Bilag 1

Ydelsesaftale

mellem

Forsvarets Efterretningstjeneste

og

Danmarks Tekniske Universitet

om

forskningsbaseret myndighedsbetjening inden for sikkerhedsområdet

2025

Indholdsfortegnelse

1 Formål

Denne ydelsesaftale (herefter "Ydelsesaftalen) indgår som bilag til Rammeaftale mellem Forsvarets Efterretningstjeneste (FE) og Danmarks Tekniske Universitet (DTU) om forskningsbaseret myndighedsbetjening 2025-2028 (herefter "Rammeaftalen"). Ydelsesaftalen beskriver arten og omfanget af de ydelser, som DTU i henhold til Rammeaftalen udfører for FE i 2025.

Ydelsesaftalen er bygget op om faglige indsatsområder, hvor Parterne samarbejder om forskning- og vidensopbygning, løsning af korte og længerevarende rådgivningsopgaver samt evt. særlig formidling af resultater til FE's medarbejdere.

Som bilag til Ydelsesaftalen udarbejder Parterne et konkret opgavebilag for indsatsområdet (Bilag A). Uanset opgavebilagenes indhold vil der løbende over året være fleksibilitet til at omprioritere og inddrage nye opgaver, efter en konkret vurdering og skriftlig aftale herom.

2 Faglige indsatsområder

DTU's forskningsbaserede myndighedsbetjening af FE omfatter aktiviteter inden for forskning og forskningsbaseret rådgivning. Aktiviteterne er fordelt på indsatsområder.

Som input til denne Ydelsesaftale blev der d. 17. september 2024 afholdt workshop mellem de to faglige miljøer mhp. at drøfte indsatsområderne for de kommende år. Fra DTU deltog forskere fra DTU Compute, DTU Space, DTU Aqua, DTU Physics, DTU Engineering Technology og DTU Management.

Første del af workshoppen var dedikeret til de syv projektaktiviteter. Anden del var generelle indlæg med introduktion til FE, sikkerhed i samarbejdet samt forskningsbaseret myndighedsbetjening. Efter en postersession i et åbent forum var den sidste del af workshoppen ~~var~~ opdelt i de tre temaområder - AI/ML, Cyber og Situational Awareness med faglige drøftelser mellem de faglige miljøer.

Ydelsesaftalen vil blive forelagt Ledelsesgruppen til godkendelse.
Det er DTU's ansvar at sørge for at indsatsområderne dækkes med et tilstrækkeligt forskningsmæssigt niveau og indhold, indenfor aftalens økonomiske rammer, til at kunne levere de relevante ydelser på de aftalte indsatsområder.

Der kan i forlængelse af projekterne igangsættes formidlingsaktiviteter, som er skræddersyet til FE's behov.

Fordelingen af forskningsmidlerne mellem disse indsatsområderne aftales mellem FE og DTU, og afspejler både det det aktuelle behov for aktiviteter på områderne og forventningen til det fremtidige behov.

Der er generelt også mulighed for strategisk forskningssamarbejde med internationale partnere.

2.1 Indsatsområde Kunstig Intelligens

Det ene tema for samarbejdet er kunstig intelligens herunder machine learning. Kunstig intelligens giver mulighed for at automatisere både ressourcekrævende og komplicerede processer.

For FE er det især mulighederne for at kunne analysere meget store datasæt hurtigere, som er i fokus. Der er lige nu et misforhold mellem den kraftige stigning i datamængder og -kompleksiteten og FE's evne til at udnytte data. Det skal kunstig intelligens (AI) være med til at løse ved bl.a. at automatisere manuelle analytiske arbejdsgange. I FE-sammenhæng vil der altid være en 'human-in-the-loop' og der vil altid være konkrete personer som har ansvaret for de vurderinger og varslinger, som udgår fra FE.

Imidlertid hviler sådanne slut-produkter ofte på meget omfattende manuelle undersøgelser og processer, som kan automatiseres i højere grad end i dag. Dette især for at sænke responstiden, øge opdagelsesevnen og højne kvaliteten i FEs leverancer.

FE benytter åbent tilgængelige metoder og værktøjer til AI, som udspringer dels fra globale private aktører, dels fra globale forskningsmiljøer. Med samarbejdet håber FE også specifikt at styrke de danske AI-talenter.

For DTU er det vigtigt at opretholde og styrke universitetets position som et førende forsknings- og undervisningsmiljø inden for kunstig intelligens (AI) og maskinlæring (ML).

Der foregår omfattende forskning, udvikling og anvendelse af AI på mange af DTU's institutter herunder DTU Compute, DTU Management, DTU Energy og DTU Space.

Den grundlæggende forskning i AI finder primært sted på DTU Compute, hvor der forskes i mange af de kerneområder, der er vigtige for den fortsatte udvikling og succes indenfor AI, herunder machine learning, computer vision, billedanalyse, kognition/perception, formelle metoder, numerisk analyse/optimering, statistik, matematik, logik, distribuerede computer/data systemer software og data science.

En styrkeposition for DTU Compute, er forskning i statistisk ML, hvilket omfatter udvikling og analyse af grundlæggende matematiske metoder til modellering, læring, og beslutningstagen baseret på store og/eller komplekse datasæt (billeder, lyd, tekst, komplekse netværk og grafer), herunder forskning i dybe neural netværk.

Motiveret af et voksende samfundsmæssigt behov for robuste og sikre AI systemer, har DTU Compute desuden et øget fokus på menneskelige og samfundsmæssige aspekter af udbredelsen af AI, herunder *privacy, safety, fairness* og *trustworthiness* som bl.a. indbefatter grundlæggende forskning i *explainable* AI (XAI), usikkerhedskvantificering (UQ), bruger oplevelse (UX), menneske-maskine interaktion (HCI), og beslutningstagen i usikre og kritiske situationer.

2.2 Indsatsområde Cyber Defence

The second theme of the collaboration is cyber defence. Cyber defence concerns with the safeguarding of cyber-physical assets and infrastructure against cyber threats.

As technology continues to advance, in particular with AI-based systems, so do the sophistication and frequency of cyber threats.

The importance of a robust cyber defence strategy cannot be overstated, as the potential consequences of cyber-attacks extend beyond financial losses to include compromised national security, privacy breaches, and disruption of critical services.

With the rapid expansion of digital networks and the growing reliance on technology in all aspects of our lives, a resilient cyber defence posture is not just a necessity but a fundamental requirement for ensuring the stability, security, and continuity of our modern, interconnected world.

Organizations, governments, and individuals alike must adopt a proactive approach to cybersecurity in order to prevent, detect, and respond to cyber-attacks effectively.

FE has a broad interest in research in cyber-related areas, in order to understand developments and be at the forefront of future cyber capacitates.

For FE, it is important to contribute to the Danish cyber security research environment, and at the same time gain access to new and specialized knowledge in cyber security. This includes research into next-generation capabilities and new areas of cybersecurity.

Cyber deception including honey pots as a defence against cyber-attacks, and as a method of gathering information about cyber-attacks, is a research area with FE's interest.

Threat models help to understand cyber threats and inform the defences against them. As the internet changes, it is important that our threat models change to keep up and provide the best possible protection. This is an area where research can contribute significantly to future solutions.

Developments in secure algorithms and opportunities for the application of AI are proven and promising areas, where research will help the cyber defences of the future, FE wants to research in this area.

The battle between hackers and cyber defenders is an ongoing development, research into detection methods, including anomaly detection, will help improve FE's ability to detect and combat cyber attacks
For DTU, the research interests in the area are numerous, covering everything from cybersecurity in pervasive computing to privacy-enhancing technologies and applied cryptography.

In particular, DTU research focuses on the design, development and testing of cybersecurity services for networked computing systems, including models, policies and mechanisms to support secure collaboration in open dynamic systems, such as sensor networks, mobile systems, the Internet of Things (IoT) and Cyber-Physical Systems (CPS).

Key research areas include cyber-deception, intrusion detection, secure multi-party computation, cyber-biometric authentication, trust management, malware detection, blockchain, machine/deep learning, IoT/CPS/edge security, botnet monitoring, and alert data correlation, to mention a few.

2.3 Indsatsområde Situational Awareness

Situational Awareness (SA) er en kerneopgave for FE.

SA illustreres ofte ved at vise slutresultatet, nemlig det store overblik projiceret op på væggen. Men i virkeligheden er SA en lang kæde af dataanalyse, som starter med adskillige sensorer, og først til allersidst giver overblik.

DTU har stor viden og erfaring inden for sensorteknologier og FE håber at kunne styrke sin portefølje af sensorer med nye og bedre varianter, inden for alle kendte, såvel som nye typer af sensing.

DTU har stor erfaring med udvikling af automatiserede dataanalyser, herunder AI/ML. Denne erfaring kan potentielt udvide værktøjsporteføljen for FEs analytikere.

Det afsluttende overblik kræver sammenstilling af data fra mange kilder. For at være på forkant, skal denne sammenstilling gøres intelligent, og dette kræver metoder som rækker langt ud over, bare at lægge ting oven på hinanden på en graf, eller et kort.

DTU kan hjælpe med flere led i denne kæde, og bidrage med avancerede, forskningsbaserede, nytænkende, state-of-the-art løsninger på mange af de underliggende udfordringer.

SA vedrører overvågning bredt, til lands, til vands, i luften og på havbunden. Ligeledes anvendes et bredt spektrum af sensorer som radarer, antenner, optisk synlige, infrarøde, termiske og hyperspektrale kameraer, akustiske sensorer som hydrofoner, sonarer, optiske fibre, osv.

Sensor- og datafusion er essentielt for SA. Sammenligning af data fra forskellige sensorer kan give væsentligt forbedrede efterretninger, både når komplementerende sensorer kan bekræfte et mål eller når en given sensor ikke har optimale forhold, fx pga. vejrforhold.

Der forefindes flere metoder til at forbedre overvågning, fx bedre udnyttelse af sensorer, nye sensorer, sensor fusion, fejlkilder (herunder jamming og spoofing) samt anomalisøgning i big data.

For FE er det især mulighederne for at detektere og identificere objekter som er i udvikling.

FE er interesseret i mulighederne for at analysere og især sammenstille store mængder data, indsamlet med forskellige typer sensorer (for eksempel, radar hhv. optisk) og med variationer i både temporal og rumlig opløsning.

Hensigten med forskningstemaet er at stimulere DTU til at udnytte sine forskningskompetencer til at pege på nye metoder og løsninger.

For DTU er forskningsinteresserne inden for området talrige dækkende fra civile til dual use.

De er ligeledes spredt udover en række institutter ofte med overlap i emner:
- DTU Space analyserer primært satellitdata.
- DTU Elektro analyserer netværk, optiske fibre, magnetometre, samt sensorer på autonome systemer, mm.
- DTU Aqua analyserer akustiske signaturer fra sonarbøjer og lignende.
- DTU Fysik og Elektro forsker i kvanteteknologier, der har anvendelser i kvantesensorer, -kryptering, -computere, mv.
- DTU Compute analyserer datastrømme, og mønstre i store datamængder

3 Økonomi fordelt på indsatsområder for 2025

Det er Parternes forventning, at forskningsandelen hhv. rådgivningsandelen hver vil udgøre 50 % af den samlede kapacitetsramme, jf. Rammeaftalen. Bevillingens tentative fordeling på indsatsområder fremgår af tabellen nedenfor.

Bevillingen for 2025 udgør 6 mio. kr.