerhed* og *Digital og kritisk infrastruktur* for at skabe og opretholde tilliden til teknologianvendelse. Dette vil ske ved, at vi udvikler en dansk digital test-, demonstrations- og udviklingsfacilitet (TDU), der skal være med til sikre, at danske virksomheder kan skabe forretning og spille ind i danske og europæiske initiativer for ansvarlig brug af teknologier[8,9,10,11,12,13,14].

TDU'en vil i løbet af perioden blive opbygget og komme til at indeholde en samling af teknologiske services, sådan at de virksomheder, der har behov for rådgivning og hjælp til ideer eller tekniske udfordringer inden for digital sikkerhed, tillid og dataetik, kan henvende sig og få hjælp til at komme videre. Der vil blive gennemført aktiviteter inden for fem hovedtemaer, der alle sigter mod at udvikle teknologier og rådgivning og gøre disse mere tilgængelige for aktørerne:

- **Standarder, test og certificering:** Her vil vi arbejde med internationale standarder og test og certificering op imod disse inden for både cybersikkerhed og brug af kunstig intelligens.
- **Sikring af kritiske systemer og kritisk infrastruktur**: Når kritiske systemer og kritisk infrastruktur bliver digitaliseret, er det vigtigt, at de stadig er robuste, og at vi kan have tillid til dem. Dette er vigtigt både i Danmark og udlandet, og det er vigtigt, at danske virksomheder kan lave forretning på dette.
- **Dataadgang og anonymisering:** Adgang til data er ofte et meget stort problem i udviklingen af AI og datadrevne tjenester og forretning. Vi vil i dette tema arbejde med både tekniske løsninger omkring bl.a. anonymisering og generering af syntetiske data samt rådgivningsydelser om samtykke og datadeling.
- **Ansvarlig udvikling og anvendelse af kunstig intelligens**: Kunstig intelligens til beslutningsstøtte og automatiske beslutninger medfører nye udfordringer for gennemsigtighed, forklaringer og ansvarlig anvendelse, såvel teknologiske som organisatoriske. Vi vil arbejde med udvikling og udbredelse af ansvarlig AI.
- **Tillid og udvikling af Dansk AI**: Tillid til AI-systemer baserer sig også i stor grad på brugerens evne til at forstå systemet og vice versa. En af de vigtigste komponenter her er systemers evne til at kommunikere i brugerens sprog. Her vi vil arbejde med videreudvikling af danske sprogressourcer for AI.

TDU'en vil være tilgængelig for alle landets virksomheder og offentlige institutioner. I løbet af perioden gennemføres pilot-cases med min. 20 virksomheder. TDU'en 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 mellem Alexandra Instituttet, FORCE Technology og Nordic IoT Centre.

Den tilstræbte effekt er, at danske virksomheder kan holde sig i front i den globale konkurrence ved at opnå dyb viden om og kompetencer inden for sikker og ansvarlig AI samt om de teknologiske og procesmæssige redskaber til at udvikle og implementere det. Den forventede effekt monitoreres gennem indsatsen via en række af nedenstående indikatorer, som evalueres årligt:

| | 2021 | 2022 | 2023 | 2024 | Total |
|---|---|---|---|---|---|
| Virksomheder der deltager i vidensprednning (antal) | 90 | 90 | 90 | 90 | 360 |
| Case- og demonstrationsprojekter med virksomheder (antal) | 3 | 4 | 5 | 5 | 17 |
| Teknologiske services under udvikling | 2 | 2 | 2 | 2 | 8 |
| Forskning og udvikling (F&I-ansøgninger, kompetenceopbygning) | 1 | 2 | 2 | 1 | 6 |
| Samarbejder med videnpartnere og øvrige aktører | 4 | 4 | 5 | 5 | 18 |

[6] https://www.wired.com/story/we-need-to-build-up-digital-trust-in-tech/ og https://home.kpmg/dk/da/home/indsigt/2019/07/mistillid-bremser-digitaliseringen.html
[7] https://www.verdensmaalene.dk/maal/16
[8] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[9] https://digst.dk/strategier/cyber-og-informationssikkerhed/
[10] https://fe-ddis.dk/cfcs/nyheder/arkiv/2019/Pages/sektorstrategier.aspx
[11] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
[12] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
[13] https://digst.dk/strategier/kunstig-intelligens/strategi-for-kunstig-intelligens/
[14] https://webshop.ds.dk/da-dk/søgning/35-020-informationsteknologi-it-generelt/ds-pas-2500-12020

**Aktivitetstemaer/emner:**

**Standarder, test og certificering** *(videnspredning, rådgivning, standardisering):*
Denne aktivitet vil fortsætte og udvide Alexandra Instituttets og FORCE Technology's involvering i standardisering af nye avancerede digitale teknologier. Det er vigtigt, at Danmark kan spille ind i arbejdet med at udvikle standarder, og at danske SMV'er er repræsenteret, så det sikres, at arbejdet tilpasses danske forhold. Både Alexandra Instituttet og FORCE Technology er allerede involveret i standardiseringsarbejde, hvilket vil blive intensiveret i denne aktivitet. Standarder kan hjælpe virksomheder med at navigere i de forskellige sikkerhedsniveauer og give dem redskaber til at placere sig selv og deres produkter på disse niveauer – noget, vi ved fra virksomhederne (især SMV'erne), kan være en stor udfordring. Desuden er standarder en måde for virksomheder at kommunikere sikkerhedsniveau med deres kunder, hvilket er vigtigt, da vi begynder at se flere og flere krav fra kunder om, at produkter skal leve op til visse standarder.

Vi vil udbygge og udvikle digitale test- og certificeringsfaciliteter. På IoT-området vil dette ske i en forlængelse af det tætte samarbejde mellem FORCE Technology og Alexandra Instituttet fra samarbejde om IoT- og cybersikkerhed i de to tidligere RK-perioder og gennem Nordic IoT Centre.

Der vil være et samarbejde med den nye Mærkningsordning for It-sikkerhed og Ansvarlig Dataanvendelse, som i øjeblikket er i gang med at specificere nogle krav, hvor GTS-institutterne spiller ind med konkret teknisk viden.

Derudover vil vi tilbyde udvidelser til virksomheder, der har brug for at gå skridtet videre og vise, at de lever op til yderligere standarder, både inden for cybersikkerhed og AI samt inden for kombinationen af de to områder. Indenfor AI vil dette være en udvidelse af det standardiseringsarbejde, Alexandra Instituttet har bidraget til på styregruppeniveau såvel nationalt som internationalt. På cybersikkerhedsområdet vil dette være knyttet til cybersikkerhedsforordningen[11], hvor vi både vil formidle viden og rådgive om cybersikkerhed samt certificere produkter.

**Sikring af kritiske systemer og kritisk infrastruktur** *(forskning, udvikling, videnspredning)*:
Både Danmark og andre lande er i gang med at digitalisere kritiske systemer og kritisk infrastruktur og forbinde dem til internettet. Det gælder rent digital kritisk infrastruktur, som vores samfund er afhængig af, og dermed spiller denne aktivitet ind i verdensmålene 16.6 og 16.7. Det gælder også fysisk kritiske systemer i vores virksomheder og fysisk kritisk infrastruktur, der digitaliseres. Dette gælder i særdelshed OT-netværk (operational technology, dvs. datanetværk i fabriks- og produktionsmiljøer modsat klassiske it-netværk), IoT-enheder samt samfundsmæssigt kritisk infrastruktur i f.eks. forsyningssektoren.

Begge steder åbnes der op for digital kommunikation og koordinering – blandt andet for at opnå økonomiske og energimæssige effektiviseringer for at sikre den grønne omstilling. Aktiviteten understøtter dermed verdensmålene 9.1, 9.4, 7.2 og 7.3. Det er vigtigt, at vi stadig kan have tillid til disse systemer. Det kræver fokus på cybersikkerhed og håndtering af nye designmæssige og organisatoriske udfordringer inden for AI og IoT. Det omfatter dels sikker udvikling af produkter samt test og certificering af produkter og systemer, dels avancerede løsninger til at undgå og til at opdage angreb – bl.a. løsninger baseret på AI. Det kræver viden om og løsninger på nye trusler, herunder f.eks. udvikling af kvantecomputere.

Denne aktivitet vil både omhandle sikring af kritiske systemer i danske virksomheder og dansk kritisk infrastruktur, men vi vil hovedsageligt fokusere på at hjælpe danske virksomheder med at kunne levere produkter og tjenester til kritiske systemer og kritisk infrastruktur i både Danmark og udlandet. Både herhjemme og i udlandet er der øget fokus på cybersikkerheden i kritisk infrastruktur – bl.a. via NIS-direktivet.

**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. Det samme gælder generel udnyttelse af den stadigt større mængde data, der opsamles. Disse data kan være både personfølsomme og forretningsfølsomme.

Der findes en lang række teknologiske muligheder for at udnytte data, samtidig med at der er fokus på sikring af data. Vi vil i denne aktivitet udvikle og stille disse teknologier til rådighed i form af ydelser: Både teknologiudvikling i form af softwarekomponenter (f.eks. FRESCO) og rådgivningsydelser om brug af teknologierne, samt hjælp til valg af teknologi. Eksempler på teknologier kan være *federated learning*, *edge computing*, *brugercentriske løsninger*, *anonymisering*, *syntetiske data*, *multi-party computation (MPC)*, *blockchain* og *smarte kontrakter*.

**Ansvarlig udvikling og anvendelse af kunstig intelligens** (*forskning, udvikling, videnspredning*):
Der er stor efterspørgsel på konkrete og tilgængelige værktøjer til at udvikle ansvarlig kunstig intelligens. Vi vil således udarbejde og tilpasse eksisterende metoder og værktøjer til udvikling af gennemsigtig, forklarlig og cybersikker AI med udgangspunkt i en tværfaglig tilgang med øje for teknologiske muligheder, brug, organisation/kultur og kontekst.

Disse værktøjer vil blive udviklet på baggrund af viden og kompetencer, der er indsamlet og oparbejdet i bl.a. forrige RK-periode, hvor vi har identificeret en lang række af de udfordringer, virksomheder står overfor, når de skal udvikle og implementere ansvarlig AI, herunder mål for indsatsen, komplicerede juridiske og etiske spørgsmål, inddragelse af datasubjekter og brugere af løsningerne[15].

Vi vil med udgangspunkt i dette udvikle prototyper, der demonstrerer mulighederne, både i forhold til brugerflade og databenyttelse samt gennemsigtige og forklaringsbaserede AI-løsninger (XAI), langs de fire akser: *Fairness*, *Explainability*, *Auditability* og *Safety*[16]. Herunder også en kvalificering af teknologiernes potentiale for at skabe reel *impact* gennem udvikling af metoder og værktøjer og teknologiske komponenter, der styrker tilliden til AI-løsninger. At sikre tillid til AI-løsninger handler også om at brugerne forstår, hvad løsningerne gør og kan, og hvordan de bruger dem i praksis. Målet er at styrke teknologiforståelsen og udvikle nye metoder og inddragelsesprocesser, der bidrager til, at brugere og borgere oplever, at de kan have tillid til AI – en aktivitet, porteføljen også vil indeholde.

**Tillid og udvikling af dansk AI** *(Forskning, udvikling og videnspredning)*:
At sikre tillid til AI-løsninger handler i høj grad også om, at løsningerne anvender et sprog, der forstås af brugerne. Derfor er det helt afgørende at sikre udviklingen af danske sprogmodeller, der gør det muligt at udvikle AI-løsninger på dansk. Med udgangspunkt i det open source repository (DaNLP[17]), som blev udviklet i forrige RK-periode, etablerer vi en test- og demonstrationsplatform for benchmark og gentræning af modeller samt udvikler nye basismodeller og datasæt, som virksomheder frit kan benytte i udviklingen af AI-løsninger. Dette vil være med til at skabe indhold til den nye platform www.sprogteknologi.dk, som Digitaliseringsstyrelsen har lanceret i sommeren 2020, og vil være et vigtigt teknologisk fundament for sikre, at brugerne i sidste ende får tillid til de løsninger, der udvikles.

## 2) Indsatsens relevans og potentiale

Målgruppen for dette initiativ er danske virksomheder, både SMV'er og større virksomheder, som ønsker at sikre udvikling, vækst og eksport gennem digitalisering. Der ligger et enormt, uforløst potentiale i de fleste danske virksomheder for at anvende kunstig intelligens i deres produkter, tjenester og drift. Ligeledes er der en voldsom vækst i behov for cybersikkerhed, både i eksisterende produkter og i kraft af væksten af IoT- og AI-baserede produkter. Indsatsen vil understøtte danske virksomheders anvendelse af den nyeste teknologi inden for kunstig intelligens og cybersikkerhed, så vi sammen kan leve op til de høje sikkerhedsstandarder, høje etiske standarder og beskyttelse af kundes data, som blandt andet beskrives i ATVs vision "Trusted AI – made in Denmark" i Bedre sundhed med AI?.

Det samlede potentiale for digital sikkerhed, tillid og dataetik er enormt. For cybersikkerhed anslås potentialet at være 8 milliarder DKK i 2025 for traditionelle produkter (alene i Danmark). Hertil kommer det behov for cybersikkerhed, som den anslåede vækst for *cloud computing* (markedsstørrelse på 5.400 milliarder DKK i 2025) og IoT (markedsstørrelse på 10.000 milliarder DKK i 2025) genererer[3]. Potentialet for kunstig intelligens i Danmark er anslået til 35 milliarder DKK i 2030[18] i direkte vækst og 9 milliarder DKK i forbedret velfærd. McKinsey estimerer, at anvendelsen af kunstig intelligens kan generere en værdi på 36.000 milliarder DKK på verdensplan[19]. Tallene på verdensplan viser, at dette område er et stort og voksende marked, som det er vigtigt for danske videnvirksomheder at være på forkant af.

*"Digital ansvarlighed har potentialet til at blive et vigtigt konkurrenceparameter for danske virksomheder. I DI er vi blandt initiativtagerne til mærkningsordningen for it-sikkerhed og digital ansvarlighed. Som sådan er vi meget interesserede i beslægtede initiativer, der kan være med til at styrke den sikre og ansvarlige datanvendelse i dansk erhvervsliv. I den forbindelse finder vi dette initiativ som værende særdeles relevant."*

Christian Hannibal (Digitaliseringspolitisk chef, DI) på bedreinnovation.dk

I en undersøgelse fra IDA svarer 69% af de adspurgte virksomheder, at kundernes (digitale) tillid i høj eller meget høj grad er vigtig[20]. Alligevel er tilliden til digitale tjenester faldende både i Danmark[21] og internationalt[22,23]. Tillid til digitale systemer kræver, at brugerne ved og stoler på, at disse systemer er cybersikre, så de virker, som de skal, og så hverken data eller systemer kan misbruges. Cybersikkerhed bliver et stadigt større konkurrenceparameter, særligt fordi det er et krav, der stilles enten direkte fra kunderne eller i form af regulering.

Inden for cybersikkerhed kommer der flere og flere krav – både danske[9,10], fra EU[11,8] og andre eksportmarkeder til virksomheder, der vil levere produkter, komponenter og services til kritisk infrastruktur. Samtidig begynder danske og udenlandske kunder at stille cybersikkerhedskrav til deres it-, IoT- og OT-leverandører.

---

[15] Kunstig intelligens i praksis, oplevelser og erfaringer fra +20 virksomheder. Alexandra Instituttet, September 2020
[16] E. Toreini, et al., 2020. The relationship between trust in AI and trustworthy machine learning technologies. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT* '20). Association for Computing Machinery, New York, NY, USA, 272–283. https://dl.acm.org/doi/abs/10.1145/3351095.3372834
[17] https://danlp.alexandra.dk
[18] https://innovationsfonden.dk/sites/default/files/2019-09/an-ai-nation-harnessing-the-opportunity-of-ai-in-denmark.pdf
[19] https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Notes%20from%20the%20frontier%20Modeling%20the%20impact%20of%20AI%20on%20the%20world%20economy/MGI-Notes-from-the-AI-frontier-Modeling-the-impact-of-AI-on-the-world-economy-September-2018.pdf
[20] https://ida.dk/media/5580/daarlig-dataetik-er-koncentreret-blandt-virksomheder-der-ikke-bruger-kundedata-csl.pdf
[21] https://www.pwc.dk/da/artikler/2019/10/tillidsbarometeret-2019-digitalisering-data.html
[22] https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/03/consumer-loss-barometer-2019.pdf
[23] https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/

*"Der er ingen tvivl om, at Danmark skal have førertrøjen, når det kommer til ansvarlige digitale løsninger. Behovet herfor er ikke blevet mindre med den accelererende ibrugtagning af AI/ML uden egentlig governance på området. […] Derfor er det også et væsentligt område for Danmarks eksportmuligheder på gov-tech området. […]"*
Claus Rosenstand (Digital Hub Denmark Professor, Digital Hub Denmark) på bedreinnovation.dk

En manglende indsats inden for ansvarlig anvendelse af digital teknologi vil hindre danske virksomheder i fortsat at udnytte digitaliseringens muligheder, og det vil svække deres konkurrenceevne internationalt. Denne indsats har som formål at bringe danske virksomheder op blandt eliten af internationale leverandører ved at tage udgangspunkt i de styrkepositioner, som understøtter sikker og ansvarlig digitalisering[2,24]. Eksempelvis beskriver den nationale strategi for kunstig intelligens[25] Danmarks styrkepositioner inden for ansvarlig brug af AI og generel digitalisering. Heri beskrives specielt: "et ansvarligt grundlag for kunstig intelligens" (initiativ 1.1), som også sætter "sikkerhed i højsædet" (initiativ 1.3). Disse styrkepositioner er vores stærkeste kort i den internationale konkurrence. Samtidig understøtter denne indsats EU's europæiske tilgang til ekspertise og tillid[26]. Alt i alt skal Danmark kunne levere "Trusted AI made in Denmark" med høje sikkerhedsstandarder, høje etiske standarder og beskyttelse af kundernes data.
**Målgruppens fremtidige behov** er afdækket gennem en række analyser udarbejdet af Alexandra Instituttet:

- **The Future Market for Cybersecurity**: Baseret på desk-research og en række ekspertinterviews. Udarbejdet i samarbejde med Innovationsfonden og Deloitte.
- **Analyse af modenheden inden for IoT-sikkerhed:** Dybdegående undersøgelse af danske virksomheders arbejde med IoT-sikkerhed samt udvikling af modenhedsmodel.
- **Virksomhedsforløb med 20 danske virksomheder:** Case-forløb med fokus på virksomhedernes individuelle udfordringer med IoT-sikkerhed i CIDI-projektet støttet af Industriens Fond.
- **Tilstandsmåling af cyber- og informationssikkerheden i Danmark:** Analyse til understøttelse af Initiativ 3.6 i den danske strategi for cyber- og informationssikkerhed.
- **Markedsafdækning omkring Security by Design:** Undersøgelse om behov og potentialer for at løfte kompetencerne i Security by Design hos mellemstore virksomheder i Danmark
- **Kunstig intelligens i praksis**: Analyse som afdækker udfordringer og tilgangen når man implementerer AI i virksomheder. Anbefalingerne bygger på interviews med mere end 20 danske virksomheder.

Derudover har vi en god dialog med relevante branche-og interesseorganisationer, bl.a. DI, IT-Branchen, Dansk Erhverv, 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 sikkerhed om certificering, standarder og lovgivning.

**3) Markedssvigt og konkurrencesituation**

Understøttelse af udvikling og anvendelse af kunstig intelligens og cybersikkerhed kræver høj specialistviden kombineret med viden og erfaring med organisatorisk implementering. Der er mange situationer, hvor en virksomhed uproblematisk kan indkøbe systemer og kompetencer fra en af mange leverandører. Der er også mange situationer, hvor en virksomhed har behov for leverancer, som er i henhold til standarder eller tilmed certificeret. Sidst, men ikke mindst er der mange situationer, hvor man som virksomhed er interesseret i at benytte en neutral og uvildig leverandør; enten for at undgå eksempelvis vendor lock-in, sikre uvildighed, anvende fælles ressourcer (f.eks. open source), eller fordi markedet p.t. ikke kan levere den nyeste viden.

Som GTS-institut står Alexandra Instituttet i en unik position for at fungere som mediator for generelt tilgængelige ressourcer og kompetence. Vi er forpligtet til at levere den nyeste viden til en bred skare af virksomheder i en neutral og uvildig form.

En af de største udfordringer i forhold til at gennemføre AI-projekter i virksomheder 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 vigtig med nem adgang til uvildig rådgivning inden for tillid og digital sikkerhed, hvilket er en central GTS-rolle.

Indenfor eksempelvis dansk sprogteknologi (NLP) er der et udtalt behov for generelt tilgængelige ressourcer, som alle kan benytte sig af. Der er desuden et udtalt behov for adgang til den nyeste forskningsbaserede viden om anvendelse af NLP. Det drejer sig om basiskomponenter, der gør det muligt at konstruere AI-baserede systemer, der fungerer på dansk. Der er en generel konsensus blandt relevante danske virksomheder om, at normale markedskræfter ikke kan

[24] https://atv.dk/udgivelser-viden/verdens-foerende-tech-regioner-danmarks-styrkepositioner-globalt-perspektiv
[25] https://digst.dk/strategier/kunstig-intelligens/strategi-for-kunstig-intelligens/
[26] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_da.pdf

håndtere dette, og at kun en neutral og uvildig virksomhed kan fungere som mediator. En lang række virksomheder har udtrykt ønske om, at Alexandra Instituttet påtager sig denne rolle, herunder bl.a. KMD, Topdanmark, TV2 Regioner, Unsilo og MaxManus.

*"Vi er meget entusiastiske omkring DaNLP's eksisterende arbejde og tanker fremadrettet. Som jeg ser det, leverer DaNLP håndgribelig værdi, som vi selv har efterspurgt ifm. dansk sprogteknologi – og tilmed i en form, som er anvendelig for særligt SMV'er."*

Marius Hartmann, Chefkonsulent, Erhvervsstyrelsen

En lignede situation findes inden for eksempelvis anonymisering af data og modeller samt produktion af syntetisk data til træning af maskinlæringssystemer. Maskinlæringssystemer kræver generelt adgang til store mængder data. Noget som i særdeleshed mindre virksomheder kan have vanskeligt ved at være i besiddelse af. Moderne maskinlæringsmetoder, såsom federated learning (distribueret maskinlæring), kan være en metode til at håndtere udnyttelse af data på tværs af virksomheder. På samme måde er der forskellige tilgange til at træne modeller på data, for derefter at eksponere modellerne, som ikke er almindeligt tilgængelige. På samme måde som med basis-omponenter til dansk sprogteknologi er der bred konsensus om, at flere af disse måder at håndtere mangel på data på forudsætter en neutral og uvildig part.

Vi ser også situationer inden for cybersikkerhed, hvor der er brug for GTS'ernes uvildighed og fokus på SMV'er – især i forbindelse med standardisering og certificering. Inden for standardisering er der brug for en stemme, der kan understøtte SMV'erne, da standardernes udformning er afgørende for konkurrenceevnen, og de færreste SMV'er har ressourcer til selv at deltage i dette arbejde. Det er vigtigt for Danmark generelt at kunne deltage i standardiseringsarbejde med nogen, der støtter danske virksomheder, så det ikke kun er de helt store udenlandske virksomheder, der er til stede. Det er især vigtigt i disse år, da standardisering på området gennemgår en stor udvikling. ETSI EN 303 645 er lige blevet frigivet og vil sandsynligvis danne baggrund for EU-regulering. Samtidig har ENISA med udgangspunkt i *cybersecurity act* netop udgivet et kandidatforslag (EUCC) til en EU cybersecurity-certificeringsordning, som sandsynligvis hurtigt kan blive vedtaget som lov. Det er vigtigt, at danske virksomheder har adgang til certificering og uvildig rådgivning, som kan give indblik i standarderne, og som kan understøtte virksomhederne i processen mod en certificering. Alexandra Instituttet har i flere analyser peget på, at de danske SMV'er ofte anser standardisering som så komplekst og arbejdskrævende, at de ikke har ressourcer og kompetencer hertil.

For at imødekomme virksomhedernes behov for ansvarlighed og tillid vil dette arbejde afhjælpe det eksisterende markedssvigt i forhold til certificering, standarder, neutral og uvildig støtte til danske virksomheder. Der er ikke nogen anden enkelt aktør i Danmark, som kan påtage sig denne rolle, hvilket minimerer risikoen for konkurrenceforvridning. Gennem en proaktiv risikostyring under hele indsatsen vil vi løbende følge "state-of-the-industry" for at identificere risici for konkurrenceforvridning, med særlig fokus på: Rådgivning inden for cybersikkerhed og rådgivning omkring kunstig intelligens. I det omfang risici identificeres drøftes forebyggende tiltag med følgegruppen og der igangsættes en inddragende dialog med de pågældende aktører. Der vil gennem hele indsatsen være dialog med virksomheder, rådgivere og offentlige organisationer gennem bl.a. følgegruppen. Derudover er der etableret et godt samarbejde med DI. Gennem disse dialoger (3 møder med følgegruppen samt 1-2 årlige dialogmøder med DI) vil vi løbende holde os orienteret om markedssituationen og sikre, at udviklingen af teknologierne og ydelserne er til gavn for markedet og udfylder et hul, der ikke dækkes af lignende tilbud.

**4) Videnspredning og inddragelse i indsatsområdet**

Videnspredning og involvering af virksomheder, myndigheder og brancheorganisationer vil foregå på forskellige måder – både gennem direkte inddragelse i udviklingsarbejdet og forskellige videnspredningsaktiviteter, som sikrer, at resultaterne fra resultatkontrakten deles og bringes i spil i erhvervslivet.

**Løbende inddragelse af virksomheder**

Som udgangspunkt vil aktiviteterne i indsatsområdet tage afsæt i virksomhedsnære problemstillinger. Det tætte samarbejde med virksomheder bliver en vigtig del af udviklingsarbejdet i indsatsområdet. Dette sikrer vi løbende gennem interviews og case-samarbejder med virksomheder, hvor vi udvikler og afprøver løsninger og redskaber i tæt samspil med virksomhedernes behov og udfordringer.

**Formidlingsaktiviteter**

Formidlingen af viden og resultater vil være en central del af indsatsens formål, og vi har i tilrettelæggelsen af aktiviteterne en ambition om at sikre, at viden og resultater når så bredt ud som muligt og modne virksomhederne til at arbejde med indsatsens fokusområder. Derfor vil formidlingsaktiviteterne både bestå af klassiske formidlingsarrangementer, der inspirerer og styrker teknologiforståelsen, såsom workshops og webinarer, hvor vi bringer vores metoder og redskaber i spil og giver virksomhederne vejledning i, hvordan de anvender resultaterne i praksis. Ligeledes består formidlingen i at poste indsigter og resultater via sociale medier, hvor vi linker til faglige indlæg på f.eks. blogs og artikler på egne eller andres medieplatforme. Vi formidler løbende satsningens resultater gennem artikler i fagmedier,

blogs, konferencer (nationale og internationale), whitepapers og hands-on guides, der helt overordnet vil have til formål at klæde virksomheder på til at udvikle og implementere ansvarlige løsninger. Det vil både handle om at formidle eksisterende standarder og om at hjælpe virksomheder med, hvordan de bedst anvender standarder og certificeringer i deres arbejde. Vi vil desuden udarbejde case-beskrivelser, der formidler erfaringer og opmærksomhedspunkter fra virksomheder.

**Samarbejde med eksisterende initiativer**
Vi vil bruge vores store netværk og tætte relationer til eksisterende teknologiklynger, virksomheder og netværk til at nå bredt ud i vores formidling og inddrage virksomheder og myndigheder. Vi har etablerede samarbejder med forskellige brancheorganisationer (herunder DI, DE og IT-Branchen) og har gode erfaringer med fælles konferencer, webinarer og netværksarrangementer. Vi har desuden samarbejde med Danish Hub for Cybersecurity og CenSec og indgår i klyngerne DigitalLead og MADE som partner. Dette i kombination med etablerede samarbejder med Erhvervshus Midtjylland og Erhvervshus Hovedstaden og den kommende European Digital Innovation Hubs (DIHs) giver et stærkt fundament for at nå ud til et bredt spektrum af danske virksomheder.

Vi har allerede tætte relationer til Dansk Standard – både inden for standardiseringsarbejdet omkring cybersikkerhed og AI. Dette samarbejde vil blive styrket og modnet i forbindelse med den kommende satsning, ligesom der vil være fokus på at få opbygget et tæt samarbejde med den nye Mærkningsordning for it-sikkerhed og ansvarlig anvendelse.

**Advisory Network**
Som følgegruppe for projektet vil vi bruge og udvide Alexandra Instituttets allerede etablerede faglige netværk og følgegrupper fra den nuværende RK-periode. Vi vil inddrage relevante netværk som følgegruppe i de aktiviteter, de har interesse i. Vi har omkring 70 virksomheder i disse netværk og vi bruger dem allerede aktivt til sparring, som følgegruppe og som mål for vidensprednin. Nogle af de virksomheder, der er repræsenteret i disse netværk, er: KMD, Kamstrup, Lyngsøe Systems, Hounö, Seluxit, Itadel, Bankdata, Danske Bank, Novo Nordisk, Grundfos og NOVAX.

**5) Nyhedsværdi og ambitionsniveau**

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.

**Standarder, test og certificering:** Vil hovedsageligt være anvendelse af eksisterende state-of-the-art (SotA) og bred vidensprednin om SotA og regulering på området. På trods af, at det er SotA, er dette stadig en vigtig aktivitet, der både indeholder videnhjemtagning, cases med virksomheder, opbygning og markant styrkelse af GTS'ernes kompetencer inden for certificering af cybersikkerhed, hvor FORCE Technology har stor erfaring med certificering generelt, og hvor Alexandra Instituttet har stor erfaring med cybersikkerhed. På trods af, at disse aktiviteter teknologisk omhandler SotA, så har det en høj nyhedsværdi, da der sker rigtig meget på standardiseringsområdet lige nu. Vi vil markant udvide danske test- og certificeringskompetencer inden for cybersikkerhed, så danske virksomheder har nemmere adgang til certificering af deres produkter og rådgivning på området. Vi forventer ydelser inden for dette felt fra år 1, men disse vil blive udbygget til at omhandle flere standarder og dybere ydelser gennem projektet.

**Sikring af kritiske systemer og kritisk infrastruktur:** Vil være en blanding, hvor reguleringsdelen handler om videnhjemtagning og -spredning af SotA og anvendelse af SotA i flere danske virksomheder, blandt andet gennem cases og vidensprednin. Den del, der omhandler brug af AI for at øge sikkerheden i kritiske systemer og infrastruktur, vil indeholde anvendt forskning og udvidelse at SotA. Dette vil være en udbygning af kompetencer opnået i nuværende RK-periode og fra andre F&I-projekter, herunder et projekt bevilget af Center for Cybersikkerhed (CFCS) omkring Honeypots i OT-systemer, samt et ansøgt projekt hos innovationsfonden: CRUCIAL. Vi forventer flere case-forløb med virksomheder i løbet at de første 2 år og derefter større fokus på ydelser inden for dette felt.

**Dataadgang og anonymisering:** Mange virksomheder har haft et stort fokus på simpel compliance med GDPR, hvilket har sat visse projekter på pause. Men der er nu et større fokus på at få data i brug inden for rammerne af GDPR, herunder databeskyttelse gennem design. Virksomhederne mangler dog viden og tekniske værktøjer for at kunne indfri værdien af data, både persondata og brug af forretningskritisk data på tværs af organisationer. Der mangler viden om ansvarlig brug af data og om tekniske løsninger som anonymisering (*differential privacy*), *privacy preserving machine learning* (f.eks. *federated learning*) og generering og brug af syntetiske data. Alle metoder til at få mest mulig værdi ud af data på en sikker og ansvarlig måde. Men det er også områder, hvor der er et gab mellem forskningen på området og anvendelsen af denne. Rådet for Digital Sikkerhed anbefaler, at der prioriteres ressourcer til arbejde med syntetiske sundhedsdata.[27]

[27] Kommer i løbet af få dage.

Aktiviteterne bygger på viden og erfaring fra projekterne BlockDAP (Industriens Fond), HedaX (Innovationsfonden), HD360 (Innovationsfonden) og SODA (H2020), og vi vil dermed kunne udvikle og tilbyde ydelser baseret på cutting edge-forskning.

**Ansvarlig udvikling og anvendelse af kunstig intelligens (AI):** Der er stadig et gab mellem visionerne for ansvarlig AI og udviklingen, implementeringen og brugen af det. Denne aktivitet vil fokusere på konstruktion af teknikker til et bredt AI-metodesæt, som bygges op under ansvarlig udvikling og anvendelse af kunstig intelligens. Her læner vi os op ad SotA-metoder inden for forklaringer (XAI), sporbarhed og reproducerbarhed samt den voksende mængde forskning inden for hybridsystemer (symbolske og sub-symbolske metoder i samme løsning). Arbejdet med organisering, governance af AI-systemer og forretningsudvikling for danske virksomheder hænger uløseligt sammen med tekniske tilgange til ansvarlig kunstig intelligens. Heri indgår også arbejdet med at udvikle værktøjer til implementering af AI i organisationer, da en succesfuld implementering er en vigtig forudsætning for, at den ønskede effekt opnås.

**Tillid og udvikling af dansk AI:** Aktiviteterne vil fokusere på at anvende internationalt udviklede modeller såsom BERT og GPT-3 og etablere en platform til benchmark/vurdering af modeller i en dansk kontekst. Det skal gøre det lettere for danske virksomheder at overskue nye internationale modellers performance på forskellige danske datasæt, hvilket vil spare dem for 'besværet' med hver især løbende at undersøge og afprøve nye modeller.

Et andet område vil være at opbygge både infrastruktur og rutine i at gentræne modeller, når der er ny data tilgængelig. Det vil særligt handle om at have GPU'er nok til for eksempel at træne og gentræne modeller, og hvad der kommer herefter.

Det tredje område fokuserer på snittet mellem moderne distribueret maskinlæring (såsom *federated learning*) og forretningsmodeller, som gør det muligt at udnytte data på tværs af organisationer – med et specielt fokus på dansk tekst. Herunder dækkes også arbejde med kontekstualiseret anonymisering (*refraction*), hvilket p.t. er et problem, hvor der ikke findes gode, stabile og nemt tilgængelige løsninger, specielt på dansk.

**6) Indsatsområdets kobling til viden- og innovationssystemet**

Der samarbejdes med blandt andre:

**Universiteter –** Inden for dette indsatsområde har vi allerede et stærkt samarbejde med AU, DTU, KU, ITU og AAU via andre F&I-projekter. Desuden er Alexandra Instituttet en central partner i Digital Research Centre Denmark (DIREC), hvor også DTU, KU, ITU, CBS, SDU, AU, AAU er partnere. Både Alexandra Instituttet og FORCE Technology er partnere i Danish Hub for Cybersecurity sammen med alle de danske universiteter og flere andre uddannelsesinstitutioner og nuværende innovationsnetværk[28]. Der er derudover et samarbejde med en række europæiske universiteter. Vi forventer at fortsætte og udvide samarbejdet med både danske og udenlandske universiteter i løbet af denne indsats. Dette er en vigtig grænseflade til ny viden, hvor GTS'erne kan tage rollen med at bringe denne viden i anvendelse i danske virksomheder. Samarbejdet med forskningsmiljøerne vil omfatte sparring ift. teknologisk kompetenceopbygning, fælles nye forskningsansøgninger, eventuel deltagelse i cases med fokus på at løse forskningstunge opgaver og udarbejde fælles videnskabelige publikationer.

**GTS-institutter -** FORCE Technology og Alexandra Instituttet har inden for dette indsatsområde allerede et godt samarbejde fra nuværende og tidligere RK-projekter og Nordic IoT Centre. De to GTS'er komplementerer hinanden godt. FORCE Technology har stor erfaring med certificering og hardware, mens Alexandra Instituttet har stor erfaring med både de tekniske, organisatoriske og forretningsmæssige sider af digitalisering, AI, software og cybersikkerhed. Ud over FORCE Technology og Alexandra Instituttet kan der være case-samarbejde med DBI om it-resiliens.

**Internationale organisationer -** Alexandra Instituttet er medlem af European Cyber Security Organisation (ECSO) og IoT Security Foundation.

**Virksomheder -** Danske virksomheder vil indgå i en lang række centrale aktiviteter, herunder case- og demonstrationsprojekter, behovsafdækning og vidensspredning.

**Brancheorganisationer og Erhvervshuse** - blandt andet Dansk Erhverv. Dansk Industri samt IT-Branchen og de regionale erhvervshuse, særligt Erhvervshus Midtjylland og Erhvervshus Hovedstaden. Omdrejningspunktet for samarbejdet med brancheorganisationer og erhvervshuse vil være virksomhedsrekruttering til case-projekter, assistance med afklaring af konkurrenceforhold, behovsafdækning og domæneviden.

**Organisationer og standardisering -** Mærkningsordningen for it-sikkerhed og ansvarlig dataanvendelse, Dansk Standard, CenSec, Rådet for Digital Sikkerhed, ATV og Danish Hub for Cyber Security.

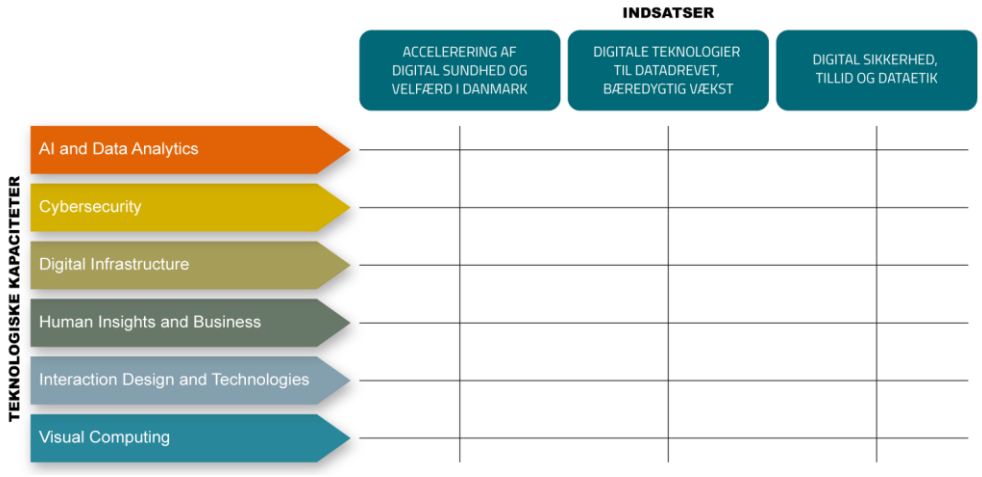
**Innovationsnetværk og klynger -** Nye netværk og klynger inden for digitale teknologier og sikkerhed. Samarbejdet vil omhandle fælles vidensspredningsaktiviteter samt matchmaking til relevante virksomheder fra målgrupperne.

**Private fonde** - Industriens Fond. Fokus på gearing af indsatsens aktiviteter med nye F&I-projekter.

[28] DIREC er et nationalt center for forskning i digitale teknologier som beskrevet i regeringens mål for forskning og innovation fra 2017. Danish Hub for Cybersecurity er støttet af Industriens Fond. Både DIREC og Danish Hub for Cybersecurity er sat i verden for at facilitere samarbejde inden for forskning og anvendelse af forskning inden for dette indsatsområde.

## 7) Sammenhæng med instituttets strategi og afsæt i instituttets ressourcer

Indsatsen er baseret på Alexandra Instituttets forslag på Bedreinnovation.dk af samme navn, hvor forslaget fik stor opbakning. Indsatsen udgør én ud af tre strategiske indsatser, som sammen med Alexandra Instituttets teknologiske kapaciteter udfolder vores strategiske faglige fokus i 2021-24 (se figur).




Den nye RK-model introducerer to dimensioner i form af *indsatser*, som er baseret på samfunds- og erhvervsmæssige behov, og af *teknologiske kapaciteter*, som er Alexandra Instituttets teknologiske styrkepositioner, der skal til for at imødekomme behov i indsatserne. Matricen udfolder Alexandra Instituttets samlede Resultatkontraktindsats. Der forventes store horisontale synergier, hvor basisteknologier fra de teknologiske kapaciteter bidrager til løsning af udfordringer i flere indsatser.

Cybersikkerhed og AI og Data Analytics er centrale teknologier for denne indsats og er både i nuværende og tidligere RK- og strategiperioder centrale teknologiske kapaciteter for Alexandra Instituttet.

Indsatsen er tæt koordineret med følgende andre indsatser:

- IoT-drevet forretningsdesign, FORCE Technology og Alexandra Instituttet: Indsatsen bidrager med opbygning af viden om IoT til ”Digital sikkerhed tillid og dataetik".
- Accelerering af digital sundhed og velfærd i Danmark, Alexandra Instituttet og Teknologisk Institut: Denne indsats bidrager med viden og teknologiske løsninger om sikker brug af sundhedsdata og ansvarlig brug af AI til ”Accelerering af digital sundhed og velfærd i Danmark”.
- Digitale teknologier til datadrevet, bæredygtig vækst, Alexandra Instituttet og FORCE Technology: Denne indsats bidrager med viden og teknologiske cybersikkerhedsløsninger til ”Digitale teknologier til datadrevet, bæredygtig vækst”.

## 8) Konkrete aktiviteter

De gennemgående aktivitetstemaer i indsatsen er 1) forskning og teknologisk kompetenceopbygning, 2) udvikling af TDU og teknologisk service, og 3) vidensprednin og samarbejder. Som opstart af aktiviteterne beskrevet under afsnit 1, forventes følgende aktiviteter igangsat under disse temaer:

**Forskning og teknologisk kompetenceopbygning:**

Med det formål at opbygge viden vil vi fra projektets start igangsætte:

- Afdækning af juridiske, tekniske, forretningsmæssige, organisatoriske, brugermæssige såvel som standardiseringsmæssige behov for og krav til ansvarlighed.
- Udvikling af teknikker til dataadgang og anonymisering af data under GDPR, copyright og anden lovgivning: Anonymisering af ikke-strukturerede data, generering af syntetiske data, secure multiparty computation i brug i nye domæner, distribuerede maskinlæringsteknikker til træning af modeller.
- Forskning inden for privacy-by-design/databeskyttelse gennem design med fokus på ansvarlig brug af data.
- Udvikling af AI-teknikker til opdagelse af angreb (*intrusion detection*) på OT-netværk og IoT-netværk (bygger videre på et nuværende projekt mellem Alexandra Instituttet og Aalborg Universitet kombineret med AI- og cybersikkerhedsviden hos Alexandra Instituttet)
- Standardiseringsarbejde – dette vil foregå fra start og i hele projektets levetid. Arbejde i standardiseringsudvalg i Dansk Standard, i EU-regi (f.eks. CEN/CELEC) og internationalt (f.eks. ISO) og videnhjemtagning fra internationale standarder (f.eks. NIST). Bidrag og overvågning af standarder og fremtidig certificering inden for NLP, ansvarlighed og kunstig intelligens, cybersikkerhed i IoT og OT på produkt- og systemniveau, cybersikkerhed generelt og avanceret kryptografi.

**Udvikling af TDU og teknologisk service:**
Ovenstående aktiviteter udføres for at understøtte ydelser i den digitale TDU omkring indsatsområdet. På baggrund af disse aktiviteter vil vi i løbet af det første år starte følgende aktiviteter omkring teknologisk service:

- Udvikling af konkrete tekniske værktøjer til dataadgang og anonymisering af data under GDPR, copyright, og anden lovgivning: Anonymisering af ikke-strukturerede persondata, generering af syntetiske data, secure multiparty computation (beregning på krypterede data) i brug i nye domæner, distribuerede maskinlæringsteknikker til træning af modeller.
- Sideløbende med ovenstående vil vi udvikle rådgivningsydelser om ansvarlig brug af data rettet både mod virksomhedernes tekniske, organisatoriske og forretningsmæssige udfordringer.
- Tekniske samt organisatoriske, governance- og brugerrettede værktøjer til støtte for ansvarlig AI.
- Infrastruktur og processer for opdatering af danske modeller for NLP med tilhørende ydelsesudvikling omkring udvikling og vedligehold af danske sprogressourcer
- Certificering: Vi forventer at kunne certificere efter ETSI EN 303 645 "Cyber Security for Consumer Internet of Things: Baseline Requirements" efter det første år. Vi vil fra første år arbejde på at kunne certificere efter standarder inden for IEC 62443.

For at understøtte udviklingen af TDU og afprøve services vil vi gennemføre minimum 3 demonstrations-projekter med virksomheder det første år.

**Vidensprednin**g **og samarbejder**

- Udvikling af format for referencegruppe/Advisory Network baseret på allerede etablerede faglige netværk og følgegrupper fra den nuværende RK-periode. Vi vil afholde tre møder med følgegruppe/Advisory Network, hvor vi inddrager relevante netværk i de aktiviteter, de har interesse i. Dette vil sikre videnspredning, relevans for målgruppen samt sikre konkurrencesituationen.
- Etablere samarbejde med Mærkningsordning for It-sikkerhed og Ansvarlig Dataanvendelse
- Udvikling af metoder og formater, der styrker teknologiforståelse i forbindelse med organisatorisk implementering af komplekse teknologier, som AI og cybersikkerhed er.
- Klassiske formidlingsarrangementer i samarbejde med eksisterende initiativer og andre aktører i innovationssystemet, herunder workshops og webinarer, artikler i fagmedier, blogs, konferencer (nationale og internationale), whitepapers og hands-on-guides.