Innovatsiooniprojekti ideekavand[1]

AVALIKU SEKTORI INNOVATSIOONIVÕIMEKUSE TÕSTMINE

Ideekavandit täites palume tutvuda riigikantselei veebilehel toodud soovituste ja juhistega projekti esitajale.

Innovatsiooniprojekti nimi	AI mudelite treeningkeskkond
Innovatsiooniprojekti fookusvaldkond	☐ Droonitehnoloogiate valdkond ☒ Tehisintellekti lahenduste valdkond
Innovatsiooniprojekti panus valitsuse tegevuskava prioriteetidesse	☒ Riigi kriisikindluse suurendamine ☒ Majanduse kasvule kaasa aitamine ☒ Riigi tõhus juhtimine
Innovatsiooniprojekti esitajad (tulevased RK partnerid) (asutus/asutused)[2]	Sihtasutus CR14
Projektijuht või ideekavandi esitaja kontaktisik (nimi, asutus, e–posti aadress ja telefon)	Carl-Robert Reidolf, SA CR14, carlreidolf.cr14.ee, +372 513 2294
Innovatsiooniprojekti kestus (kuudes)	18 kuud *Ajaarvestust alustame üldjuhul partnerluslepingu sõlmimisest.*
Innovatsiooniprojekti kogumaksumus (sh käibemaks, kui on abikõlblik)	Kogumaksumus: 1 828 000 eurot
Käibemaks	CR14 ☒ jääb kulu tegija kanda (käibemaks abikõlblik) ☐ saab küsida riigilt tagasi (käibemaks ei ole abikõlblik) *Vastav info täita iga partneri kohta (kopeeri ridu ning kirjuta partneri nimi juurde)*
Lühendid	AIDA – Artificial Intelligence Deployable Agent; Euroopa Kaitsefondi projekt AI-põhiste küberkaitselahenduste arendamiseks AI – Artificial Intelligence; API – Application Programming Interface; CR14 – Sihtasutus CR14; DCM – Defence Cyber Marvel; EDF – European Defence Fund; EDF-2023-DA-CYBER-DAAI – konkreetne EDF projekt; AI ja küberkaitse arendusprojekt GBR – United Kingdom; Suurbritannia riigikood GDPR – General Data Protection Regulation;

[1] Juhul kui ideekavand on mõeldud **asutusesiseseks kasutamiseks**, siis lisage vastav alus ideekavandi päisesse.
[2] **Partner EL struktuurivahendite mõttes**, kes viib ise läbi innovatsiooniprojekti elluviimisega seotud hanked, sõlmib lepingud ning vastutab aruandluse eest.

	GPU – Graphics Processing Unit; HPC – High Performance Computing; IKT – Info- ja kommunikatsioonitehnoloogia; JDM – Justiits- ja Digiministeerium; KMAK – Kaitseministeeriumi arengukava; KM – Kaitseministeerium; KM VA – Kaitseministeeriumi valitsemisala; LLM – Large Language Model; ML – Machine Learning; MKM – Majandus- ja Kommunikatsiooniministeerium; MLOps – Machine Learning Operations; MoD – Ministry of Defence; MTÜ – Mittetulundusühing; NATO – North Atlantic Treaty Organization; NATO ACT – Allied Command Transformation; NATO DIANA – Defence Innovation Accelerator for the North Atlantic; RBAC – Role-Based Access Control; RK – Riigikantselei; valitsust toetav keskne riigiasutus RKAK – Riigikaitse arengukava; TAIE – Teadus- ja arendustegevuse, innovatsiooni ning ettevõtluse arengukava;
1. Probleemikirjeldus (max 2 lk) ***Kirjeldage lahendamist vajavat probleemi, selle olulisust ning keda see probleem puudutab.*** • *Selgitage, miks on probleem aktuaalne.* • *Hinnake probleemi mõju (nt rahaline kokkuhoid, keskkonna- või sotsiaalne kasu).Kirjeldage probleemi tausta. Mida on probleemi lahendamiseks Eestis juba tehtud või mis on tegemisel? Tooge välja relevantsed teiste riikide kogemused probleemi lahendamisel.*	
Riigikaitse arengukava 2022–2031 rõhutab kaasaegsete tehnoloogiliste ja infosüsteemide arendamist, eelhoiatus- ja luurevõime tugevdamist ning innovatsioonivõime kasvatamist kaitsevaldkonnas. Kaasaegne riigikaitse sõltub üha enam andmepõhistest otsustest ning kiiresti arenevatest tehisintellekti lahendustest. Arvutusvõimsuse kasv ja AI tehnoloogiate areng on viimastel aastatel oluliselt suurendanud süsteemide võimekust töödelda suuri andmemahtusid ja toetada keerukaid otsustusprotsesse. See on toonud kaasa ka sõjanduses kognitiivsete töövahendite laialdasema kasutuse, tõstes operatsioonide tempot ning suurendades infomahu keerukust, mida tuleb reaalajas hallata. Sellises keskkonnas tekib kaitsevaldkonnas selge vajadus võimekuse järele hinnata ja kasutada tehisintellekti lahendusi turvaliselt, usaldusväärselt ja kontrollitud tingimustes. Eriti kriitiline on see olukordades, kus AI süsteemide töökindlus ja käitumine peavad olema prognoositavad ka kriisi- või konfliktitingimustes. Ilma vastava võimekuseta on keeruline tagada, et kasutusele võetavad lahendused vastavad riigikaitselistele nõuetele ning ei tekita täiendavaid riske. Täna on probleemiks see, et: • puudub piisav praktiline kogemus, kuidas rakendada AI lahendusi kõrge turvanõudlusega keskkondades; • puuduvad testitud ja valideeritud lähenemised, mis võimaldaksid hinnata erinevate tehnoloogiliste valikute sobivust; • organisatsioonidel ei ole ühist arusaama sobivaimatest arhitektuuridest ja tööprotsessidest AI kasutamiseks kaitsevaldkonnas. Lisaks raskendab olukorda asjaolu, et paljud olemasolevad AI lahendused põhinevad pilvetehnoloogiatel, mis ei pruugi olla sobivad tundlike andmete töötlemiseks ega kriitiliste operatsioonide	

toetamiseks. Samas on lokaalsed lahendused sageli keerukad, ressursimahukad ning nõuavad spetsiifilist kompetentsi, mida ei ole alati piisavas mahus olemas.

CR14 roll kahese kasutusega tehnoloogiate valdkonnas toob esile vajaduse arendada võimekust, mis võimaldaks:

- hinnata AI lahenduste turvalisust ja usaldusväärsust,
- testida nende käitumist realistlikes tingimustes,
- ning toetada kaitsevaldkonna eesmärkide saavutamist kontrollitud keskkonnas.

Praegune olukord, kus selline võimekus on killustunud või puudulik, piirab võimalust võtta tehisintellekti lahendusi kasutusele süsteemselt ja teadlikult. See omakorda aeglustab AI strateegia elluviimist ning suurendab riski, et tehakse tehnoloogilisi valikuid, mille tegelik sobivus ilmneb alles hilisemas faasis.

Sellest tulenevalt on keskne probleem mitte üksiku tehnilise lahenduse puudumine, vaid ebapiisav teadmiste ja praktikate baas, mis võimaldaks teha põhjendatud ja turvalisi otsuseid tehisintellekti kasutuselevõtuks kaitsevaldkonnas. Kaitsevaldkonnas põrkub tehisintellekti kasutusse võtmine järgmiste väljakutsetega:

PROBLEEM 1: Kaitsevaldkonna toodetesse tehisintellekti ja masinõppe võimekuste integreerimiseks on vaja GPU-põhiseid lahendusi mudelite treenimiseks ja häälestamiseks. Praktikas on organisatsioonidel kaks valikut: rajada oma treeningtaristu või kasutada pilveteenuseid. Oma infrastruktuuri loomine on aga kulukas, aeganõudev ja eeldab spetsiifilist tehnilist kompetentsi, samas kui pilvelahenduste kasutamine ei pruugi olla sobiv tundlike andmete töötlemiseks, andmesuveräänsuse tagamiseks ega kriitiliste süsteemide töökindluse kindlustamiseks. Lisaks võib sõltuvus välistest teenusepakkujatest ja keerukused olemasolevate turvanõuetega integreerimisel piirata nende praktilist kasutust. Seetõttu puudub täna universaalne, turvaline ja praktiliselt rakendatav viis AI võimekuste arendamiseks ja testimiseks kõrge nõudlusega kaitsevaldkonna keskkonnas.

PROBLEEM 2: KM VA asutused toodavad hulgaliselt dokumentatsiooni ning dokumentatsioonis orienteerumine võib olla keerukas. On teada, kuidas copiloti agendid võimaldavad vestelda ettevõtte dokumentide ja protseduuridega. Kuid mis saab siis, kui dokumentide sensitiivsuse tase ei võimalda neid pilveteenuse pakkuja AI-vestlussüsteemi üles laadida? Sellisel juhul tuleb kasutada lokaalset AI-süsteemi või rajada organisatsiooni sisene lahendus.

PROBLEEM 3: Mitmed kaitsetööstuse ettevõtted arendavad tarkvararakendusi ja koodi seadmetele või infrastruktuurile. Nende lähtkoodi sensitiivsus ei võimalda kasutada tuntud koodi-copiloteid, nagu GitHub Copilot või muud pilvepõhised lahendused. Samas on avalikult kättesaadavad avatud AI-mudelid, mis võivad tarkvaraarendust kiirendada. Kuid kohaliku LLM-i käitamine on aeglane ning seab arendaja sülearvutile või töölauale väga suured nõudmised.

Positiivne MÕJU: CR14 suudab pakkuda väärtust ja optimeerida kulusid AI-ga seotud arendusprojektides lähtuvalt KM VA Tehisintellekti strateegias sätestatud tegevustele ning loob uue ja kaasaegse mõõtme küberkaitse õppuste läbiviimisse. Lähim selline projekt on EDF-2023-DA-CYBER-DAAI. AI/ML tegevusi treenitakse DCM (GBR) seeria õppusel juba neljandat aastat. Käesoleval hetkel kasutatakse selleks pilvetehnoloogiatel baseeruvaid AI rakendusi. Eraldiseisva taristu omamine võimaldab eelpool mainitud, aga ka tulevasi kaitsevaldkonna projekte tagada turvalises kontrollitud keskkonnas. Praegused soovid CR14 suunal on pidevalt kasvavad. Erinevad kliendid (näiteks NATO ACT, GBR MoD, JDM, MKM) soovivad tegeleda laiemalt AI/ML teemadega koos meiega.

Lisaks riiklikule kontekstile mõjutab antud probleem ka Eesti positsiooni rahvusvahelises kaitse- ja innovatsiooni ökosüsteemis. CR14 on NATO DIANA (Defence Innovation Accelerator for the North Atlantic) võrgustiku raames valitud ametlikuks testkeskuseks ning kuulub NATO Innovation Range'i võrgustikku, kus CR14 vastutab IKT, tehisintellekti ja kübervaldkonna testimise suuna eest ühe viiest määratud testkeskkonnast. Selline roll eeldab võimet pakkuda kaasaegset, turvalist ja operatiivselt realistlikku tehnoloogilist keskkonda, kus arendada ja valideerida ka tehisintellekti lahendusi. Kui vastav võimekus puudub või on piiratud, vähendab see oluliselt Eesti suutlikkust täita oma rolli liitlassuhetes ning osaleda täismahus NATO innovatsiooniprogrammides. Samuti piirab see kohalike ettevõtete ja

arenduspartnerite võimalusi testida ja arendada lahendusi rahvusvahelisel tasemel. Seetõttu ei ole tegemist üksnes organisatsioonisisese või riikliku probleemiga, vaid see omab laiemat mõju Eesti konkurentsivõimele, kaitsetööstuse arengule ning rollile NATO ja Euroopa tehnoloogilises koostöös.

Negatiivne MÕJU: Täiendava rahastuse mittetagamine tooks kaasa Kaitseministeeriumi valitsemisala tehisintellekti strateegias seatud võime- ja ajaraamide nihkumise vähemalt 1–2 aasta võrra, vähendades ministeeriumi suutlikkust integreerida AI-põhiseid lahendusi riigikaitse võtmeprotsessidesse ettenähtud tempos. See omakorda pidurdab võimearendust valdkondades, mille kiire areng on NATO-s ja liitlaste seas strateegiliselt vältimatu.

Taotlusega toetame KM valitsemisala AI strateegia elluviimist ning tehisintellekti võimekuse süsteemset arendamist CR14-s. Käesolev algatus on seotud CR14 varasemate arendustegevustega, sh AIDA projektiga (Artificial Intelligence Deployable Agent), mis on Euroopa Kaitsefondi (EDF) rahastatud rahvusvaheline arendusprojekt. AIDA projekti eesmärk on arendada AI-põhiseid küberkaitse lahendusi, sealhulgas autonoomseid ja poolautonoomseid agente, mis toetavad küberintsidentide tuvastamist, analüüsi ja käsitlemist kogu elutsükli ulatuses. CR14 osaleb projektis koordinaatorina, panustades rahvusvahelise koostöö kaudu AI rakendamise praktilise kogemuse kujundamisse. AIDA projekti raames loodav teadmus ja esialgne võimekus keskendub konkreetsetele kasutusjuhtumitele (nt küberkaitse), kuid ei kata laiemat vajadust hinnata ja rakendada AI lahendusi süsteemselt kogu kaitsevaldkonnas. Seetõttu on vajadus arendada edasi lähenemist, mis võimaldaks hinnata erinevaid tehnoloogilisi ja arhitektuurseid valikuid laiemas kontekstis. Oluline on tagada, et nii varasemates projektides loodud kui ka käesoleva katseprojekti raames tekkiv teadmus ja võimekus ei jääks ajutiseks, vaid oleks rakendatav ka pärast projekti lõppu. Vastasel juhul tekib oht, et mitme aasta jooksul kogutud teadmised ja arendatud lahendused ei leia jätkusuutlikku kasutust ning investeeringute mõju väheneb oluliselt. Projekti järjepidev rahastamine tagab, et Eesti positsioon Euroopa kaitsetööstusökosüsteemis tugevneb, liitlaste usaldus kasvab ning AI-võime areng ei takerdu strateegilise teetõkke taha.

ALTERNATIIVID: pilvepõhised lahendused, kus kood ja taristu asub mõne suure teenusepakkuja juures (Google; Microsoft jne).

RISK: Kaitseotstarbelisi projektide tegemine pilveplatvormidel on täiendava riskiga. AI/ML näol on tegemist tulevikku vaatava valdkonnaga, kus modernse sõja võidab riik, kellel on tugevam AI.

2. Projekti eesmärk

Sõnastage konkreetne, selge ning mõõdetav eesmärk[i], mille saavutamist või mitte saavutamist on võimalik hinnata.

- *Kirjeldage, kuidas plaanite projekti eesmärgi saavutamist mõõta.*

Projekti eesmärk on katseprojekti raames välja töötada ja valideerida tehniline keskkond ning sellega seotud toimemudel, mis võimaldavad kaitsevaldkonnas turvaliselt, autonoomselt ja skaleeritavalt arendada ja rakendada tehisintellekti lahendusi.
Fookus on hinnata:

1. kuidas rajada ja opereerida GPU-põhist AI/ML treeningkeskkonda;
2. kuidas rakendada lokaalseid LLM-lahendusi tundlike andmete töötlemiseks (nt organisatsioonisisene AI-juturobot);
3. kuidas toetada tarkvaraarendust turvalise AI-lahendusega ilma lähtekoodi välisteenustega jagamata.

Projekti tulemusena ei looda ainult tehnilist lahendust, vaid pilootide kaudu valideeritud kriteeriumite raamistik, mis määratleb KM VA AI võimekuse arendamiseks sobivaimad tehnoloogilised, arhitektuursed ja organisatsioonilised valikud.
Katseprojektis valideeritakse lahendusi vähemalt kolmes kasutusstsenaariumis:

- AI mudelite treenimine ja arendamine,
- dokumentidel põhinev teadmusotsing ja otsustustugi,
- AI-toega tarkvaraarendus turvalises keskkonnas.

Projekti edukust hinnatakse eelkõige katsetuste ja pilootide tulemuste ning nende põhjal tehtavate järelduste kaudu, mitte ainult valmis süsteemi olemasolu alusel.

1. Tehnilise lähenemise valideerimine
   - Loodud ja testitud on GPU-põhise treeningkeskkonna prototüüp (määratud mahus)
   - Katsetatud on vähemalt:
     - 1 dokumentidel põhinev AI-juturobot
     - 1 tarkvaraarendust toetav AI lahendus
   - Hinnatud lahenduste jõudlust (kiirus, kasutatavus, ressursikasutus)
2. Kasutatavuse ja sobivuse hindamine
   - Vähemalt 2–3 organisatsiooni/üksust (CR14, KM VA, partnerid) osalevad pilootkasutuses
   - Läbi viiakse vähemalt 3 pilootprojekti või kasutusjuhtumit, tagamaks, et iga kaasatud organisatsioon/üksus saab osaleda vähemalt ühes konkreetses katsetuses ning erinevad kasutusstsenaariumid on kaetud
   - Dokumenteeritakse kasutusstsenaariumid ja piirangud
3. Mõju ja efektiivsuse hinnang
   - Hinnatakse arendus- või analüüsiprotsesside ajavõitu (eesmärk kuni ~30% potentsiaalne paranemine pilootkasutuses)
   - Analüüsitakse alternatiividega (nt pilvelahendused) võrreldes kulusid, paindlikkust ja riske
   - Koostatakse hinnang sõltuvuse vähenemisest välistest teenustest
4. Turvalisuse ja autonoomia valideerimine
   - Katsetatakse lahenduste toimimist ilma tundlike andmete välisteenustele edastamiseta
   - Hinnatakse vastavust KM VA infoturbe nõuetele
   - Kaardistatakse peamised riskid (nt andmelekked, mudeli käitumine)
5. Väljund: otsustus- ja skaleerimisraamistik
   - Koostatakse soovitused lõpliku arhitektuuri ja investeeringute osas
   - Defineeritakse eeltingimused võimekuse skaleerimiseks (2027+)
   - Tulemusi kasutatakse sisendina KM AI strateegia edasiseks rakendamiseks

3. Võimalikud lahendussuunad (max 2 lk)

Kirjeldage võimalikke lahendusi ning tegevusi, millega projekti eesmärk saavutatakse.

- *Kirjeldage võimalikke lahendussuundi, põhjendage eelistatud lahendussuuna valikut (NB! Valitud lahendussuund ei ole siduv, see võib projekti käigus muutuda).*
- *Kirjeldage probleemi lahendamiseks vajalikke tegevusi, mida antud katseprojekti raames plaanitakse teha.*
- *Selgitage, kuidas lahendust katsetatakse. Selgitage, kuidas läbi viidavat katsetust ja selle edukust hindate.*

Projekti eesmärk ei ole ühe konkreetse lahenduse juurutamine, vaid erinevate võimalike lahendussuundade katsetamine ja võrdlev hindamine, et leida sobivaim lähenemine AI võimekuse arendamiseks kaitsevaldkonnas.
Katseprojekti käigus analüüsitakse ja võrreldakse kolme peamist lahendussuunda:

Lahendussuund 1: Tsentraalne GPU-põhine AI treeningkeskkond
Selle lähenemise puhul luuakse prototüüp kesksest AI taristust, kus:
- mudelite treenimine ja häälestamine toimub jagatud GPU-resurssidel,
- kasutajad pääsevad keskkonnale ligi standardiseeritud arendusprotsesside kaudu (MLOps),
- arendus toimub kontrollitud ja turvalises infrastruktuuris.

Katsetamise eesmärk:
- hinnata, kas tsentraliseeritud mudel vähendab arenduskulusid ja -aega,
- mõõta ressursikasutust ja skaleeritavust,
- tuvastada võimalikud kitsaskohad (nt ressursside jagamine, halduskoormus).

Võrdlus alternatiividega: võrreldakse nii hajusa (igas organisatsioonis eraldi) kui ka pilvepõhise lähenemisega.

Lahendussuund 2: Lokaalsed LLM-lahendused (dokumentide ja teadmuse haldus)
Selles suunas katsetatakse, kuidas rakendada lokaalseid keelemudeleid:
- organisatsioonisiseste dokumentide põhjal teadmuse otsimiseks ja töötlemiseks,

- tundlike andmete töötlemiseks ilma välisteenustele ligipääsu andmata.

Katsetamise eesmärk:

- hinnata, kas lokaalne LLM suudab pakkuda piisavat kvaliteeti võrreldes pilvelahendustega,
- mõõta jõudlust (latentsus, täpsus) erinevate mudelite ja konfiguratsioonide lõikes,
- analüüsida turvalisuse ja andmekaitse eeliseid.

Oluline küsimus katsetuses: milline on praktiline kompromiss turvalisuse, kiiruse ja mudeli kvaliteedi vahel?

Lahendussuund 3: Lokaalne AI tarkvaraarenduse toetus

Kolmanda suunana testitakse AI kasutamist tarkvaraarenduse abivahendina:

- koodi genereerimine ja analüüs lokaalse LLM põhjal,
- arendusprotsesside kiirendamine tundlikku lähtekoodi väljastamata.

Katsetamise eesmärk:

- hinnata mõju arendajate produktiivsusele,
- mõõta kvaliteeti võrreldes pilvepõhiste copiloti lahendustega,
- hinnata riistvaranõudeid ja kasutusmugavust.

Katseprojekti lähtekohaks on eeldus, et tsentraalne ja turvaline AI võimekus võib pakkuda parimat tasakaalu:

- kulutõhususe,
- turvalisuse,
- ja skaleeritavuse vahel.

Samas ei ole see valik siduv – projekti käigus võib selguda, et:

- hübriidlahendus (osa lokaalne, osa pilves),
- või hajus lähenemine

on teatud kasutusjuhtumites sobivam.

Katseprojekti raames viiakse läbi järgmised tegevused:

1. Nõuete ja arhitektuuri defineerimine
   – kasutatakse erinevaid arhitektuurimudeleid (tsentraalne vs hajus vs hübriid)
2. Prototüübi loomine (piiratud mahus)
   – GPU-põhine treeningkeskkond
   – lokaalne LLM runtime
   – arendusprotsessi tööriistad
3. Pilootkasutuse läbiviimine
   – vähemalt 2–3 erinevas kasutusstsenaariumis
   – kaasates reaalsed kasutajad (KM VA, partnerid)
4. Andmete kogumine ja analüüs
   – tehnilised mõõdikud (latentsus, jõudlus, kasutus)
   – kasutajakogemus (kasutatavus, väärtus)
5. Võrdlusanalüüs alternatiividega
   – pilvelahendused
   – hajusad lokaalsed lahendused
6. Soovituste ja järelduste koostamine
   – sobivaim arhitektuur
   – edasiarenduse vajadused
   – riskid ja kulumudelid

Katsetamine toimub pilootprojektide ja võrdlusanalüüsi kaudu, kus iga lahendussuunda hinnatakse järgmiste kriteeriumite alusel:

1. Tehniline jõudlus
   - mudelite treenimise kiirus
   - süsteemi latentsus ja töökindlus
   - ressursikasutus (GPU, energia)
2. Kasutatavus
   - arendajate ja lõppkasutajate tagasiside
   - kasutuselevõtu lihtsus

- integreeritavus olemasolevate tööprotsessidega

3. Turvalisus
   - tundlike andmete töötlemise kontroll
   - vastavus infoturbenõuetele
   - riskide olemasolu (nt andmelekke oht)
4. Kulutõhusus
   - arenduskulude muutus
   - operatiivkulud vs pilvelahendused
   - investeeringu tasuvuse hinnang

4. Projekti uuenduslikkus

Tuua selgelt välja projekti uuenduslikkus –mida tehakse senisest teisiti kas see hõlmab uusi tehnoloogiaid, protsesse, toimemudeleid, disaini, turgu vms?

- *Selgitage lahenduse uuenduslikkust nii Eesti kui globaalses kontekstis.*
- *Mis on projektis sellist, mis vajab katsetamist?*

Projekti uuenduslikkus seisneb mitte ainult tehnoloogilises lahenduses, vaid uue AI rakendamise mudeli katsetamises kaitsevaldkonnas, kus ühendatakse autonoomne infrastruktuur, kõrged turvanõuded ja praktiline kasutus.Erinevalt tavapärasest lähenemisest, kus valitakse üks tehniline lahendus ja see juurutatakse, keskendub projekt erinevate arhitektuursete ja tehnoloogiliste valikute katsetamisele, nende võrdlevale hindamisele ning tõenduspõhise otsustusraamistiku loomisele.

Mis tehakse senisest teisiti? Hetkel kasutatakse AI arenduses valdavalt kahte mudelit:

- pilvepõhised lahendused, mis ei sobi tundlike andmete jaoks;
- lokaalsed, killustatud lahendused, mis ei skaleeru ja on kallid.

Projektis katsetatakse kolmandat lähenemist: tsentraalne, turvaline ja jagatud AI võimekus (AI-as-a-capability). Uuenduslikkus seisneb selles, et:

- sama infrastruktuuri peal testitakse mitut kasutusjuhtumit (treening, LLM, arendus),
- hinnatakse reaalset sobivust, mitte ainult tehnilist teostatavust,
- ja tulemuseks ei ole ainult süsteem, vaid mudel, kuidas AI-d riigis kasutada.

Projektis katsetatakse esmakordselt Eestis:

- kaitsevaldkonna jaoks mõeldud tsentraalset GPU-põhist AI infrastruktuuri,
- lokaalsete LLM-ide kasutamist tundlike andmetega,
- AI võimekust kui jagatud teenust mitmele organisatsioonile.

Samas ei eeldata ette, et see mudel ka töötab — seda empirismiga kontrollitakse.

Rahvusvaheliselt on selge trend pilvepõhine AI vs kasvav vajadus andmesuveräänsuse ja autonoomia järele. Projekt on uuenduslik, sest see ei vali neid kahte äärmust, vaid katsetab nende vahelist ruumi ja loob teadmise, millised lahendused töötavad kõrge turvalisuse nõuetega keskkonnas. Projekti keskne väärtus tekib läbi hüpoteeside testimise.

Hüpotees 1: Tsentraalne AI taristu on kulutõhusam ja kiirem kui hajus lähenemine
Eeldus: Ühine GPU-põhine keskkond vähendab arendusaega ja dubleerimist.
Kuidas katsetatakse:

- viiakse läbi pilootprojektid tsentraalses keskkonnas
- võrreldakse:
  - arendusaega
  - ressursside kasutust
  - setup time'i

Mõõdikud:

- arendustsükli kestus
- kasutajate arv vs infrastruktuuri koormus
- kuluhinnang võrreldes alternatiiviga

Hüpotees 2: Lokaalsed LLM-id on piisava kvaliteediga tundlike use case'ide jaoks
Eeldus: Open-source mudelid suudavad katta vähemalt osa kasutusvajadustest ilma pilveta.
Kuidas katsetatakse:

- sama ülesanne lahendatakse:
  - lokaalse LLM-iga
  - pilvepõhise mudeliga

Mõõdikud:

- vastuste kvaliteet
- latentsus
- kasutajate hinnang

Hüpotees 3: AI-toega arendus ilma pilveta annab reaalse tootlikkuse võidu
Eeldus: Lokaalne coding assistant suudab parandada arendajate efektiivsust.
Kuidas katsetatakse:

- arendajad teevad samu ülesandeid:
  - ilma AI-ta
  - lokaalse AI-ga

Mõõdikud:

- ülesande täitmise aeg
- koodi kvaliteet
- kasutajate rahulolu

Hüpotees 4: Turvaline AI arhitektuur on praktiliselt teostatav
Eeldus: On võimalik kasutada AI-d nii, et tundlikud andmed ei lahku kontrollitud keskkonnast.
Kuidas katsetatakse:

- viiakse läbi teststsenaariumid tundlike andmetega
- hinnatakse süsteemi käitumist

Mõõdikud:

- andmelekke risk
- auditilogid
- vastavus infoturbenõuetele

Hüpotees 5: Jagatud AI võimekus on organisatsiooniliselt kasutatav
Eeldus: Mitme organisatsiooni ühine AI keskkond on hallatav ja kasutatav.
Kuidas katsetatakse:

- kaasatakse mitu partnerit pilootkasutusse
- testitakse juurdepääsu, ressursijaotust, töövooge

Mõõdikud:

- kasutusaktiivsus
- konfliktide/arendusprobleemide arv
- kasutajate tagasiside

5. Projekti elluviimisega (katsetusega) seotud riskid ja nende maandamismeetmed

Kirjelda peamisi riske, mis võivad takistada projekti elluviimist või eesmärkide saavutamist, ning kavanda maandamismeetmed.

Projekti elluviimine hõlmab nii tehnoloogilisi, organisatsioonilisi kui ka strateegilisi riske, mis tulenevad uudse AI-võimekuse arendamisest kaitsevaldkonnas. Allpool on välja toodud peamised riskid ja nende maandamise meetmed.

Risk	Tõenäosus	Mõju	Riski olulisus	Maandamismeetmed
Tehnoloogiline risk – lokaalse AI võimekuse ebapiisav kvaliteet (LLM-id jäävad alla pilvelahendustele)	Keskmine	Kõrge	Kõrge	Mitme mudeli testimine ja võrdlus; pilootide läbiviimine; fine-tuning; kasutusjuhtumite täpne piiritlemine

Turvarisk – tundlike andmete lekkimine või mudelite kaudu taastootmine	Madal–keskmine	Väga kõrge	Kõrge	RBAC ligipääsukontrollid; auditilogid; andmete anonümiseerimine; red-teaming; vastavus infoturbenõuetele
Ressursirisk – GPU riistvara tarneviivitused või spetsialistide puudus	Keskmine	Kõrge	Kõrge	Varajane hankimine; mitme tarnija kasutamine; piloot olemasoleval taristul; partnerite kaasamine
Integreerimisrisk – lahenduse sobivus olemasolevate tööprotsessidega	Keskmine	Keskmine–kõrge	Keskmine–kõrge	Pilootprojektid reaalses keskkonnas; API-põhine arhitektuur; lõppkasutajate varajane kaasamine
Kasutuselevõtu risk – madal adopteerimine kasutajate poolt	Keskmine	Keskmine	Keskmine	Koolitus; „early adopter" kaasamine; selged kasutusjuhtumid; kasutajatoe tagamine
Finants- ja jätkusuutlikkuse risk – edasise rahastuse ebakindlus	Keskmine	Kõrge	Keskmine–kõrge	KMAK rahastuse ettevalmistamine; seos strateegiatega; rahvusvahelised projektid; kulumudeli optimeerimine
Strateegiline risk – tehnoloogia kiire areng	Kõrge	Keskmine	Keskmine	Modulaarne arhitektuur; open-source lahendused; pidev tehnoloogiauuendus; rahvusvaheline koostöö

6. Projekti ajakava

Koostage realistlik ajakava, mis hõlmab kõiki projekti tegevusi ning annab sellega sisendi projekti eelarve koostamisele.

- *Ajakava koostamisel arvestage vajalike eel- ja järel- või vahetegevustega (nt partnerluslepingu sõlmimise ettevalmistus kuni 2 kuud, vajalike lubade saamine projekti jooksul vms).*
- *Milliste võimalike puhvritega oleks ajakavas mõistlik arvestada?*
- *Jagage tegevused loogilisteks etappideks, arvestage tegevuste omavahelisi seoseid ning ajalist järgnevust või paralleelsust.*
- *Hangete läbiviimise ajaraami kavandamiseks kasuta hankekalkulaatorit Hankekalkulaator - EIS*

Tegevused	Tegevuse algus (mitmes kuu)	Tegevuse lõpp (mitmes kuu)	Kestus kokku (mitu kuud)
I etapp – katseprojekti ettevalmistus ja tehniline disain			
Projekti käivitamine, detailplaneerimine	1	3	3
Partnerite ja töökorralduse kinnitamine	1	3	3
Nõuete täpsustamine (AI taristu, LLM, turve)	1	3	3
Hangete ettevalmistamine (GPU, tarkvara)	2	4	3
Hangete läbiviimine	3	6	4
II etapp – taristu rajamine ja tehniline ülesehitus			
Riistvara tarne ja paigaldus	5	9	5
GPU keskkonna seadistamine	6	9	4
AI treeningkeskkonna ülesehitus (MLOps)	6	10	5

LLM platvormi paigaldamine (chatbot + coding)	7	10	4
Andmeturbemeetmete rakendamine	6	10	5
III etapp – lahenduste arendus ja katsetamine			
AI mudelite treeningu piloteerimine	11	16	6
Dokumentidel põhineva chatboti piloteerimine	11	16	6
AI tarkvaraarenduse tööriista piloteerimine	11	16	6
Kasutajate kaasamine ja testimine	11	16	6
Süsteemi optimeerimine ja täiendused	11	15	5
IV etapp – testimine ja valideerimine			
Projekti tulemuste hindamine	17	18	2
Dokumentatsioon ja raportid	17	18	2
Jätkutegevuste ja KMAK taotluse ettevalmistus	17	18	2
KOKKU			**18 kuud**

Projekt on kavandatud 18 kuu pikkuse katse- ja käivitamisfaasina, mille eesmärk on luua esmane tehniline baasvõimekus (taristu ja AI teenuste prototüübid) ning valideerida peamised kasutusjuhtumid pilootkeskkonnas.
Ajakava koostamisel on arvestatud järgmiste oluliste teguritega:

- hangete ettevalmistuse ja läbiviimise ajakuluga (ligikaudu 2–4 kuud);
- tegevuste osalise paralleelsusega, et tagada efektiivne ajakasutus;
- taristu tarne- ja paigaldusprotsesside võimalike viivitustega;
- pilootkasutuse ja katsetuste läbiviimisega;
- kriitiliste etappide juures vajalike ajapuhvritega.

Projekti ajakavas on teadlikult planeeritud järgmised ajapuhvrid riskide maandamiseks:

- hangete võimalik viibimine: kuni +1 kuu;
- riistvara tarne ja seadistuse viibimine: kuni +1 kuu;
- pilootfaasi iteratsioonid ja täiendused: kuni +1 kuu;
- ressursside ja tööde ajastamise risk on maandatud paralleeltegevuste planeerimisega.

Selline ajakava loob piisava paindlikkuse katsetuste läbiviimiseks ning võimaldab reageerida projekti käigus ilmnevatele tehnilistele ja organisatsioonilistele väljakutsetele ilma kogu projekti ajaraami oluliselt ohustamata.

7. Projekti eelarve

Koostage realistlik eelarve detailsusega, mis hõlmab kõiki projekti tegevusi ning võimaldab seeläbi hinnata planeeritud kulude vajalikkust ja mõistlikkust.

- *Arvutage eelarves summad kogumaksumusena (st sisaldavad kõiki makse), sh projektijuhi kogukulu.*
- *Lisage eelarvele kirjeldusena selle kujunemise põhjendused, arvutuste ja hinnangute alused.*
- *Eelarve kogusumma palume esitada 1000 euro täpsusega.*

Kohandage eelarvetabelit oma projekti vajadustele vastavaks.

Tegevused	CR14 kulud	Hankepartner 1 kulud	Hankepartner 2 kulud	Hankepartner 3 kulud	Kulud kokku
I etapp – katseprojekti ettevalmistus ja tehniline disain					
Tehniline arhitektuur ja nõuete täpsustamine	140 000 (2000h)				140 000
II etapp – katsetamiseks vajalik taristu					
AI serverite soetamine		350 000			350 000
Andmesalvestussüsteem/andmemassiiv (objektipõhine salvestus)		300 000			300 000
Serveriruumi rent	20 000				20 000
Sidekulud	12 000				12 000
Elektrikulu	100 000				100 000
III etapp – lahenduste arendus ja katsetamine					
AI treeningkeskkonna arendus (MLOps, LLM)	120 000 (1715)		120 000 (1200h)		240 000
Turvalahenduste arendus ja implementeerimine	120 000 (1715)		40 000 (400h)		160 000
Pilootprojektid (chatbot, arendusabi)	75 000 (1072)		75 000 (750h)		150 000
Välised eksperdid ja sisseostetud teenused			60 000 (600h)		60 000
IV etapp – testimine ja valideerimine					
Testimine ja optimeerimine	40 000 (715h)		40 000 (400h)		80 000
Dokumentatsioon ja raportid	20 000 (286h)	5 000	5 000 (50h)		30 000
Muud kulud					
Litsentsid ja tootetoed				96 000	96 000
Projektijuhtimine					
Projektijuhtimine	90 000 (1285h)				90 000
KOKKU	737 000	655 000	340 000	96 000	**1 828 000 eurot**

Eelarve kujunemise põhjendus

Projekti eelarve on üles ehitatud põhimõttel, et kõik kulud on otseselt seotud katseprojekti läbiviimise, hüpoteeside testimise ja lahenduste valideerimisega. Eelarve ei kata üldisi organisatsioonikulusid ega püsitaristu arendust, vaid keskendub teadlikult realistliku testkeskkonna loomisele ja erinevate lahendussuundade võrdlemisele.

Eelarve loogika lähtub sellest, et kaitsevaldkonna AI lahendusi ei ole võimalik hinnata väikemahulistes või simulatsioonipõhistes keskkondades – vajalik on piisava mahuga infrastruktuur ja reaalse kasutuse lähedased katsetingimused.

1. Personalikulud

Personalikulud katavad ainult neid rolle, mis panustavad otseselt projekti sisusse – arendusse, katsetamisse ja valideerimisse.

- Projekti juht
  - tagab katseprojekti tervikliku juhtimise (etapid, sõltuvused, tulemused)
  - koordineerib erinevaid osapooli (tehniline tiim, partnerid, pilootkasutajad)
  - struktureerib katsetuste tulemused otsustusmaterjaliks
- AI arhitekt (kajastatud disaini ja arenduse kuludes)
  - disainib erinevad arhitektuurilised lahendusvariandid
  - sõnastab ja kontrollib tehnilised hüpoteesid
  - teeb tehnoloogilised valikud ja võrdlused
- MLOps / AI insener (kajastatud arenduse kuludes)
  - ehitab ja opereerib katsekeskkonna (treening, inference, LLM-id)
  - viib läbi mudelite treeningu ja testimise
  - kogub tehnilised mõõdikud (jõudlus, latentsus, kasutus)
- Välised eksperdid
  - pakuvad spetsiifilist kompetentsi (nt turvalisus, LLM optimeerimine)
  - osalevad sõltumatute hinnangute andmisel
  - aitavad valideerida tulemusi rahvusvahelise praktika kontekstis

Personalikulud on seotud konkreetsete katsete ja hüpoteeside elluviimisega, mitte üldise organisatsioonilise tegevusega. Enda ekspertide tunnihind on 70eur/h ning turuküsitlus näitas, et saaksime läbi hanke kaasata eksperte 100 eur/h.

2. Taristukulud

Taristu on katseprojekti kriitiline osa, kuna võimaldab testida lahendusi realistlikes tingimustes.

- AI serverid
  - võimaldavad lokaalselt treenida ja jooksutada AI mudeleid
  - vajalikud jõudluse ja skaleeritavuse hindamiseks
- Andmemassiiv
  - toetab suurte andmekogumite ja mudelite haldamist
  - võimaldab paralleelseid katseid
- Elektrikulu
  - võimaldab mõõta reaalseid opereerimiskulusid
  - oluline sisend edasiste investeeringute hindamiseks
- Serveriruum ja side
  - tagavad turvalise ja töökindla keskkonna

Taristu ei ole käsitletav lõpliku lahendusena, vaid eksperimentaalse keskkonnana katsetuste läbiviimiseks.

3. Arendus ja katsetamine

Projekti keskne kulublokk, mis katab tegelikud katsetused.

- AI treeningkeskkond
  - erinevate arhitektuuride realiseerimine
  - MLOps pipeline'ide loomine ja testimine
- Turvalahendused
  - ligipääsukontroll ja auditilogid
  - andmekaitse mehhanismid
  - turvariskide testimine
- Pilootprojektid
  - dokumentide chatbot
  - AI-toega tarkvaraarendus
  - analüütilised kasutusjuhtumid
- Sisseostetud teenused
  - spetsiifilised katsetused ja analüüsid
  - tehnoloogiate võrdlus
  - valideerimise toetamine

Need kulud võimaldavad kontrollida projekti keskseid hüpoteese:

- kas tsentraalne AI töötab,
- kas lokaalne LLM on piisav,
- kas AI annab reaalset tootlikkuse kasvu.

4. Testimine ja valideerimine

Katseprojekti väärtus tekib just selles etapis.

- Testimine ja optimeerimine
  - jõudlus, latentsus, töökindlus

    - tehniliste lahenduste võrdlus
- Dokumentatsioon ja analüüs
    - tulemuste koondamine
    - järeldused ja soovitused
    - sisend edasiseks rahastuseks

See etapp tagab, et projekt ei lõpe prototüübiga, vaid annab otsustamiseks vajaliku teadmise.

5. Muud otsesed kulud

- Litsentsid
    - vajalikud ainult katsetuste läbiviimiseks
    - ajutised tööriistad ja arenduskomponendid

Eelarve on üles ehitatud nii, et:

- iga kulu toetab konkreetset katset või valideeritavat hüpoteesi,
- infrastruktuur võimaldab realistlikke, mitte teoreetilisi katseid,
- tulemuseks on otsus, milline lahendus töötab ja milline mitte.

See ei ole arendusprojekti ega tootmissüsteemi eelarve, vaid riskide vähendamise ja teadmusloome eelarve, mis võimaldab teha järgmises etapis (2027+) põhjendatud ja kulutõhusaid investeeringuid.

8. Võimalikud lahenduste pakkujad

Tooge välja võimalikud hankepartnerid, kes soovitud lahendussuunas tooteid/ teenuseid/ pakuvad.

- *Otsige ja nimetage võimalikke probleemile lahenduste pakkujaid (nt erinevate valdkondade eksperdid, teadlased, ettevõtted, kes on probleemi lahendamisega varasemalt tegelenud).*

Mõelge nii Eesti kui rahvusvaheliste pakkujate peale.

Projekti elluviimiseks vajalikud lahendused hangitakse tõenäoliselt kombineeritud lähenemisena, kus erinevad turuosalised pakuvad nii terviklahendusi kui ka spetsiifilisi komponente. Realistlikult on oodata, et hankemenetlustes osalevad eelkõige süsteemiintegraatorid ja IT-teenusepakkujad, kellel on võimekus pakkuda "võtmed kätte" lahendusi, hõlmates nii taristut, tarkvara kui ka integratsiooni.

Eesti ja Baltikumi turul on sellisteks pakkujateks näiteks:

- Telia Eesti, Elisa Eesti, Tele2 ICT üksused
- Atea, Santa Monica Networks / Conscia
- ByteLife Solutions

Rahvusvahelisel tasandil võivad hangetes osaleda ka suuremad integraatorid, näiteks:

- T-Systems, Tietoevry
- Accenture, Capgemini
- Atos / Eviden

Need ettevõtted on regulaarselt osalenud avaliku sektori IT hangetes ning omavad kogemust keerukate, turvapoliitikast lähtuvate süsteemide juurutamisel.

Lisaks süsteemiintegraatoritele on oluline roll AI ja tarkvaraarenduse partneritel, kes panustavad konkreetsete lahenduste arendamisse ja kohandamisse (nt AI mudelid, chatbotid, arendusvahendid). Eestis tegutsevad selliste teenuste pakkujatena näiteks MindTitan, AlphaBlues, Nortal, Cybernetica ja Uvik Software, kellel on kogemus nii AI arenduses kui ka riigisektori projektides. Rahvusvahelisel tasandil võivad sarnastes hangetes osaleda ka DataArt, EPAM või SoftServe, kes pakuvad spetsiifilist AI ja andmelahenduste kompetentsi.

Taristu poolel on oodata, et hangetes või alamlepingutena osalevad ka andmekeskuse ja infrastruktuuri teenusepakkujad, kes suudavad tagada turvalise majutuse, elektri ja ühenduvuse. Näidetena võib tuua:

- Telia andmekeskused
- Greenergy Data Centers
- DEAC (Baltikum)

Samuti võivad projekti realiseerimisse olla kaasatud riistvara tarnijad (nt GPU serverid) ja HPC lahenduste pakkujad, kuid nende roll on pigem läbi süsteemiintegraatorite kui otseste hankepakkujatena. Täiendava ekspertiisi kaasamiseks on võimalik teha koostööd ka teadus- ja arendusasutustega (nt TalTech, Tartu Ülikool), eelkõige katsetuste ja valideerimise toetamiseks.

Kokkuvõttes võib eeldada, et turul on olemas piisav konkurents ja kompetents:

- terviklahenduste pakkumiseks süsteemiintegraatorite poolt,

- AI arenduse ja kohandamise teenusteks spetsialiseerunud ettevõtete poolt,
- ning infrastruktuuri tagamiseks andmekeskuse teenusepakkujate poolt.

Selline mitmetasandiline turg loob eeldused konkurentsipõhiste hangete läbiviimiseks ning võimaldab valida projekti jaoks sobivaimad tehnilised ja organisatsioonilised lahendused.

9. Projekti meeskond ja töökorraldus

Tooge välja projekti edukaks elluviimiseks kaasatavad või vajalikud osapooled (asutused ja/või inimesed) ning täiendav ekspertiis, mida meeskonda juurde vajate.

- *Kirjeldage rollide ja töö jaotust projektimeeskonnas.*
- *Kirjeldage projekti juhtimise korraldust.*
- *Märkige ära, kui suure koormusega projektijuht (võimalusel ka teised võtmeisikud) projekti panustavad.*
- *Kirjeldage, missugust täiendavat ekspertiisi tuleb juurde kaasata (nt tehniline ekspertiis, andmekaitse), mis on meeskonnaliikmete poolt katmata.*

NB! Kui nimetate konkreetseid meeskonnaliikmeid, siis nendega (või nende juhtidega) peab olema projektis osalemine läbi räägitud!

Projekti elluviimiseks moodustatakse tuumikmeeskond, millel on vajalik kompetents AI taristu arendamiseks, MLOps praktikate juurutamiseks ning projekti juhtimiseks. Vajadusel kaasatakse täiendavad partnerid ja eksperdid.

Projekti põhimeeskond koosneb järgmistest rollidest:

Projekti juht (1,0 koormus)

Vastutab projekti tervikliku elluviimise eest. Tegemist ei ole administratiivse rolliga, vaid sisulise juhtimisfunktsiooniga.

Peamised ülesanded:

- katseprojekti etappide ja ajakava juhtimine (disain → piloot → valideerimine)
- erinevate osapoolte (tehniline tiim, partnerid, kasutajad) koordineerimine
- katsetuste tulemuste struktureerimine ja järelduste kujundamine
- otsustusmaterjalide ettevalmistamine edasiseks arenduseks

AI arhitekt (1,0 koormus)

Vastutab projekti tehnilise tuuma eest – erinevate lahendussuundade kujundamise ja võrdlemise eest.

Peamised ülesanded:

- erinevate arhitektuuriliste lähenemiste disain (tsentraalne, hajus, hübriid)
- tehniliste hüpoteeside defineerimine ja valideerimine
- tehnoloogiavaliku suunamine (LLM-id, MLOps lahendused)
- lahenduste võrdlus ja analüüs

MLOps / AI insener (1,0 koormus)

Tagab katseprojekti praktilise teostatavuse ja tehnilise töökindluse.

Peamised ülesanded:

- AI treening- ja inference keskkonna loomine ja seadistamine
- mudelite treenimine, fine-tuning ja juurutamine
- LLM lahenduste käitamine ja optimeerimine
- tehniliste mõõdikute (jõudlus, latentsus, kasutus) kogumine

Kõik võtmerollid panustavad projekti täiskoormusega, mis on vajalik, et tagada katsete järjepidevus ja kvaliteet.

Projekti juhtimise korraldus - projekt viiakse ellu tsentraalse juhtimismudeli alusel, kus:

- projekti juht vastutab strateegilise juhtimise ja sidusrühmadega suhtlemise eest,
- tehniline juhtimine on AI arhitekti ja MLOps inseneri koostöös,
- administratiivne tugi tagab sujuva igapäevase toimimise.

Juhtimine põhineb:

- etapiviisilisel lähenemisel (setup → piloot → kasutuselevõtt),
- regulaarsetel töörühmakoosolekutel ja vahetähtaegadel,
- selgetel deliverable'itel iga arendusetapi lõikes.

Täiendav kaasatav ekspertiis on vajalik. Kuigi tuumikmeeskond katab peamised tehnilised ja juhtimisvajadused, kaasatakse projekti raames täiendavat ekspertiisi. CR14-siseselt panustavad projekti AIDA projekti meeskond, kellel on varasem kogemus tehisintellekti lahenduste arendamisel ja rakendamisel rahvusvahelises kaitsekoostöös, samuti CR14 infrastruktuuriinsenerid, kes tagavad katsekeskkonna tehnilise toimivuse ja töökindluse. Lisaks on oluline roll CR14 juhtkonnal, kes panustab strateegiliste valikute tegemisse ning tagab projekti tulemuste seotuse organisatsiooni pikaajaliste arendusprioriteetidega.
Riigi tasandi ekspertiisi kaasatakse läbi Kaitseministeeriumi valitsemisala esindajate, sealhulgas innovatsiooni valdkonna juhi ja AI eksperdi, kes annavad sisendi strateegilise suuna, kasutusjuhtumite ning nõuete kujundamisse. Täiendavalt panustab Tulevikuvõime ja innovatsiooni väejuhatuse AI valdkonna ekspert, kes aitab hinnata lahenduste sobivust kaitseoperatsioonide ning tulevikuvõime arendamise kontekstis, tagades seeläbi, et katsetatavad lahendused vastavad reaalsele operatiivvajadusele.
Töökorralduse põhimõtted:

- Iteratiivne arendus (piloot → testimine → laiendamine)
- Tihe koostöö lõppkasutajatega (KM VA ja partnerid)
- Standardiseeritud MLOps praktikad (reprodutseeritavus, versioonihaldus, monitooring)
- Selge vastutusjaotus tehnilise ja juhtimise tasandi vahel

10. Projekti tulemuste elluviimine

Kirjeldage oma valmisolekut ja võimekust pärast katseprojekti edukat lõppu projekti tulemusi kestlikult ellu viia.

.

- *Kas projekti tulemuste edasine arendus ja kasutuselevõtt seostub asutuse prioriteetsete tegevustega, on tööplaanis vms?*
- *Kas tulemuste hilisemaks elluviimiseks vajalik rahastus ja muud ressursid on olemas või tegeletakse selle leidmisega?*
- *Tooge välja olulisemad riskid projekti tulemuste hilisemal kasutuselevõtul. Kuidas plaanite neid riske maandada?*
- *Kirjeldage, kas ja mil määral on tulemused skaleeritavad ning kasutatavad avalikus sektoris laiemalt.*

CR14 käsitleb käesolevat projekti osana mitmeaastasest võimearendusprogrammist, mille eesmärk on kujundada kaitsevaldkonnas toimiv ja jätkusuutlik tehisintellekti rakendamise mudel. Innofondi taotlus katab programmi katse- ja käivitamisfaasi, mille käigus valideeritakse nii tehniline keskkond kui ka sellega seotud tehnoloogilised ja organisatsioonilised toimemudelid. Projekti tulemusena luuakse ja hinnatakse AI lahenduste arendamist ja kasutamist toetav katsekeskkond (sh treening- ja LLM-võimekus) ning selle põhjal kujundatakse arhitektuurilised valikud, kasutusmudelid ja kuluhinnangud, mis loovad aluse edasisteks otsusteks ja suuremahulisteks investeeringuteks. Seos asutuse prioriteetsete tegevustega.
Projekti tulemused on otseselt seotud:

- Kaitseministeeriumi valitsemisala AI strateegia rakendamisega,
- CR14 põhitegevustega (küberkaitse, õppused, analüüs),
- rahvusvaheliste koostööprojektide (nt EDF, NATO) AI fookusega.

Katseprojekti käigus valideeritud lahendused viiakse järk-järgult kasutusse:

- otsustustoe ja analüütika töövahenditena,
- õppuste ja simulatsioonide osana,
- tarkvaraarenduse toetamiseks.

Seeläbi ei ole tegemist eraldiseisva arendusega, vaid sisendiga CR14 ja KM valitsemisala strateegiliste tegevuste elluviimiseks. CR14 plaanib tugineda katseprojekti tulemustele ning taotleda täiendavat rahastust KMAK lisataotluse kaudu 2026. aasta lõpus.
Projekti jätkusuutlikkus põhineb etapilisel rahastusmudelil:

- 2026 (Innofond – katsefaas):
  - prototüübid ja piloodid,
  - tehniliste valikute valideerimine,
  - kompetentsi kujundamine.
- 2027–2030 (planeeritav KMAK lisataotlus):
  - valideeritud lahenduste edasiarendus,

- taristu laiendamine ja opereerimine,
- püsikulude katmine (andmekeskus, hooldus),
- spetsialistide kaasamine.

Lisaks kasutatakse:

- olemasolevaid CR14 ressursse,
- EDF ja rahvusvaheliste projektide sünergiat,
- partnerite kaasamist (nii tehniline kui sisuline panus).

Olulisemad riskid on esitatud tabelina:

Risk	Tõenäosus	Mõju	Olulisus	Maandamismeetmed
Edasise rahastuse ebakindlus	Keskmine	Kõrge	Kõrge	Varajane KMAK taotluse ettevalmistus; tugeva äriloogika ja tulemuste esitamine; sidumine strateegiliste eesmärkidega
Valideeritud lahenduse mitte-ülekantavus operatiivkasutusse	Keskmine	Kõrge	Kõrge	Pilootide läbiviimine reaalses keskkonnas; kasutajate varajane kaasamine; iteratiivne arendus
Võimekuse alakasutamine	Keskmine	Keskmine–kõrge	Keskmine–kõrge	Selged kasutusstsenaariumid; õppuste ja projektide integreerimine; teenuspõhine pakkumine
Kompetentsi jätkusuutmatus	Keskmine	Keskmine	Keskmine	Püsivate rollide planeerimine; koostöö ülikoolide ja partneritega; teadmussiirde mehhanismid
Tehnoloogia kiire muutumine	Kõrge	Keskmine	Keskmine	Modulaarne arhitektuur; open-source komponentide kasutamine; pidevuuendamine

Projekti tulemused on kavandatud kõrge skaleeritavusega, kuid skaleerimisotsused tehakse katseprojekti tulemuste põhjal.

Tehniline skaleeritavus:

- GPU taristut saab laiendada vastavalt vajadusele,
- lahendus toetab mitme kasutaja ja organisatsiooni samaaegset kasutust,
- arhitektuur on modulaarne ja laiendatav.

Organisatsiooniline skaleeritavus:

- lahendusi saab rakendada kogu KM valitsemisalas,
- potentsiaal laiendada teistele avaliku sektori valdkondadele (nt sisejulgeolek),
- võimaldab AI võimekuse pakkumist jagatud teenusena.

Rahvusvaheline mõõde:

- lahendusi saab kasutada rahvusvahelistes projektides ja õppustel,
- toetab Eesti rolli kaitsetehnoloogia ja AI koostöövõrgustikes.

11. Mõju ettevõtlusele

☒ Projekt omab positiivset mõju innovatsioonile ettevõtlussektoris. Kõige otsesemalt väljendub mõju läbi ettevõtete, kes osalevad tegevuste elluviimiseks korraldatavatel hangetel ja/või konkurssidel. Innovatsiooni hankimine avaliku sektori poolt aitab kaasa innovatsioonitegevuste kasvule erasektoris.

12. Seos nutika spetsialiseerumise valdkondadega

- *Eesti teadus- ja arendustegevuse, innovatsiooni ning ettevõtluse (TAIE) arengukaval 2021-2035 on fookusvaldkonnad, s.o Eesti arenguvajadustele ja -võimalustele vastavad riigi, ettevõtete ja teadusasutuste koostöös eelisarendatavad teadus- ja arendustegevuse, innovatsiooni ja ettevõtluse valdkonnad. Ettevõtluse ja majanduslikU arengupotentsiaaliga TAIE fookusvaldkonnad on ühtlasi Eesti nutika spetsialiseerumise valdkonnad (täpsem info: https://www.hm.ee/korgharidus-ja-teadus/teadus-ja-arendustegevus/taie-fookusvaldkonnad).*
- *Kirjeldage teie projekti võimalikU lahenduse seost vähemalt ühe valdkonnaga (rõhuasetusega teadmus- ja tehnoloogiasiirdel).*

Digilahendused igas eluvaldkonnas (vt teekaarti)	Projekt panustab sellesse valdkonda läbi tehisintellekti (AI) ja masinõppe võimekuse arendamise ja rakendamise kõrge turvanõudlusega keskkondades, eelkõige kaitse- ja julgeolekuvaldkonnas. Loodav lahendus hõlmab: • AI mudelite treenimise ja juurutamise taristut, • organisatsioonisisest AI-juturoboti lahendust, • tarkvaraarendust toetavat AI keskkonda, mis kokku moodustavad tervikliku digitaalse platvormi otsustustoe, analüütika ja arendustegevuse automatiseerimiseks. Projekti keskne väärtus seisneb teadmus- ja tehnoloogiasiirde kiirendamises järgmistel telgedel: 1. Akadeemia → rakendus • AI ja masinõppe teadustulemuste (mudelid, algoritmid, meetodid) rakendamine reaalses kaitsevaldkonna keskkonnas; • koostöö ülikoolidega (TalTech, Tartu Ülikool) uute lahenduste piloteerimiseks. 2. Rahvusvaheline → riiklik võimekus • rahvusvaheliste arendusprojektide (nt EDF, NATO) tulemuste toomine Eestisse praktilisse kasutusse; • globaalselt arendatud open-source AI mudelite kohandamine riigikaitse vajadustele. 3. Era- ja avalik sektor • Eesti AI ettevõtete (nt ML, chatbot, analüütika) kompetentsi sidumine riigikaitse vajadustega; • ühise AI taristu pakkumine partneritele (“shared capability”), mis vähendab dubleerimist ja kiirendab innovatsiooni. Projekt loob Eestis uue tüüpi võimekuse: • turvaline ja autonoomne AI arenduskeskkond, mida saab kasutada tundlike andmetega • AI kui jagatud infrastruktuur (AI-as-a-capability), mis on skaleeritav erinevatele organisatsioonidele • praktiline sild teadusarenduse ja operatiivse kasutuse vahel Selline lähenemine aitab lahendada ühe peamise kitsaskoha digilahenduste arengus – kuidas viia kiiresti arenevad AI tehnoloogiad turvaliselt ja efektiivselt reaalsesse kasutusse valdkondades, kus pilvelahendused ei ole sobivad. Laiem mõju - kuigi projekti esmane fookus on kaitsevaldkond, on loodav võimekus: • laiendatav teistesse avaliku sektori valdkondadesse (nt sisejulgeolek, kriisijuhtimine); • rakendatav olukordades, kus on vajalik: ○ tundlike andmete töötlemine; ○ autonoomne AI võimekus; ○ kõrge töökindlus ka piiratud ühenduvusega keskkondades;
Tervisetehnoloogiad ja -teenused (vt teekaart)	-
Kohalike ressursside (toit, puit, maapõueressursid, teisene toorme ja jäätmed) väärindamine (vt teekaart)	-

Nutikad ja kestlikud energialahendused (vt teekaart)	-

13. Seos strateegias Eesti 2035 toodud arenguvajadustega

- *Selgitage, kuidas panustavad projekti tegevused ja valitud lahendussuund "Eesti 2035" strateegias kirjeldatud arenguvajadustesse.*
- *Tooge välja, kui projekti tegevused panustavad muudesse olulistesse valdkondlikesse arengukavadesse või -dokumentidesse.*

Käesolev projekt panustab otseselt strateegias „Eesti 2035" välja toodud arenguvajadustesse, eelkõige digivõimekuse, julgeoleku, majanduse konkurentsivõime ja riigi tehnoloogilise autonoomia tugevdamise kaudu.

1. Digiriigi ja tehnoloogilise võimekuse arendamine – „Eesti 2035" seab eesmärgiks arendada Eestit kui tipptasemel digiriiki, kus kasutatakse laialdaselt andmeid ja uusi tehnoloogiaid.
Projekt panustab sellesse läbi:
- tehisintellekti süsteemide süsteemse rakendamise riigikaitses,
- andmepõhiste otsustustööriistade loomise,
- kaasaegse AI infrastruktuuri arendamise, mis võimaldab luua ja kasutada tipptasemel digilahendusi.

Loodav AI treening- ja kasutuskeskkond aitab viia Eesti digiriigi järgmisele tasemele, kus:
- AI ei ole üksikrakendus, vaid strateegiline baasvõimekus,
- riik suudab ise arendada ja hallata kriitilisi tehnoloogiaid.

2. Julgeoleku ja riigikaitse tugevdamine – „Eesti 2035" rõhutab tugeva ja kohanemisvõimelise riigi olulisust, kus julgeolek on tagatud ka kiiresti muutuvas tehnoloogilises keskkonnas.
Projekt toetab seda läbi:
- autonoomse AI võimekuse loomise, mis töötab ka piiratud või katkestatud ühenduvusega keskkondades,
- otsustustoe kiirendamise ja automatiseerimise,
- võimekuse hinnata ja testida AI süsteemide usaldusväärsust kaitsevaldkonnas.

See aitab tagada, et Eesti:
- ei sõltu kriitilistes valdkondades välisteenustest,
- suudab rakendada AI-d turvaliselt ja kontrollitult ka kriisiolukordades.

3. Majanduse konkurentsivõime ja innovatsiooni kasv – Strateegia rõhutab vajadust suurendada Eesti kõrgtehnoloogilist võimekust ja innovatsioonivõimet.
Projekt panustab sellesse läbi:
- AI arenduse infrastruktuuri loomise, mida saavad kasutada ka partnerid ja ettevõtted,
- teadmus- ja tehnoloogiasiirde kiirendamise avaliku ja erasektori vahel,
- Eesti positsiooni tugevdamise Euroopa kaitsetööstuse ja AI ökosüsteemis.

Lahendus loob eelduse:
- uute AI-põhiste toodete ja teenuste tekkeks,
- Eesti ettevõtete suuremaks rolliks rahvusvahelistes arendusprojektides.

4. Riigi toimimise tõhusus ja andmepõhisus – „Eesti 2035" eesmärk on suurendada riigi otsustusprotsesside tõhusust ja kvaliteeti läbi andmete kasutamise.
Projekt toetab seda:
- AI-põhise otsustustoe loomisega,
- dokumentidel põhineva teadmushalduse automatiseerimisega (AI chatbot),
- töövoogude ja analüüsiprotsesside kiirendamisega.

See aitab:
- vähendada ajakulu ja käsitööd,
- parandada otsuste kvaliteeti ja kiirust.

Seos teiste oluliste arengukavade ja strateegiatega – lisaks „Eesti 2035" strateegiale panustab projekt otseselt järgmiste dokumentide elluviimisesse:
1. Kaitseministeeriumi AI strateegia

Projekt on otsene tööriist selle strateegia elluviimiseks, võimaldades:

- AI võimekuse praktilist rakendamist,
- turvalise ja autonoomse arendus- ja kasutuskeskkonna loomist,
- strateegiliste eesmärkide saavutamist (nt otsustustugi, automatiseerimine, situatsiooniteadlikkus).

2. Riigikaitse arengukava (RKAK 2022–2031)
Projekt toetab RKAK eesmärke:

- tehnoloogilise ülekaalu saavutamine,
- luure- ja eelhoiatusvõime tugevdamine,
- digitaalse riigikaitse arendamine.

AI võimekus loob uusi võimalusi:

- andmete analüüsiks,
- operatiivseks planeerimiseks,
- õppuste realismi ja kvaliteedi tõstmiseks.

3. TAIE arengukava 2021–2035
Projekt toetab:

- digilahenduste arendamist,
- teadmus- ja tehnoloogiasiiret,
- koostööd riigi, teadusasutuste ja ettevõtete vahel.

4. Euroopa tasandi algatused (nt EDF, NATO koostöö)
Projekt loob eelduse:

- Eesti aktiivseks osalemiseks rahvusvahelistes AI projektides,
- partneritele reaalse tehnilise võimekuse pakkumiseks,
- Eesti nähtavuse ja usaldusväärsuse kasvuks.

14. Avalike ülesannete täitmine projekti elluviimisel

- *Selgitada ning tuua välja seosed ja viited, missuguse seaduse, määruse, haldusakti või lepingu alusel täidab ideekavandi esitaja asutus innovatsiooniprojekti ellu viies avalikke ülesandeid.*
- *Kui ideekavandi esitaja on **MTÜ**, siis selgitada, kuidas ta pakub otsest avalikku teenust (loe Teenuste korraldamise ja teabehalduse alused–Riigi Teataja, §2 lg2).*

CR14 täidab projekti elluviimisel avalikke ülesandeid tulenevalt oma rollist riigikaitse ja küberkaitse võimekuse arendamisel ning toetamisel. Vastavalt Sihtasutus CR14 põhikirjale(§ 2.1 ja § 2.2) on asutuse eesmärgiks küberjulgeoleku alane teadus- ja arendustegevus, selle toetamine ning vastavate tehnoloogiate arendamine ja rakendamine, sealhulgas kahese kasutusega tehnoloogiate valdkonnas. [cr14.ee] Projekti raames arendatav ja katsetatav tehisintellekti võimekus on otseselt seotud nimetatud ülesannetega, panustades riigi küberkaitse ja digitaalse kaitsevõime tugevdamisse.
Projekt on otseselt seotud:

- Riigikaitseseadusest ja riigikaitse korraldamise põhimõtetest tulenevate ülesannetega, mille kohaselt arendatakse riigi kaitsevõimet ja tagatakse valmisolek kriisideks,
- Kaitseministeeriumi valitsemisala arengukavadest ja strateegiatest (sh AI strateegia ja RKAK), mille alusel CR14 panustab tehnoloogilise kaitsevõime arendamisse,
- halduslepingutest ja koostööprojektidest (nt rahvusvahelised õppused ja EDF projektid), mille kaudu CR14 viib ellu riigikaitselisi arendus- ja koostöötegevusi.

Projekti raames loodav AI võimekus toetab:

- küberkaitse õppuste ja riigikaitseliste tegevuste läbiviimist,
- otsustustoe ja analüüsivõimekuse arendamist,
- riigi kriitilise tehnoloogilise autonoomia tagamist.

Seetõttu on tegemist otseselt avaliku ülesande täitmisega, mis väljendub riigikaitse ja julgeoleku tagamises ning arendamises läbi uute tehnoloogiliste lahenduste.

15. Rahastus mitmest allikast

- *Kas probleemi lahendamiseks või planeeritud lahenduse katsetamiseks on taotletud või taotletakse toetust teistest rahastamisallikatest?*

- *Kui jah, siis tuua välja rahastusallikas, summa ja tegevused ning kas toetus on taotlemisel või projekt on saanud rahastusotsuse.*

Projekti ettevalmistamise käigus on hinnatud täiendavaid rahastusvõimalusi.

- 2025. aasta lõpus esitati taotlus Kaitseministeeriumi KMAK lisataotluse raames, eesmärgiga käivitada ja arendada AI võimekust.
  - Tulemus: rahastust ei eraldatud.
  - Taotletud tegevused: AI taristu rajamine, GPU-võimekuse loomine ning AI arendus- ja kasutuskeskkonna käivitamine.
- Käesoleval hetkel teistest rahastusallikatest toetust taotletud ei ole.
- Projekti jätkusuutlikkuse tagamiseks on plaan:
  - esitada uus taotlus KMAK lisataotluse kaudu 2026. aasta lõpus,
  - eesmärgiga saada rahastus projekti järgmisteks etappideks (kuni 3 aastaks), sh taristu laiendamiseks, püsikulude katmiseks ja võimekuse operatiivseks kasutamiseks.

Kokkuvõttes toimib Innofondi taotlus projekti käivitamisfaasi rahastusena, millele on kavandatud jätk rahastuse kaudu riigikaitse eelarvelistest vahenditest. Käesoleva projekti raames kavandatud tegevuste jaoks ei ole taotletud ega taotleta paralleelselt rahastust teistest allikatest ning topeltrahastust ei esine.

Kinnitused

☒ Oleme teadlikud, et Riigikantselei võib saata ideekavandi eksperthinnangu saamiseks valdkonna ekspertidele.

☐ Kinnitan, et esitatud innovatsiooniprojekt on teiste partnerite juhtkondadega kirjalikult kooskõlastatud.

Allkirjastamine

- Ideekavand tuleb allkirjastada projekti esitava(te) asutus(t)e allkirjaõigusliku juhtkonnaliikme poolt (nt kantsler, asekantsler, KOVi juht, KOVi volikogu esimees, ministeeriumi allasutuse juht/asejuht vms) ja saata riigikantselei@riigikantselei.ee.

---

[i] **Katsetamine** vastab küsimusele: *kas see töötab? Katsetuse puhul ei vaadata alati, kas lahendus praktiliselt toimib.*

Piloteerimine vastab küsimusele: *kas see töötab päriselus ja on mõistlik kasutusele võtta? Hinnata praktilist toimivust.*

Eksperiment: *Igasuguse eksperimendi eesmärk on kontrollida hüpoteese* ***põhjuslike seoste*** *kohta. Eksperiment on selline katse, mis on kavandatud põhjuslike seletusteni jõudmiseks: kui teeme x siis juhtub y.*

Prototüüp *on masina, seadme või mingi rakenduse esialgne teostus, algne mudel, mida edasi arendatakse.*