



KAITSEMINISTEERIUM

KAITSEMINISTEERIUMI VALITSEMISALA TEHISINTELLEKTI STRATEEGIA

Tallinn 2025

SISUKORD

KOKKUVÕTE	3
1. SISSEJUHATUS	4
1.1 Tehisintellekti mõiste	5
2. HETKEOLUKORD	6
2.1 Maailm, Euroopa Liit, NATO ja liitlased	6
2.2 Venemaa	7
2.3 Eesti	8
3. TEHISINTELLEKTI RAKENDAMINE KAITSEVALDKONNAS	9
3.1 Eesmärgid	9
3.2 Eesmärkide saavutamise viisid	10
3.3 Eesmärkide saavutamiseks vajalikud ressursid	11
3.4 Eetilised ja juriidilised põhimõtted ja piirangud kaitsevaldkonna tehisintellekti arendamisel ja rakendamisel	11
4. RAKENDUSKAVA	12

KOKKUVÕTE

Käesoleva Eesti esmase kaitsevaldkonna tehisintellekti arengustrateegia põhieesmärk on anda suunised kaitsealase tehisintellekti arendamiseks, määratledes selle tegevuse eesmärgid ning teostamise raamistiku.

Tehisintellekti rakendamine Kaitseministeeriumi valitsemisalas peab olema praktilise väärtusega ja suurendama Eesti kaitsevõimet, olles suunatud järgnevate eesmärkide saavutamisele:

- (1) **otsete sõjaliste eeliste loomine** otsuselangetamise toetamise, luureinfo töötlemise ja sihtmärgistamise kiirendamise kaudu;
- (2) **tugiteenuste ja logistika efektiivsemaks muutmine** kiirema ja täpsema analüüsivõime ning administratiivsete kohustuste vähendamise kaudu;
- (3) **kohaliku kaitsetööstuse tugevdamine**, kasutades ära kaitsealase tehisintellekti arendamisest ja rakendamisest tulenevaid koostöövõimalusi Kaitseväe ja kaitsetööstuse vahel.

Püstitatud eesmärkide täitmine eeldab selget valitsemisala ülest arusaama, kuidas hakkab Kaitsevägi tehisintellekti rakendamise abil paremini sõdima ja ülejäänud valitsemisala allasutused Kaitseväe tegevust toetama. Selle saavutamiseks vajalikud tegevused on jagatud viide kategooriasse:

- (1) **Kaitseväe digitaalse ja tehnoloogilise arengu eest vastutava struktuuriüksuse loomine:** Kaitseväe Peastaabi võimaliku reformi raames kaalutakse vastutava isiku ametisse määramist, soovitatavalt soovitatavalt Kaitseväe innovatsioonijuht (*Chief Innovation Officer*) ja/või digitaliseerimise juht (*Chief Digitalisation Officer*), kellel on pädevus, volitused ja kindel eelarve valitsemisala tehnoloogilisi, sh tehisintellekti-alaseid arenguid terviklikult suunata ja prioriseerida.
- (2) **Kaitseväe digitaalse infotaristu loomine:** kavandatakse ja ehitatakse üles Kaitseväe digitaalne infotaristu, et tehisintellekti süstemaatiliselt rakendada. Lisaks luuakse Kaitseministeeriumi valitsemisala ülene andmehalduse kontseptsioon ja vajalikud standardid.
- (3) **Kaitseväe kõrgtehnoloogilise teadlikkuse ja tehisintellektiga seonduvate oskuste arendamine:** uuendatakse Kaitseväe Akadeemia õppekavasid ja toetatakse kaitsevaldkonna tehisintellekti-alaseid õpinguid, et tagada valitsemisalale piisav hulk vajalikke kompetentse omavaid spetsialiste.
- (4) **Koostöö tsiviilstruktuuridega kaitsevaldkonna tehisintellekti arengu toetamiseks:** tugevdatakse koostööd erasektori ning kõrgharidus- ja teadusasutustega, et rakendada võimalikult optimaalselt olemasolevat tehnoloogiliselt pädevat inimressurssi.
- (5) **Rahvusvahelistes võrgustikes osalemine ja liitlastega koostalitlusvõime tagamine:** määratakse kindlaks rahvusvahelise koostöö eesmärgid ja prioriteedid, et tagada kaitsevaldkonna tehisintellekti areng, säilitades ja tugevdades koostalitlusvõimet NATO liitlastega.

Vaadates tulevikku, peab Kaitseministeeriumi valitsemisala ülaltoodud tegevuste elluviimise tulemusena jõudma olukorda, kus 2030. aastal toimub kaitsevaldkonna tehisintellekti areng tasemel, mille abil on võimalik tagada:

- vajalik eelhoiatustase ja nõutav otsuselangetamise kiirus kõigis sõjapidamise domeenides ja

- tasanditel;
- adekvaatne koostöövõime pidevalt arenevate liitlasvägede võimetega kõigis võtmetähtsusega valdkondades;
- kaitsevaldkonna tehisintellekti areng, tuginedes maksimaalselt tsiviilvõimetele ja –struktuuridele ning riigikaitse laiale käsitlusele;
- kaitsevaldkonna tehisintellekti arendamine koostöös Eesti kaitsetööstuse ja NATO liitlastega;
- kaitsevaldkonna tehisintellekti arendusprojektide jätkusuutlik ajakohastamine ja edasiarendamine.

Strateegia elluviimist täiendab regulaarselt, aga vähemalt kord aastas uuendatav rakenduskava, mille täitmise kaudu jõuab kaitseministeeriumi valitsemisala 2030. aastaks tehisintellekti süsteemse rakendamise võimeni. Arvestades tehisintellekti arengu kiirust, vaadatakse käesolev strateegia ja püstitatud eesmärgid üle vähemalt iga kahe aasta järel.

1. SISSEJUHATUS

Tänu arvutusvõimsuse eksponentsiaalsele kasvule on tehisintellekti süsteemide õppimis- ja kohanemisvõime viimastel aastatel oluliselt kasvanud, pälvides sellega ühiskonnas suurt tähelepanu ja tuues kaasa tehisintellekti rakenduste arvu kiire kasvu. Tehisintellekti plahvatuslik areng kannab endas potentsiaali muuta inimkonna arengut samal määral kui seda tegi tööstusrevolutsioon, mis muutis riikide jõu struktuuri, riikidevahelist jõutasakaalu kujundavaid faktoreid ning võimaldas riikidel seada endale uusi ja varem kättesaamatuid eesmärke. On selge, et tehisintellekti jõuline areng puudutab kaitsevaldkonda väga sügavalt ning nende arengutega kaasas käimine on äärmiselt oluline nii riigi üldise arengu kui Eesti Vabariigi sõjalise julgeoleku tagamise seisukohast.

2022. aasta veebruaris alanud Venemaa täiemahulises sissetungis Ukrainasse põhjustavad suure osa Ukraina kaotustest jätkuvalt traditsioonilised relvasüsteemid (eelkõige kaudtulevahendid). Sellest tulenevalt on ka Eesti võimearenduse peamiseks prioriteediks täiendavate relvasüsteemide hankimine koos piisava koguse laskemoonaga, mis võimaldab mõjutada vastast piisavalt distantsilt ning kaitsta riiki ja Kaitseväge vastase mõjutuste eest. Seda peegeldab Kaitseministeeriumi valitsemisala [2025–2028 arengukava](#), mille 5,3 miljardi eurosest kogumahust investeeritakse 1,55 miljardit eurot laskemoona.

Teisest küljest, suurt tulejõudu peab toetama kiire ja täpne sihtmärgistamine ning võime langetada õigeaegseid ja adekvaatseid otsuseid. Tehisintellekti plahvatuslik areng on kaasa toonud kognitiivsete töövahendite kiire arengu ja rakendamise sõjanduses, mis on suurendanud sõjapidamise kiirust ja autonoomsete relvasüsteemide hulka lahinguväljal. Ukrainas ja Gazas toimuvates sõjalistes konfliktides on tehisintellekt leidnud rakendamist peamiselt otsuselangetamise toetamisel, luureinfo töötlemisel ja sihtmärgistamisel. Ukraina saavutused muudab eriti muljetavaldavaks sõjapidamise doktriini muutuste kiirus ning ukrainlaste võime sõja ajal arendada ja efektiivselt kasutusele võtta ridamisi tehisintellektiga varustatud süsteeme, sh erinevaid sensoreid, relvasüsteeme ja üksusi ühendav interaktiivne olukorrateadlikkuse süsteem [Delta](#) ning sensorite kogutud lahingupilti analüüsiv lahendus [Avengers](#). Lisaks on õhukaitse süsteemidesse integreeritud tehisintellekt on võimaldanud tõrjuda raketirünnakuid, mille käigus on vastane kasutanud üheaegselt nii ballistilisi kui tiibrakette.

Arvestades Eesti territooriumi väiksust ja sõjaliseks riigikaitseks kasutada olevate ressursside piiratust, on tehnoloogiliste lahenduste rakendamine riigikaitse sarnaselt Ukrainaga Eesti jaoks elutähtis. Tehisintellekti ja autonoomsete süsteemide koostoime ning efektiivne kasutamine on üks Eestile kättesaadavastest

võimalustest vastase suurusele vaatamata endale asümmeetrilisi ja kuluefektiivseid eeliseid luua. Uusi tehnoloogiaid targalt ja süsteemselt kasutades tõstame me enda heidutus- ja lahinguvõimet ning lükkame edasi või paremal juhul hoiaime ära kallaletungi Eestile.

Käesoleva strateegia koostamises osalesid lisaks Kaitseministeeriumile ka Kaitseväe (Küberväejuhatuse, Luurekeskus, Kaitseväe Akadeemia), Kaitsealiidu, Välisluureameti, NATO küberkaitse koostöökeskuse ja riikliku sihtasutuse CR14 esindajad. Valitsemisala väliselt toimusid konsultatsioonid Välisministeeriumi, Siseministeeriumi, Majandus- ja Kommunikatsiooniministeeriumi, Justiitsministeeriumi ning Riigikantseleiga. Strateegia koostamisel on arvestatud ka Eesti kaitsetööstussektori ettepanekutega.

Strateegias püstitatud eesmärkide ja eelduste täitmiseni jõutakse järgmises riigikaitse arengukavas (2026-2035) tagatud ressursside toel. Käesolev strateegia arvestab ka järgmiste valdkondlikku arengut koordineerivate dokumentidega:

- [Eesti julgeolekupoliitika alused](#)
- [Kaitseministeeriumi valitsemisala teadus- ja innovatsioonipoliitika](#)
- [Kaitsetööstuspoliitika](#)
- [MKMi avalikustatud tehisintellekti tegevuskava 2024–2026](#)
- [Eesti Vabariigi Valitsuse koalitsioonilepe: Eesti Reformierakonna, Erakonna Eesti 200 ja Sotsiaaldemokraatliku Erakonna valitsusliidu uuendatud tegevusplaan aastateks 2024–2027](#)
- [NATO tehisintellekti strateegia](#)
- [NATO Teadus- ja Tehnoloogiaorganisatsiooni \(STO\) 2020–2040 trendide raport](#)
- [NATO Teadus- ja Tehnoloogiaorganisatsiooni \(STO\) 2023–2043 trendide raport](#)

1.1 Tehisintellekti mõiste

Kuigi tehisintellekt on viimastel aastatel pöördeliselt edasi arenenud, kasutati tehisintellekti mõistet esimest korda juba 1950. aastate keskel. Ka sõjapidamises ei ole tehisintellekti rakendamine midagi uut; näiteks Ameerika Ühendriikide kaitseministeeriumi 2023. aasta novembris avalikustatud [andmete, analüüsi ja tehisintellekti kasutuselevõtu strateegia](#) kohaselt on andme- ja tehisintellektipõhiseid süsteeme arendatud ja sõjapidamises rakendatud juba üle 60 aasta.

NATO Teadus- ja Tehnoloogiaorganisatsiooni (STO) [2020–2040 trendide raport](#) käsitleb tehisintellekti kui masinate võimet täita ülesandeid, mille täitmine eeldab tavaliselt inimhõimust; näiteks mustrite äratundmine, kogemustest õppimine, järelduste tegemine, prognoosimine või tegutsemine – kas digitaalselt või autonoomsetes füüsilistes süsteemides toimiva tarkvarana.

STO [2023–2043 trendide raport](#) laiendab tehisintellekti definitsiooni, käsitledes neid süsteemidena, mis näitavad üles intelligentset käitumist, analüüsivad oma keskkonda ja tegutsevad teatud määral iseseisvalt konkreetsete eesmärkide saavutamiseks. Tehisintellektipõhised süsteemid võivad olla puhtalt tarkvarapõhised, tegutsedes virtuaalses maailmas (nt hääluhitavad assistendid, pildianalüüsi tarkvara, otsingumootorid, kõne- ja näotuvastussüsteemid). Teise võimalusena võib tehisintellekt olla integreeritud riistvarasse (nt kõrgtehnoloogilised robotid, autonoomsed autod, droonid või asjade Interneti rakendused).

Erinevalt automatiseerimisest, mille puhul täidetakse konkreetseid ülesandeid eelnevalt määratletult reeglitest lähtuvalt, on tehisintellektil põhinevad süsteemid võimelised õppima ja uute olukordadega autonoomselt vähemal või rohkemal määral kohanema.

2. HETKEOLUKORD

2.1 Maailm, Euroopa Liit, NATO ja liitlased

Tehisintellekti kiire arengu ja üha kasvava mõju tõttu ühiskonnale teevad nii riigid kui rahvusvahelised organisatsioonid aktiivselt jõupingutusi tehisintellekti rakendamise võimaluste kaardistamiseks ja sellega seonduvate väljakutsete lahendamiseks. 2024. aasta Stanfordi ülikooli avalikustatud tehisintellekti [raporti](#) sõnul on maailmas 75 riiki, kes on koostanud oma rahvuslikud tehisintellekti arengustrateegiad.

Tehisintellekti jõuline areng on loonud ka vajaduse seda seadusandluse tasemel reguleerida. 2021. aastal esitles Euroopa Komisjon Euroopa Liidu [tehisintellekti määrust](#), mida hakatakse täies ulatuses liikmesriikidele, sh Eestile, kohaldama 2026. aasta suvest. Kuigi ka ELi mittekuuluvad riigid on tehisintellekti reguleerivat seadusandlust arendamas, saab ELi määrust lugeda maailmas kõige ulatuslikumaks ja ambitsioonikamaks.

Käesoleva strateegia valguses on võtmetähtsusega, et ELi määrus ei kohandu tehisintellekti süsteemidele, mida kasutatakse üksnes riigikaitsealistel või julgeoleku tagamise eesmärkidel, olenemata sellest, kas neid eesmärke viib ellu avaliku või erasektori organisatsioon. Kuigi tagatud erand on kaitsevaldkonna tehisintellekti arendamiseks möödapääsmatu, tõstatab lääneriikide soov tehisintellekti tugevalt reguleerida ja eetiliselt kasutada küsimuse, kuidas selliste piirangute tingimustes tagada tehisintellekti kaitsealaste rakenduste piisav efektiivsus ning mitte alla jääda tehnoloogilises konkurentsivõitluses tunduvat väiksemate piirangute tingimustes sõjalist tehisintellekti arendavate Venemaa ja Hiinaga.

NATO avalikustas 2021. aasta oktoobris [esimese tehisintellekti strateegia](#), mille laiem eesmärk oli tehisintellekti rakendamise kaudu kindlustada alliansi tehnoloogilise eelise säilitamine ning kollektiivse julgeoleku tagamine kiirelt muutavas julgeolekukeskkonnas. NATO Teadus- ja Tehnoloogiaorganisatsiooni avalikustatud [2023–2043 trendide raport](#) käsitleb tehisintellekti ühena võtmetähtsusega tehnoloogiatest, mis mõjutab NATO operatsioone ja võimeid väga suurel määral.

2024. aasta Washingtoni tippkohtumisel tutvustati tehisintellekti strateegia [uut versiooni](#), millel on neli peamist eesmärki:

- (1) luua NATOle ja liitlastele alus eeskuju näitamiseks ning julgustada tehisintellekti vastutustundlikku arendamist ja kasutamist kollektiivse kaitse- ja julgeolekueesmärkidel;
- (2) kiirendada ja peavoolustada tehisintellekti kasutuselevõttu võimearenduses, suurendades koostalitlusvõimet kui alliansi põhilist tugevust, sh tehisintellekti kasutuslugude kaudu;
- (3) kaitsta ja jälgida alliansi tehisintellekti tehnoloogiaid, juhtida seotud riske ja säilitada innovatsioonivõimet, võttes arvesse turvakaalutlusi, sh vastutustundliku kasutamise põhimõtted;
- (4) tuvastada tehisintellekti vaenulikust kasutamisest tulenevad ohud ja neid tõrjuda.

Eesti tähtsamatest liitlastest on tehisintellekti rakendamisel kaitsevaldkonnas vaieldamatult juhtpositsioonil Ameerika Ühendriigid, kes on avaldanud kaitsevaldkonna tehisintellekti rakendamise strateegia ning kelle lähemine põhineb n-ö kolmandal vastaste sõjalise ülekaalu tasalülitamise strateegial (*Third Offset Strategy*), mille eesmärk on edendada ja võtta kasutusele tehnoloogiad, mis tagaksid Ühendriikide relvajõudude ülekaalu võrgupõhises täppisrahangas sõjas. Strateegia üheks osaks on teatud protsesside ja süsteemide autonoomseks muutmine ning säärase süsteemide lisamine relvajõudude lahinguvälja võrgustikku, toetamaks lahinguväljal võitlevaid inimesi ja parandades viimaste sooritust. Samas näeb Ühendriikide kaitseministeerium ka tehisintellekti laiemat potentsiaali ning tehisintellekti rakendamiseks kogu valitsemisala ulatuses on loodud

Chief Digital and Artificial Intelligence Office.

Lisaks Ühendriikidele on kaitsevaldkonna tehisintellekti strateegia avaldanud Ühendkuningriik, Kanada, Norra, Prantsusmaa, Saksamaa ja Holland. Taani ja Türgi on kajastanud riigikaitseelisi eesmärke enda rahvuslikus tehisintellekti strateegias; Soome ja Hispaania on teinud sama digitaalsete muutuste strateegias. Belgia, Kreeka, Ungari ja Läti on teavitanud, et nad tegelevad kaitsevaldkonna tehisintellekti strateegia loomisega.

Arvestades kaitsevaldkonna tehisintellekti intensiivset arendamist liitlasriikides, ei ole kaitsevaldkonna tehisintellekti arendamine ja rakendamine Eestis mitte ainult vajadus, vaid teatud määral ka kohustus, et säilitada koostöövõime riikidega, kes aitavad tagada Eesti julgeolekut.

2.2 Venemaa

Kaitseministeeriumi valitsemisala, sh Eesti Kaitseväge tehnoloogilise arengu suunamine peab arvesse võtma meie tõenäolise vastase tehnoloogilist arengut. Kaitsevaldkonna tehisintellekti rakendamise kontekstis on vastuvõtmatu olukord, kus Eesti kaitseväelastel puuduvad lahinguväljal vaenlase autonoomsete süsteemiga kohtudes nende tõrjumiseks vajalikud teadmised, oskused ja vahendid.

Vaatamata sellele, et enamik Vene relvajõudude saavutustest Ukraina-vastases sõjategevuses tugineb traditsiooniliste relvasüsteemide rakendamisele, otsib ka Venemaa võimalusi tulemuslikumalt ja targemalt sõidida – nii praeguses sõjas Ukraina vastu kui ka valmistudes potentsiaalseks vastasseisuks NATOga. Nii Ukraina kui Vene relvajõud on Ukrainas tõestanud, et nad suudavad nii kopeerida kui ka ise välja töötada ning kasutusele võtta innovaatilisi lahendusi. Näiteks on Vene relvajõududes laialdaselt kasutusel vaatlus- ja ründedroonid¹ (nt Orlan ja Lancet), millele arendatakse pidevalt uusi lisavõimeid ja kasutamise taktikaid. Innovatsioonitsükli pikkust mõõdetakse Ukrainas toimivas sõjas nädalates ning vastase uus taktika või tehnoloogiline lahendus suudetakse lühikese aja jooksul neutraliseerida või ise kasutusele võtta.

Norra kaitseuringute instituudi [artikkel](#) Venemaa strateegilistest eesmärkidest sõjalise tehisintellekti arendamisel avab Venemaa juhtkonna mõtlemist tehisintellekti kasutuselevõtu osas. Näiteks sõnas Vladimir Putin 2022. aastal, et tehisintellekt määrab Venemaa julgeoleku, suveräänsuse ja positsiooni maailmas. Lisaks on Putin avaldanud toetust surmavate autonoomsete relvasüsteemide kasutuselevõtule, pidades kõige efektiivsemaks relvasüsteemi, mis tegutseb kiirelt ja peaaegu automaatselt. Venemaa juhtkond näeb tehisintellekti rakendamist ka võimalusena kompenseerida tehnoloogilist mahajäämust võrreldes lääneriikidega, nii sõjalises kui majanduslikus mõttes.

Sõjalist uurimis- ja arendustööd koordineerib Venemaal kaitseministeeriumi innovaatilise arenduse peadirektoraat (GUIR), mis rajati 2013. aastal. GUIRi võrgustikku kuulub 1200 asutust, sh mitmed tehisintellekti, autonoomia ja robotika testkeskust; 2022. aastal loodi Venemaal ka rahvuslik tehisintellekti arendamise keskus. Sõjalise tehisintellekti kasutamise eesmärgid on sõnastatud kahes 2014. aastal avalikustatud dokumendis, mis käsitlevad robotika arendamist ja rakendamist sõjapidamises vastavalt 2025. ja 2030. aastani.

Lisaks asetab Venemaa juhtkond palju rõhku ka kahese kasutusega tehnoloogiate ja vahendite arendamisele ning teadusalasemale tsiviil-militaarkoostööle. Näiteks tegeles 2022. aasta seisuga tehisintellektipõhiste relva- ja lahingusüsteemide arendamisega 150 ettevõtet ja haridusasutust. Konkreetset kasutuslood, millele Vene Föderatsioon hetkel sõjalise tehisintellekti arendamisel enam rõhku paneb, on mehitamata sõidukid ja

¹ Üldnimetus „ründedroonid“ alla võib paigutada ka varitseva õhuründemoona.

süsteemid, C4ISR võime parandamine, lahingujuhtimise edendamine, küberoperatsioonide läbiviimine, info- ja mõjutusoperatsioonide läbiviimine, satelliitsüsteemide tugevdamine ning tuumavõimega raketide arendamine.

Venemaa sõda Ukrainas on suurendanud vajadust kodumaise kõrgtehnoloogilise toodangu järele ja lähendanud Venemaad Hiinale. Ligipääs Hiina tehnoloogiatele ja oskusteabele võimaldab Venemaal ka tehisintellekti rakendamisel areneda kiiremini kui ainult oma võimetele ja vahenditele tuginedes.

2.3 Eesti

Eestis on seni tehisintellekti arengut koordineerinud Majandus- ja Kommunikatsiooniministeerium, mis koostöös Justiitsministeeriumi ja Haridus- ja Teadusministeeriumiga avalikustas 2024. aasta kevadel [tehisintellekti tegevuskava 2024–2026](#), mis on jätkuks aastatel 2019–2021 ja 2022–2023 ellu viidud tegevuskavadele. 2024. aastal ellu viidud struktuurimuutusega vastutab edaspidi Justiits- ja Digiministeerium riigi üldise digitaalse arengu, sealhulgas tehisintellektiga seotud tegevuste koordineerimise eest.

Viidatud tegevuskava eesmärk on edendada tehisintellekti arendamist ja kasutuselevõttu nii avalikus kui erasektoris, aga ka haridus- ning teadusvaldkonnas. Tegevuskava püstitab lähiaastateks eesmärgid tehisintellektil põhinevate lahenduste inimkeskseks ja usaldusväärseks rakendamiseks Eestis, seeläbi suurendades e-teenuste isikustatust, kasutajamugavust, kättesaadavust ning riigi tõhusust. Lisaks analüüsib tegevuskava tehisintellekti rakendamiseks vajalikke õigusruumi muudatusi, eestikeelse keelemudeli väljaarendamist ning kõrgjõudlusega andmetöötuse võime tagamist. Küll aga ei puuduta tegevuskava tehisintellekti arenguid kaitse- ja julgeolekuvaldkonnas.

Arvestades Ameerika Ühendriikide jt liitlaste laialdast tähelepanu tehisintellekti rakendamisele kaitsevaldkonnas, on ka Eesti jaoks kriitilise tähtsusega vastava tehnoloogilise kompetentsi ja inimressursi väljaarendamine. Vastasel juhul väheneb meie koostöövõime NATO partneritega ja seega ka meie julgeolek.

Kaitsealase tehisintellekti arendamisega on Kaitseministeeriumi valitsemisalas seni piiratud mahus ja projektipõhiselt tegelenud Kaitseväe Akadeemia rakendusuringute osakond, mis toetab teaduspõhiste uuringute ja uudsete lahenduste väljatöötamise kaudu Kaitseväe väevõimete arendamist. Küberväejuhatuse otsib aktiivselt võimalusi tehisintellekti rakendamiseks, sh Kaitseväe Olukorrateadlikkuse ja Lahingujuhtimise Teenuse (KOLT) süsteemi tehisintellektiga täiendades. Tallinnas asuv NATO küberkaitse koostöökeskus puutub kaitsevaldkonna tehisintellektiga kokku projektipõhiselt. Kuigi Kaitseliidu küberkaitseüksus (KKÜ) otseselt tehisintellekti arendamisega ei tegele, võimaldab KKÜ erinevate tehisintellektil põhinevate ja muude innovaatiliste lahenduste testimist. Riiklik sihtasutus CR14 küberharjutusväli on arendamas tehisintellekti „konteinerit“, mille eesmärk on pakkuda riigiasutustele võimalust tehisintellektil põhinevaid lahendusi arendada ja ohutult testida.

Eesti kaitsetööstuses tegeleb otsese tehisintellekti arendamise või enda toodetes kasutamisega vähemalt kümnekond ettevõtet. Tartu Ülikooli juures tegutseb 2024. aasta mais avatud Eesti tehisintellekti tippkeskus (EXAI), millel on potentsiaali panustada tehisintellekti rakendamisse ka kaitsevaldkonnas.

2023. aasta detsembris ilmus Rahvusvahelise Kaitseuringute Keskuse teaduri Tomas Jermalavičiuse detailne [ülevaade](#) tehisintellekti rakendamise hetkeseisust Eesti riigikaitstes. Süvaanalüüsi kaitsevaldkonna tehisintellekti rakendamise väljavaadetest Eestis on koostanud ka professor Wolfgang Koch ja erukindral Jörg Vollmer Fraunhoferi uurimisinstituudist Saksamaal. Mõlemad uurimused näevad tehisintellekti rakendamises Eesti riigikaitse tugevdamiseks suurt potentsiaali ning konstateerivad fakti, et tulevikus edu saavutamiseks on

kaitsevaldkonna tehisintellekti kohe algusest vaja arendada väga süsteemselt, läbimõeldult ja koordineeritult.

Kui seni on kaitsevaldkonna tehisintellekti arengud Eestis toimunud lähtuvalt erinevatest initsiatiividest, siis käesolev strateegia annab kaitsealase tehisintellekti arendamisele Eestis tervikliku arengusuuna, kaasates ja motiveerides valitsemisala allasutusi, kaitsetööstust ning kõrgharidus- ja teadusasutusi kaitsevajaduste täitmise teemal kaasa mõtlema ja koordineeritult tegutsema.

3. TEHISINTELLEKTI RAKENDAMINE KAITSEVALDKONNAS

3.1 Eesmärgid

Tehisintellekti süstemaatilise rakendamise peamine eesmärk on Kaitseministeeriumi valitsemisala efektiivsuse kasv viisil, mille puhul kaitsevaldkonna tehisintellekti arendamine ja rakendamine toimub vastavuses (1) Eesti Vabariigi strateegiliste eesmärkide, (2) Eesti Vabariigi poliitiliste ja eetiliste põhimõtete ning seisukohtadega ja (3) tagab koostöövõime teiste organisatsioonide ja/või riikidega. Tehisintellekti rakendamine peab tagama aja, raha või inimressursi (või kõigi kolme) kokkuhoiu, võimaldama püstitatud ülesandeid olemasolevate ressurssidega paremini täita või looma püstitatud eesmärkide saavutamiseks täiesti uue võime.

Tehisintellekti rakendamine Kaitseministeeriumi valitsemisalas peab toetama Eesti kaitsevõime kasvu. Sellest tulenevalt jagunevad tehisintellekti rakendamise eesmärgid Kaitseministeeriumi valitsemisalas peamiselt kolmeks:

- (1) **Otseste sõjaliste eeliste loomine:** tehisintellekti rakendamine peab otsuselangetamise toetamise, luureinfo töötlemise ja sihtmärgistamise kiirendamise kaudu võimaldama tõsta lahingutegevuse kiirust ning täpsusrünnakute teostamise võimet, sh küber- ja õhukaitse valdkondades, kus domeenipõhiselt kulgevad ründe- ja kaitsetegevused toimuvad inimese reageerimiskiirusest kordades kiiremini. Tehisintellekti rakendamine autonoomsetes relva- ja muudes süsteemides võimaldab suurendada relvasüsteemide hävitusjõudu ning vähendada ohtu ja koormust inimestele lahinguväljal, sh teatud ülesannete masinatele delegeerimise kaudu (luure, logistika, valve, jms).
- (2) **Tugiteenuste efektiivsemaks muutmise:** toimiv logistika on eduka lahingutegevuse üks peamisi eelduseid. Tehisintellekti rakendamine peab muutma tugiteenused kiiremaks ja täpsemaks, näiteks tarneahela efektiivsema analüüsi või tõhusama varustuse hoolduse planeerimise kaudu. Samas seisab ka Kaitseministeeriumi valitsemisala silmitsi tavapäraste avalike asutuste väljakutsetega, nagu andme-, dokumendi- või personalihaldus, mida on samuti võimalik tehisintellekti abil lihtsustada.
- (3) **Kohaliku kaitsetööstuse tugevdamine:** kaitsetööstus on osa Eesti riigikaitsest selle laias käsitluses. Kaitsevaldkonna tehisintellekti arendamine ja rakendamine Eesti Kaitseväes loob kaitsetööstusele ühest küljest perspektiivi kaasaegseimate tehisintellektile tuginevate toodete arendamiseks ja peab teisest küljest aitama kaasa ka kaitsetööstuse enda arengule. Riigi ja kaitsetööstuse tugev koostöö, sh ühiste kaitsevaldkonna tehisintellekti arenduste ja testimiste läbiviimine koostöös Kaitseväe ja Kaitseväe ja Kaitseväe, on vajalik nii Eesti riigikaitse vajaduste rahuldamiseks kui ka kaitsetööstuse arenguks tervikuna, mis tugevdab tulemusena ka Eesti majandust ja ekspordivõimet.

3.2 Eesmärkide saavutamise viisid

Kaitsevaldkonnas tehisintellekti rakendades on vaja jõuda olukorrani, kus tehisintellekt võimaldab kogu süsteemil kui tervikul (mitte ainult konkreetsetel funktsioonidel) efektiivsemalt toimida, ehk kiiremini ja paremini täita nii otseseid lahinguvälja ülesandeid kui ka teostada neid ettevalmistavaid või toetavaid tegevusi.

Sellise võime tagamine eeldab aga vajaliku vundamendi ladumist ehk kontseptuaalse lähenemise väljatöötamist, mis peaks olema Kaitseministeeriumi valitsemisalas tehisintellekti süsteemse rakendamise esimene samm. Teisisõnu, otsused konkreetsete tehisintellekti rakenduste arendamise ja kasutamise üle eeldavad selget valitsemisala ülest arusaama, kuidas hakkab Kaitsevägi tehisintellekti rakendamise abil paremini sõdima ja ülejäänud valitsemisala allasutused Kaitseväge tegevust toetama. Vajaliku kontseptuaalse arusaamani ning sellele järgneva süsteemse tehisintellekti rakendamise valmiduseni jõudmine eeldab mitmete alustegevuste elluviimist, mis moodustavad peamise osa käesoleva strateegia rakenduskavast. Vajalikud tegevused on jagatud viide kategooriasse:

- (1) **Kaitseväge digitaalse ja tehnoloogilise arengu eest vastutava struktuuriüksuse loomine:** töötamaks välja kaitsevaldkonna tehisintellekti rakendamise kontseptuaalset lähenemist, kaalutakse Kaitseväge Peastaabi võimaliku reformi raames vastutava isiku ametisse määramist, soovitavalt Kaitseväge innovatsioonijuht (*Chief Innovation Officer*) ja/või digitaliseerimise juht (*Chief Digitalisation Officer*). Neil isikutel on pädevus, ülesanne, volitused ja kindel eelarve valitsemisala tehnoloogilisi, sh tehisintellekti-alaseid arenguid terviklikult suunata ja prioriseerida ning selleks vajalik struktuuriüksus komplekteerida. Loodav struktuuriüksus koostab edaspidi ka kaitsevaldkonna tehisintellekti detailse rakenduskava, sh määrates tehisintellekti kasutuselevõtu riski lävendi, mõõdikud ja eelarve vajaduse. Muu hulgas peab loodav struktuuriüksus hindama kahese kasutuse ehk kommertstehnoloogiate rakendamise võimalikkust teatud ülesannete täitmiseks.
- (2) **Kaitseväge digitaalse infotaristu loomine:** tehisintellekti süstemaatilise rakendamise peamine tehnoloogiline eeldus on Kaitseväge digitaalse infotaristu kavandamine ja ülesehitamine, mis võimaldab kõikide süsteemide ja üksuste vahelist andmevahetust. Lisaks luuakse Kaitseministeeriumi valitsemisala ülene andmehalduse kontseptsioon ja vajalikud andmestandardid ning viiakse läbi andmete kaardistamine ja nende omanike määramine, mis tagavad koostalitusvõime valitsemisala allasutuse vahel ning ka Eesti ja NATO liitlaste vahel. Tähelepanu peab pöörama ka andmete pikaegsele kogumisele, et luua eeldused süsteemide väljaõpetamiseks ja oluliste trendide väljaselgitamiseks.
- (3) **Kaitseväge kõrgtehnoloogilise teadlikkuse ja tehisintellektiga seonduvate oskuste arendamine:** Kaitseministeeriumi valitsemisala tehisintellekti-alane teadlikkus on hetkel madal ning vastava hariduse ja kogemusega eksperte on vähe. Olukorra muutmiseks peab Kaitseministeerium investeerima valitsemisala digitaalse ja tehnoloogilise teadlikkuse kasvatamisse nii teoreetilise kui praktilise õppe kaudu Kaitseväge Akadeemias ja teistes kõrgharidusasutustes ning looma rahaliselt toetatud kaitsevaldkonna tehisintellektile keskenduvad magistri- ja doktoriõppe programmid. Arvestades ka teiste valdkondade üha suurenevat nõudlust tehnoloogiaharidusega spetsialistide järele, keda Eesti haridussüsteem kahjuks piisaval hulgal ette ei valmista, tähendab see Kaitseministeeriumi valitsemisalale vajadust arendada tihedat koostööd tehisintellekti arendavate tsiviilstruktuuridega, et vastavat kompetentsi optimaalselt rakendada.

- (4) **Koostöö tsiviilstruktuuridega kaitsevaldkonna tehisintellekti arengu toetamiseks:** kaitsevaldkonna tehisintellekti arengud peavad olema võimalikult kooskõlas teiste riiklike tehisintellekti arengute eesmärkidega, et võimaldada ressursside ja teadmiste jagamist. See eeldab vajalike koostöövõrgustike loomist erasektori ning kõrgharidus- ja teadusasutustega. Reaalteaduslikult pädeva järelkasvu tagamine algab aga juba üldhariduskoolides, mistõttu on oluline teha koostööd Haridus- ja Teadusministeeriumiga, et suurendada noorte huvi reaalteaduste vastu. Lisaks peab Kaitseministeeriumi valitsemisala otsima võimalusi seadusandluse uuendamiseks ja paindlikumaks muutmiseks, kiirendamiseks kaitsetööstuse arengut ja võimaldamaks tehisintellekti kasutamist ka salastatud süsteemides, sh operatsiooniliste vajaduste rahuldamiseks.
- (5) **Rahvusvahelistes võrgustikes osalemine ja liitlastega koostalitusvõime tagamine:** piiratud ressursside ja teadmiste valguses on oluline jälgida rahvusvahelisi kaitsevaldkonna tehisintellekti arenguid ning nendest ligipääsetavate võrgustike kaudu osa saada. Strateegia elluviimisel määratakse kindlaks, mida soovib Eesti riik tehnoloogilise arengu mõttes saavutada osalusega NATO töögruppides, Euroopa Kaitsefondis, NATO küberkaitse koostöökeskuse ja NATO DIANA regionaalse keskuse võõrustamisest ning kuidas antud võrgustikest kogutud teavet maksimaalselt tehisintellekti rakendamiseks Eestis ära kasutada. Kaitsevaldkonna tehisintellekti-alase rahvusvahelise koostöö põhifookus suunatakse Põhjala ja Balti riikidele ning Ühendkuningriigile ja Ameerika Ühendriikidele, et arendada ja tagada Kaitseväe kasutusse minevate tehisintellekti-põhiste süsteemide koostalitusvõime Eesti lähimate liitlastega.

3.3 Eesmärkide saavutamiseks vajalikud ressursid

Strateegias püstitatud eesmärkide ja nende saavutamiseks vajalike tegevuste elluviimiseks toetatakse järgmises riigikaitse arengukavas (RKAK 2026–2035) kavandatud ressurssidele, mis omakorda jaotatakse vajaduspõhiselt kaitseministeeriumi arengukava kaudu. Kaitseministeeriumi valitsemisalas prioriseeritakse arendustegevuses kaitsevaldkonna tehisintellektile keskenduvaid projekte, et tagada Kaitseväe väevõimete nõutav areng. RKAKi iga-aastasest teadusfinantseeringust kasutatakse 30–50% teadusalaseks kaitsevaldkonna tehisintellekti arendamiseks.

Kaitsevaldkonna tehisintellekti rakenduste vajalikuks testimiseks ja arendamiseks suurendatakse rahastust eksperimenteerimise läbiviimiseks, mis peab toimuma selgelt läbi mõeldud prioriteetsete valdkondade põhiselt.

3.4 Eetilised ja juriidilised põhimõtted ja piirangud kaitsevaldkonna tehisintellekti arendamisel ja rakendamisel

Kaitsevaldkonna tehisintellektiga seonduvaid eesmärke täites on oluline, et Eesti arendab ja rakendab tehisintellekti rahvusvahelise õiguse, liitlastega kokkulepitud põhimõtete ning muude nõuete ja nende ühtse tõlgendamise raames.

NATO liikmena kohustub Eesti lähtuma alliansi 2021. aasta tehisintellekti strateegias vastuvõetud kuuest vastutustundliku kasutuse põhimõttest (PRUs – *principles of responsible use*), milleks on seaduslikkus (*lawfulness*), vastutus (*responsibility and accountability*), seletatavus ja jälgitavus (*explainability and traceability*), usaldusväärsus (*reliability*), valitsetavus (*governability*) ning kallutatuse tasalülitamine (*bias*

mitigation).

Koos enamiku NATO liikmesriikidega toetab Eesti Ameerika Ühendriikide algatatud [poliitilist deklaratsiooni](#) tehisintellekti ja autonoomsete süsteemide vastutustundliku kasutamise suhtes sõjapidamises. Tehisintellekti rakendamisega sõjapidamises kaasneb õigustatult hirm, et surmavad autonoomsed relvasüsteemid (*Lethal Autonomous Weapons Systems, LAWS*) võivad kasutada surmavat jõudu viisil, mis on vastuolus rahvusvahelise humanitaarõigusega. LAWS on tehnoloogia, mis teeb relvastatud jõu kasutamisel võtmeotsuseid (nt sihtmärgi valik ja ründamine) varasemalt programmeeritud kriteeriumide ja piirangute alusel, st vähemalt osaliselt ilma inimese samaaegse sekkumiseta. LAWS täpse definitsiooni osas puudub täna aga riikide hulgas üksmeel.

Eesti esitas enda LAWSi puudutavad seisukohad alates 2017. aastast ÜRO juures tegutsevale valitsusekspertide rühmale (Group of Governmental Experts, GGE) 2022. aastal, millest olulisemad puudutavad järgmist:

- (1) rahvusvaheline humanitaarõigus kohaldub täielikult ka uute ja arenevate tehnoloogiate kasutamisele, mh LAWSile;
- (2) LAWSi puhul ei tuleks kõneleda kõikvõimalikest autonoomsetest süsteemidest ja funktsioonidest, vaid keskenduda tuleks sihtmärgistamise ja ründamise otsustamise autonoomsele funktsioonile;
- (3) LAWSi tehtavate otsuste üle peab säilima inimkontroll tasemel, mis tagab LAWSi kasutamise kooskõlas rahvusvahelise õigusega;
- (4) lõppastmes vastutab rahvusvahelise õiguse rikkumiste eest riik ja/või konkreetne isik, mistõttu peab olema võimalik LAWSi tehtavaid otsuseid omistada riigile ja/või isikule;
- (5) Genfi konventsiooni 1. lisaprotokollis artikkel 36 järgi tuleb enne uue relva(süsteemi) kasutuselevõtmist läbi viia relvaanalüüs.

2023. aasta mais esitlesid Ühendriigid GGEle dokumenti, mis möönab, et kuigi lõplikuks vastutajaks jääb inimene, ei pea LAWS puhul alati lõplikku otsust sihtmärgi ründamise kohta tegema inimene, kui kõik teised kriteeriumid relvasüsteemi vastutustundlikul arendamisel ja kasutamisel on täidetud. Eesti on Ühendriikide ettepaneku osas suuresti toetav, ent 2022. aastal ÜROle esitatud seisukohtadele tuginedes peab Eesti oluliseks, et inimkontroll sihtmärgistamise protsessis oleks selline, mis tagab inimesele lõpliku otsustusõiguse surmava jõu kasutamise osas (nn *kill switch* lahenduste, eelseadistuste vms kaudu).

EKTL on kinnitanud, et Eesti kaitsetööstuse ettevõtted jälgivad rahvusvahelise õiguse arenguid ning toimivad nii toodete arendamisel kui teadus-arendustegevuses vastavalt rahvusvahelise õiguse sätetele. Lisaks toetatakse Euroopa Kaitsefondi [määrusele](#), mille põhjal ei soodusta fond selliste autonoomsete surmavate relvade väljatöötamist, mille üle puudub sihtmärkide valimisel ja inimeste ründamise otsuse tegemisel tegelik inimkontroll. Eesti kaitsetööstuse arendamise perspektiivist on oluline, et rahvusvahelised regulatsioonid ja normid ei muutuks liiga bürokraatlikuks ega piiravaks, mis takistaks ja aeglustaks toodete arengut, vaid toetaks vastutustundlikku innovatsiooni.

4. RAKENDUSKAVA

Rakenduskava on eraldi dokument ja keskendub ülal toodud viie peamise tegevussuuna elluviimisele, mis peavad tagama tehisintellekti süsteemse rakendamise Kaitseministeeriumi valitsemisalas. Käesoleva strateegiaga kaasas käiv rakenduskava määrab ära esmased prioriteetsed tegevused; detailse rakenduskava töötab välja ametisse määratav vastutav isik ja temale alluv struktuuriüksus. Rakenduskava ei ole avalik dokument.