SISEKAITSEAKADEEMIA

SISEJULGEOLEKU INSTITUUT

EMILIA MUUGA, RAUL SAVIMAA, JAANIKA PUUSALU,
RAMON LOIK, RINGO RINGVEE, MÄRT LÄÄNEMETS,
JÜRI SAAR, GEORG-HENRI KAUP

EESTI SISEJULGEOLEKUT MÕJUTAVATE GLOBAALSETE ARENGUTRENDIDE PROGNOOS

2026–2030

Kaasrahastanud Euroopa Liit

SISEMINISTEERIUM

EMILIA MUUGA, RAUL SAVIMAA, JAANIKA PUUSALU,
RAMON LOIK, RINGO RINGVEE, MÄRT LÄÄNEMETS,
JÜRI SAAR, GEORG-HENRI KAUP

Eesti sisejulgeolekut mõjutavate globaalsete arengutrendide prognoos 2026–2030

Autorid tänavad Jüri Vlassovi ja Mari-Liis Tori käsikirja läbivaatamise ja väärtuslike märkuste eest.

Kaanepilt: Microsoft Copilot, 2025

Makett ja küljendus: Jan Garshnek

Keeletoimetaja: Siiri Soidro

Trükk: Trükikoda Joon

ISBN 978-9985-67-530-4 (trükis)

ISBN 978-9985-67-531-1 (pdf)

DOI: https://doi.org/10.15158/ebp3-4496

www.sisekaitse.ee/kirjastus

SISUKORD

EESSÕNA

Riigid kogu maailmas on juba aastaid pidanud kohanema turbulentse multikriiside[1] ajastuga, seistes korraga silmitsi väga erinevate väljakutsetega. Ebakindlus ja ärevus ühiskonnas kasvavad. Lisaks Venemaa ja Hiina tegevusele on ohuks saanud ka näiliselt ettearvamatud otsused USA välis- ja julgeolekupoliitikas ning teadmatus, kas Euroopa Liidul ja NATO-l on stabiilsuse tagamiseks piisavalt konsensust ja jõudu.

Eesti jaoks on loomulikult suurimaks julgeolekuohuks ründava Venemaa naabrus ja selle tegevusest lähtuv võimalik julgeolekukeskkonna halvenemine. Kuigi Eesti otsese sõjalise ründamise oht on olemas, on see Välisluureameti (2025) hinnangul vähetõenäoline. Siiski tegeleme selle riski maandamisega äärmiselt tõsiselt, valmistudes halvimaks. Kahtlemata sõltub Eesti julgeolekuolukord Ukrainas toimuvatest arengutest, kuid peame ka tõdema, et Eesti sisejulgeolekut mõjutavad ohud ei tulene pelgalt Venemaa tegevusest ning kestvate kriisidega hakkamasaamise ja suurenenud sõjaliste riskide maandamise kõrval tuleb meil aktiivselt tegeleda ka muude ohtude ennetamisega.

Ajaloo suurimas infotulvas ning tehisaru teadmata tagajärgedega integreerimisel igapäevaellu on järjest olulisem kasvatada meie elanike teadmisi, kriitilise mõtlemise oskust ja manipulatsioonide äratundmist. Väärinfo ja desinformatsiooni levik on Eesti jaoks üks suurima mõjuga riskidest, mistõttu on oluline tegeleda küberruumis (sotsiaalmeedia ja digiplatvormid) eri põlvkondi valitsevate ohtudega, mida autoritaarseid režiime soosivad riigid oskuslikult propaganda levitamiseks ja sihtgruppide manipuleerimiseks ära kasutavad. Ka meie enda erakondade võimuvõitlusega kaasnev manipulatsioon ja väärinfo levitamine toidavad seestpoolt ühiskonna polariseerumist ja radikaliseerumist, mis paratamatult tekitab laiema küsimuse: kui me ise oleme enda elanike seas suutelised niisuguseid võtteid kasutama, siis kuivõrd oleme tegelikult valmis kaitsma elanikkonda väljastpoolt tuleva massimõjutuse eest?

Laiapindne riigikaitse käsitlus erinevate ohuvektorite kaudu on võti, mis võiks aidata ennetada ja valmistada ette ühiskonda toime tulema ka siis, kui peaks realiseeruma mitu ohtu samal ajal. Erinevate kriiside jätkumisel on riigil tähtis hoida kiiret arengu- ja reageerimisvõimet ning oskust integreerida arenevad tehnoloogiad edukalt valmisolekusse ja kaitsevõimekusse, mitte lasta neil areneda selle vastu. Lisaks Venemaale, millel on kombeks liikuda oma eesmärkide poole kärarikkalt, on meie ümber teisigi riskitegureid, mille arengud on latentsed ja sihikindlad. Veel mõned aastad tagasi ei näinud ükski enim kajastatavatest riskihinnangutest ette, et lähima paari aasta jooksul saab olema meie

[1] Multikriisina mõistetakse siinses raportis mitme erineva ühiskonda mõjutava kriisi samaaegset avaldumist, mis ei pruugi olla omavahel otseselt seotud ja üksteisele avalduvat mõju ilmtingimata võimendada. Sellistel kriisidel on erinevad põhjustajad ja neid ei saa lahendada ühetaoliselt.

kõige suuremaks ohuks kogu maailma haarav pandeemia ja sõjaline tegevus Euroopas. Meil tuleb sellest õppida ja valmistuda ka sellisteks ohtudeks, mis kuuldavalt praegu veel uksele ei koputa.

Eesti sisejulgeolekut mõjutavate globaalsete arengutrendide viie aasta (2026–2030) prognoosi eesmärk on pakkuda teaduspõhist strateegilist sisendit Eesti (sise)julgeolekupoliitika, sh Eesti julgeolekupoliitika raamdokumendi „Eesti julgeolekupoliitika alused", arendamiseks. Sisekaitseakadeemia sisejulgeoleku instituudi teaduskeskus on selleks 2025. aasta alguses läbi viinud uuringu, mille käigus hinnati 24 Eesti erialaeksperdi abiga 29 rahvusvaheliselt kõige tõenäolisemalt realiseeruda võivat globaalset riski ja nende võimalikku mõju Eestile. Riskide ja nende mõju hindamisel on ajahorisondina fookusesse võetud kesk-pikk perspektiiv (5–7 aastat) ning need järjestati realiseerumise tõenäosuse ja Eesti jaoks võimaliku mõju ulatuse alusel, millele Sisekaitseakadeemia teadurid on lisanud omapoolse analüüsi ja selgitused.

Head lugemist!

GLOBAALSED RISKIHINNANGUD

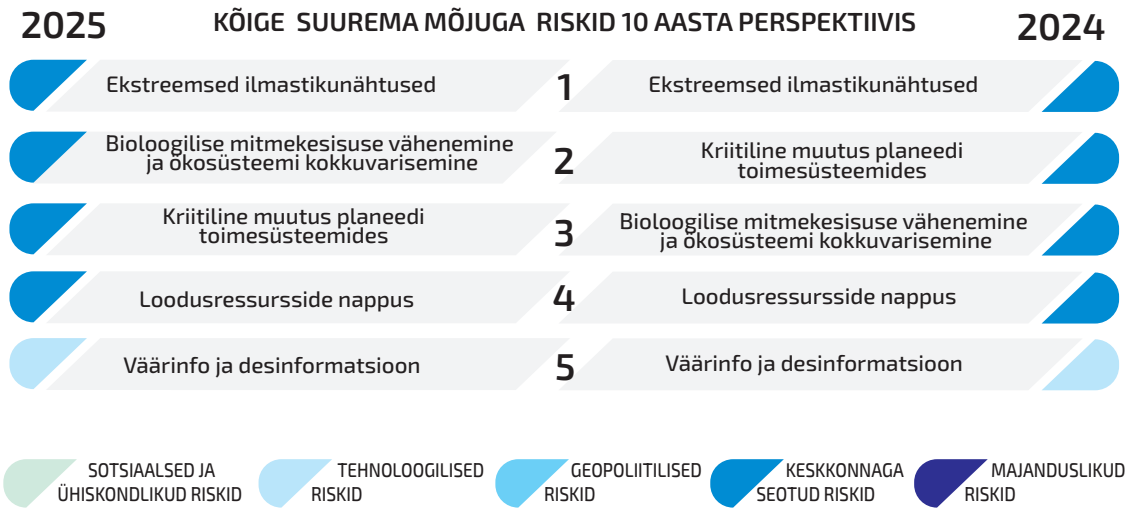
Maailma Majandusfoorum (World Economic Forum, 2025) ja European University Institute (Anghel, 2025) on 2025. aasta seisuga hinnanud Euroopas ja maailmas tervikuna lähiaastatel kõige tõenäolisemateks ning suurima mõjuga globaalseteks riskideks väärinfo ja desinformatsiooni leviku, riikidevaheliste relvastatud konfliktide esinemise, Venemaale soodsa relvarahu sõlmimise sõjas Ukrainaga ning USA taganemise Euroopa liitlastele pakutavatest julgeolekugarantiidest (vt riskide detailsemat kirjeldust lisa 2).

JOONIS 1. MAAILMA MAJANDUSFOORUMI RISKIHINNANGUTE KAHE AASTA VÕRDLUS (ALLIKAS: WORLD ECONOMIC FORUM)

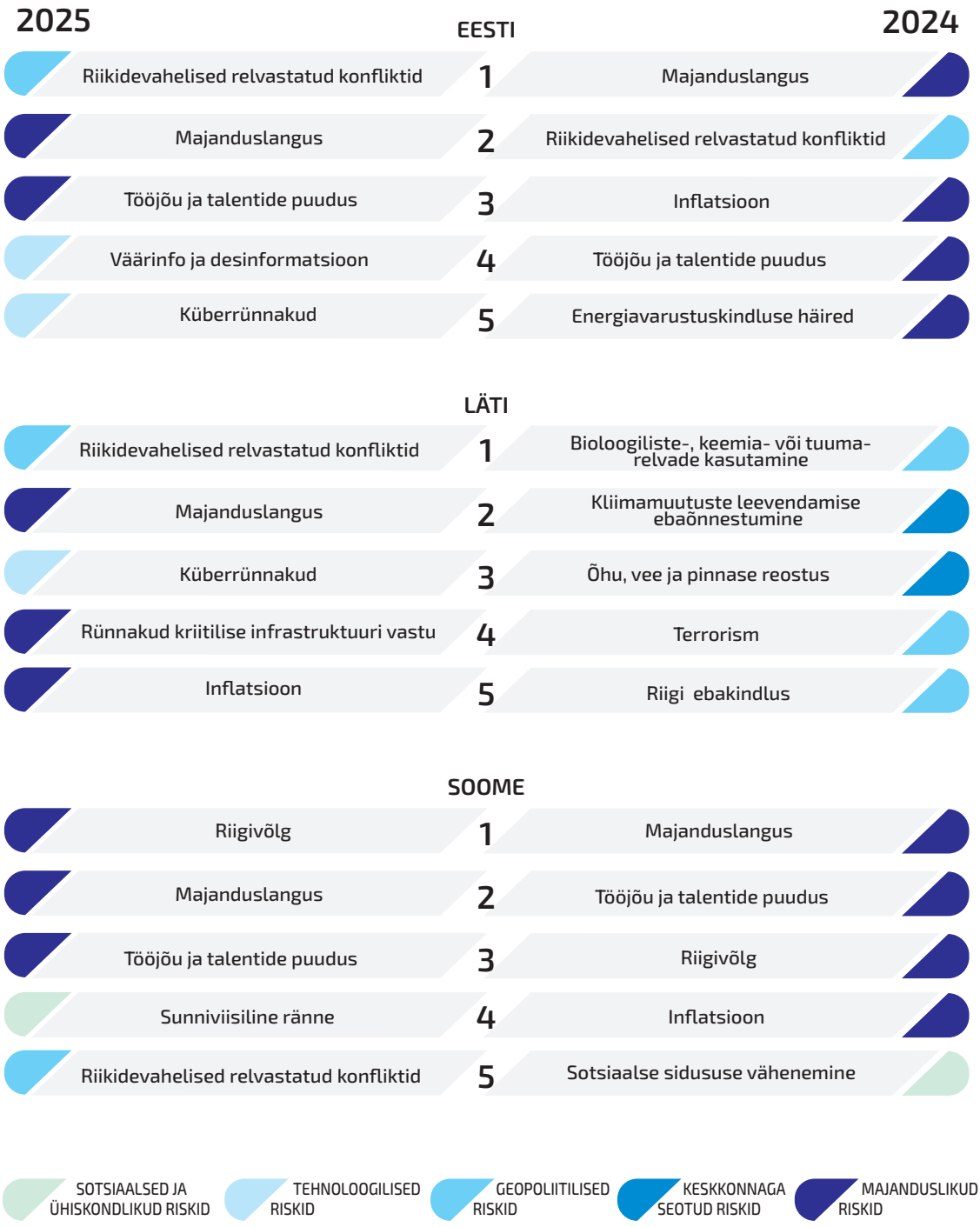
Maailma Majandusfoorumi globaalsete riskide uuringu (*World Economic Forum Global Risks. Perception Survey*) kohaselt (World Economic Forum, 2024, 2025) on kahe aasta perspektiivis kõige ulatuslikuma mõjuga riskiks nii 2024. kui ka 2025. aastal hinnatud väärinfo ja desinformatsiooni levikut. Teisel kohal on mõlemal aastal muutumatuna püsinud äärmuslike ilmastikuolude põhjustatud sündmused (joonis 1). Kui 2024. aasta raportis oli kolmandaks riskiks hinnatud ühiskonna polariseerumise oht, siis 2025. aastal on sellele kohale tõusnud riikidevahelise relvastatud konflikti oht. Võrdlusena oli näiteks aastatel 2019 ja 2007 kõige ulatuslikuma mõjuga riskiks hinnatud vastavalt massihävitusrelvade kasutamine ja varahindade mulli lõhkemine (World Economic Forum, 2020).

Aasta jooksul kõige tõenäolisemalt kriisi põhjustava riskina on võrreldes eelneva aastaga viimases raportis asendunud ekstreemsed ilmastikunähtused samuti riikidevahelise relvastatud konflikti ohuga. Aastatel 2019 ja 2007 olid sellisteks riskideks hinnatud näiteks ekstreemsete ilmastikuolude esinemine ning infrastruktuuri häired (World Economic Forum, 2020). Samas kümne aasta perspektiivis oli hinnatud riskide puhul esimesed neli kõige suurema mõjuga ohtu nii käesoleval kui ka eelneval aastal just keskkonnaga seonduvad riskid (joonis 2).

Maailma Majandusfoorumi raport sisaldab ka juhtide seas läbiviidud arvamusküsitluse tulemusi, et teha kindlaks riskid, mis kujutavad iga riigi jaoks järgneva kahe aasta jooksul kõige suuremaid ohtusid. Selle kohaselt domineeris 2025. aasta raportis Eesti ja Läti hinnangul sõjalise konflikti risk, millele järgnes majanduslanguse oht. Aasta varasemas raportis hinnati viimane Eesti jaoks kõige suuremaks riskiks (joonis 3).



JOONIS 2. MAAILMA MAJANDUSFOORUMI KÜMNEAASTASE PERSPEKTIIVIGA RISKIHINNANGUTE KAHE AASTA VÕRDLUS (ALLIKAS: WORLD ECONOMIC FORUM)

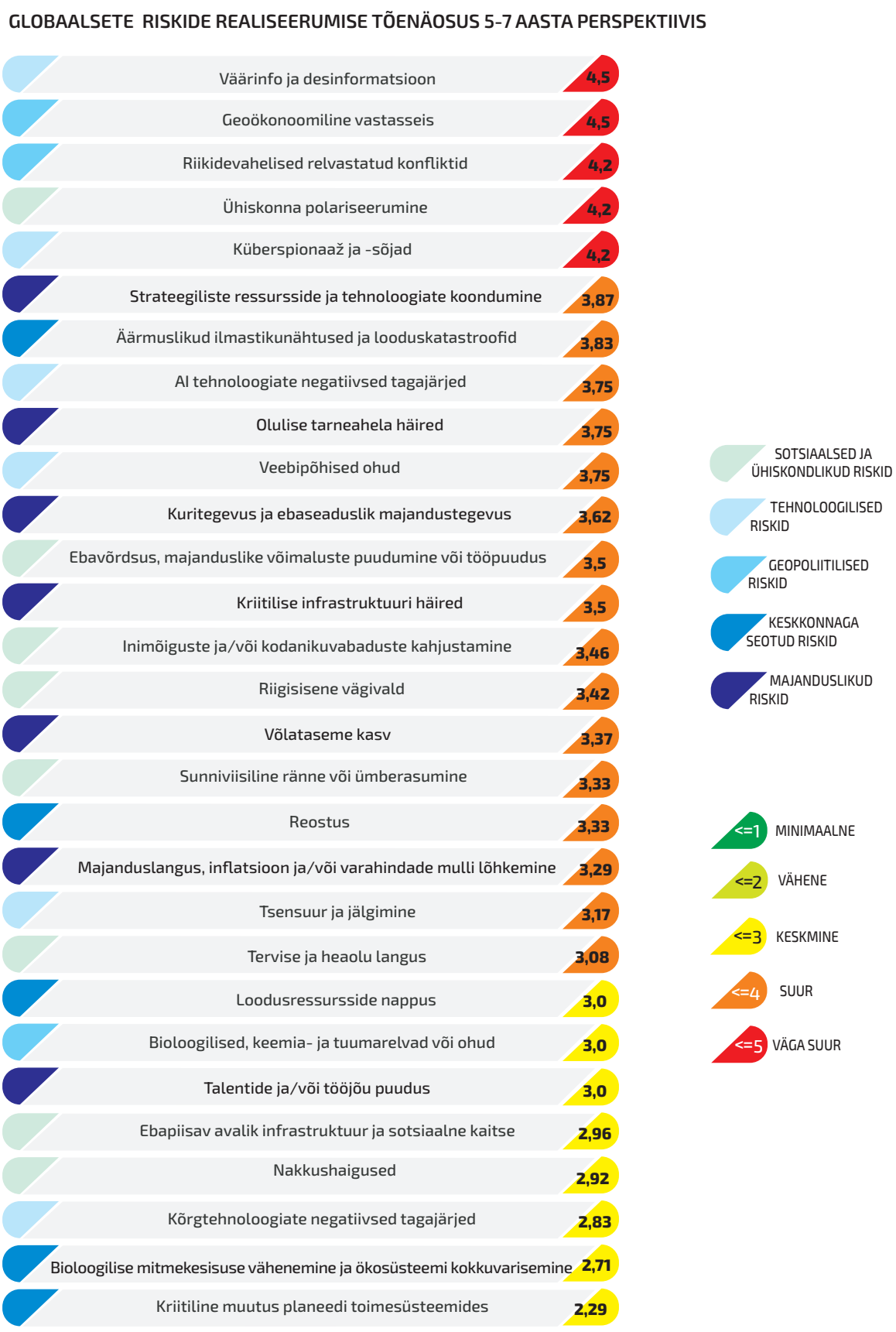


JOONIS 3. MAAILMA MAJANDUSFOORUMI JUHTIDE ARVAMUSKÜSITLUSE TULEMUSTE KAHE AASTA VÕRDLUS EESTI, SOOME JA LÄTI KOHTA (ALLIKAS: WORLD ECONOMIC FORUM)

Uuringu „Globaalsed riskid EL-ile“ (Anghel, 2025) kohaselt on kõige suurema mõjuga riskideks EL-i jaoks USA võimalik taganemine julgeolekugarantiidest Euroopa liitlastele ning hübriidrünnakud EL-i elutähtsa taristu vastu. Kõige suurema realiseerumise tõenäosusega riskideks on hinnatud Iisraeli ja Hamasi vahelise relvarahu puudumist ning Venemaad pooldava valitsuse ametisse asumist Gruusias (joonis 4).

JOONIS 4. EUROOPAT KÕIGE ENAM MÕJUTAVAD GLOBAALSED RISKID (ALLIKAS: ANGHEL, 2025)

Sisekaitseakadeemia poolt läbiviidud Eesti ekspertide uuringu järgi olid 2025. aasta alguses kõige suurema realiseerumise tõenäosusega globaalseteks riskideks väärinfo ja desinformatsiooni levik ning geoökonoomiline vastasseis (joonis 5). Veel peeti väga suure tõenäosusega realiseeruvateks riskideks riikidevahelisi relvastatud konflikte, ühiskonna polariseerumise ohtu ning küberspionaaže ja -sõdu. Kuigi 5–7 aasta perspektiivis hinnati keskkonnaga seonduvate riskide tõenäosust pigem keskmiseks, siis 10–50 aasta perspektiivis pidasid eksperdid nende realiseerumist oluliselt tõenäolisemaks.



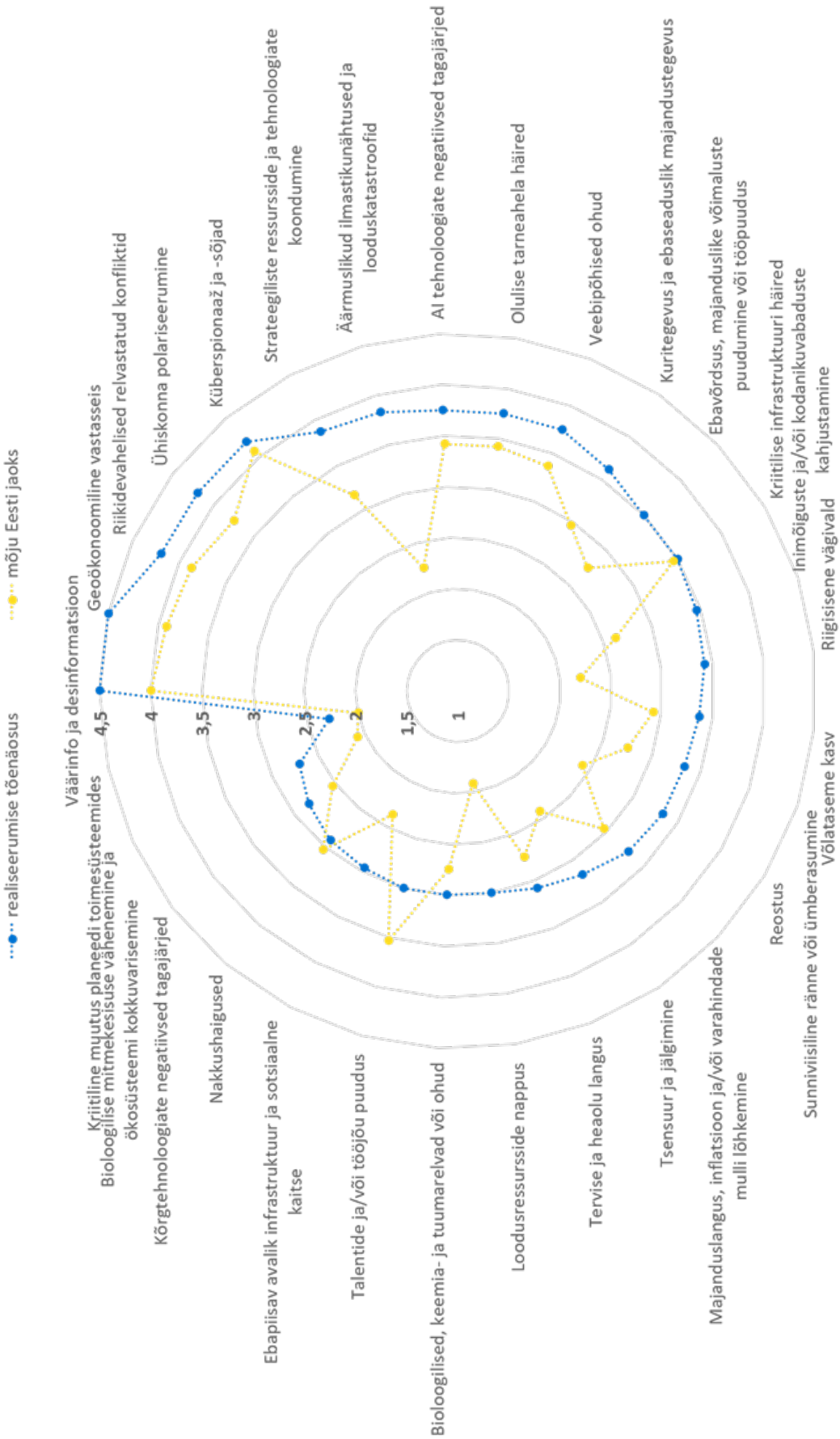
JOONIS 5. SISEKAITSEAKADEEMIA UURINGU TULEMUSENA SELGUNUD EESTI EKSPERTIDE HINNANGUD GLOBAALSETE RISKIDE REALISEERUMISE TÕENÄOSUSE KOHTA

Järgnevalt on välja toodud viie Eestit kõige enam mõjutava riski realiseerumise võimalik mõju.

EESTIT KÕIGE ENAM MÕJUTAVAD OHUD

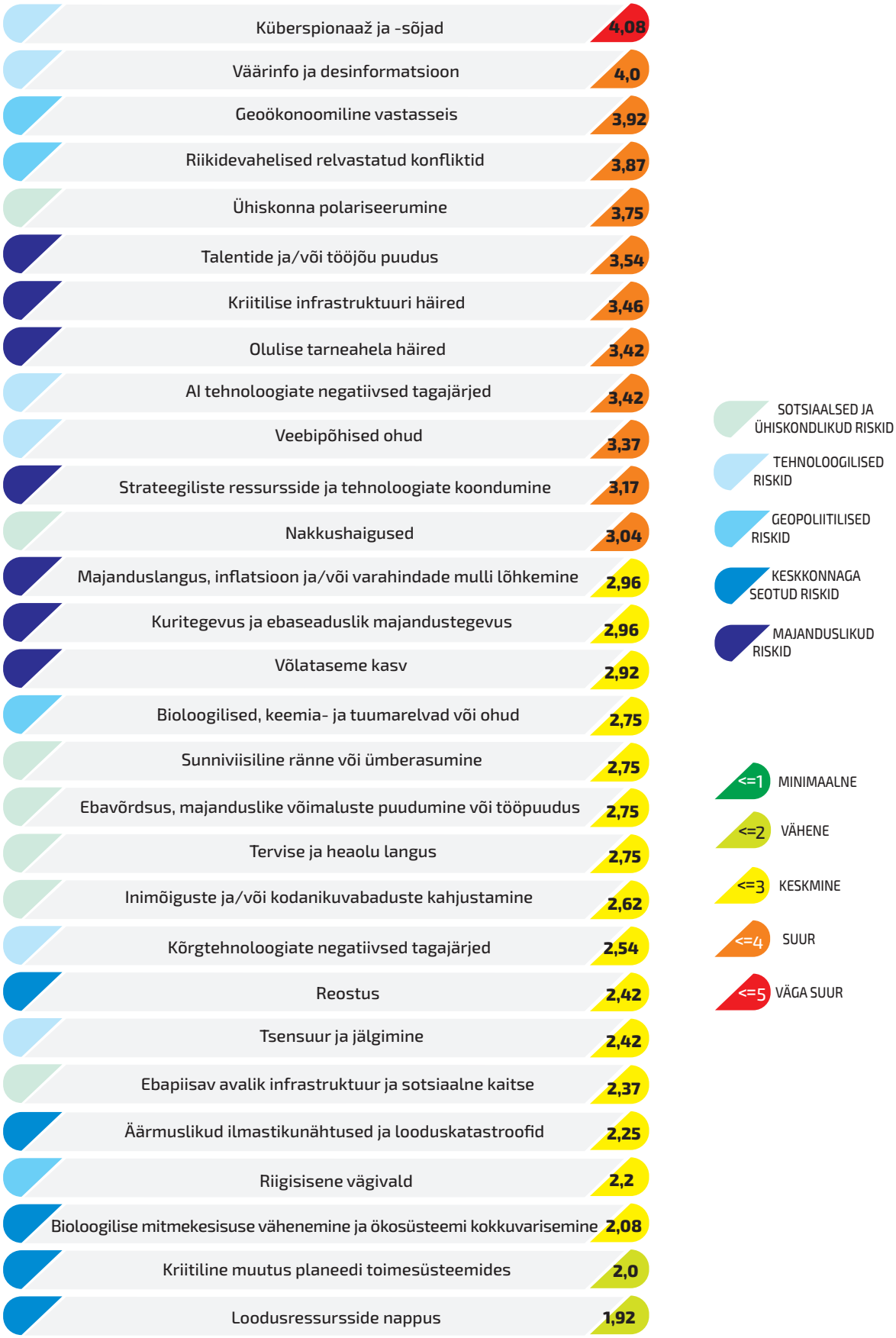
2025. aasta kevadel paluti Eesti ekspertidel hinnata (vt täpsemalt lisa 1) eraldi globaalsete riskide realiseerumise tõenäosust ja nende realiseerumisel võimalikku mõju Eesti jaoks. Kahe kriteeriumi koondvaate kohaselt (kõige suurem realiseerumise tõenäosus ja Eestile avalduv mõju) olid suurimateks riskideks küberspionaaži ja -sõdade oht ning väärinfo ja desinformatsiooni levik (joonis 6).

Eestile tõenäoliselt kõige suuremat mõju avaldavateks riskideks hinnati lisaks küberspionaaži ja -sõdade ohule ning väärinfo ja desinformatsiooni levikule veel riikidevaheliste relvastatud konfliktide, geoökonoomilise vastasseisu ja ühiskonna polariseerumise riske (joonis 7). Eksperdid ei hinnanud 5–7 aasta perspektiivis keskkonnaga seonduvate riskide mõju kõrgeks, kuid 10–50 aasta perspektiivis peeti selliseid riske oluliselt kõrgemaks.



JOONIS 6. EESTI EKSPERTIDE HINNANGUD GLOBAALSETE RISKIDE REALISEERUMISE JA EESTILE KÕIGE SUUREMA AVALDUVA MÕJU KOHTA

RISKIDE VÕIMALIKU REALISEERUMISE MÕJU EESTI JAOKS



JOONIS 7. EESTI EKSPERTIDE HINNANGUD EESTILE KÕIGE SUUREMA MÕJUGA RISKIDE KOHTA

KÜBERSPIONAAŽ JA -SÕJAD

Küberspionaaži ja -sõdade realiseerumise võimalikku mõju Eesti jaoks hindasid Eesti eksperdid kõige suuremaks (joonis 7). Selle riski all peeti silmas (vt täpsemalt lisa 2) võimalikku küberrelvade ja -vahendite kasutamist riiklike ja valitsusväliste osalejate poolt, et saavutada kontroll digitaalse keskkonna üle, põhjustada häireid tegevuses ja/või kahjustada tehnoloogilisi- ja infovõrke ning infrastruktuuri, mh kaitsvad ja ründavad küberoperatsioonid, mis toimuvad relvakonflikti ajal või vallandavad selle, ning küberrünnakud[2], millega varastatakse salastatud, tundlikke andmeid või intellektuaalomandit.

Tehnoloogia arenguga kaasnevad maailmatrendid, mis Eestile nii otseselt kui ka kaudselt järgneval viiel aastal mõju avaldavad, on tehnoloogia, sh generatiivse tehisintellekti kiire areng, protsesside automatiseerituse kasv, tehnoloogia kasutajakogemuse lihtsustumine, järjest suurenev (ülemaailmne) tehnoloogiasõltuvus, sh tehnoloogiasõltuvus elutähtsate

FOTO: PIXABAY.COM

[2] Termin küberrünnak on koondnimetaja ja viitab raportis igasugusele pahatahtlikule tegevusele, mis seisneb suunatud sissetungimises võõrasse arvutivõrku, et varastada või muuta andmeid või kahjustada süsteemi, st siinse raporti kontekstis võivad küberrünnaku toimepanijad ja motiivid olla mitmekesised.

teenuste tagamisel, küberturbe ekspertide kasvav puudus, pilveteenuse suurenev kasutus, küberrünnete läbiviimise kiire lihtsustumine ning riikide sõjalise võimekuse kiire arendamine kübervõimekuse suurendamise abil. Lisaks on vajalik tähelepanu pöörata ka tehisintellektist endast tulenevatele täiendavatele julgeolekuohtudele (Vlassov, 2025).

Selliste riskide võimaliku realiseerumise olulisem mõju Eestile on:

- Eesti e-riigi teenuste suuremahuline kahjustamine ja riigi toimimise usaldusväärsuse oluline langus;
- kriitilise infrastruktuuri ja elutähtsate teenuste toimepidevuse pikemaajalisem kahjustamine ning suurte elanikkonnagruppide haavatavuse suurenemine;
- riigikaitselise ja siseturvalisuse infosüsteemide suuremahuline kahjustamine ning andmekogude kompromiteerimine, mille tõttu kahjustub oluliselt ka riigi kaitsevõime ja sisejulgeoleku tagamine.

Küberspionaaži ja -sõdade käigus toimuvad globaalsed arengud ja trendid, mistõttu on Eestis oluline tähelepanu pöörata alltoodult selgitavatele teguritele.

KÜBERSPIONAAŽ JA KÜBERRÜNDED

Tehisintellekt, sh generatiivne tehisintellekt[3], omandab järjest suurema rolli küberrünnete kavandamisel, olles kiires muutumises ja võimestamas nii (küber)spionaaži, -ründeid kui ka -sõdu.

Suurandmete kasv, tehisintellekti võimekuse kiire areng ning protsesside automatiseerimise võimaluse suurenemine loob soodsa pinnase küberünnete arvu suurendamiseks ja rünnete mitmekesistumiseks. Trend, mis Eestit lähiaastatel mõjutab, on kõikide riikide võimalus kiiresti oma sõjalist võimekust suurendada ja ohud mitmekesistuvad. Tehisintellekti võimekuse kasvuga on hüppeliselt suurenenud ka allolevad ohud.

- Tehisintellekti, sh generatiivset tehisintellekti, kasutatakse küberünnete ja -spionaaži läbiviimiseks ning seda saab kasutada automaatselt süsteemi või võrgu nõrkuste tuvastamiseks ning rünnete toimepanemiseks (Data Guardian Hub, 2024). Ekspertide hinnangul võib tehisintellekti kasutus viia ka vastandumisel põhineva tehisintellekti kasutuselevõtuni (ingl *adversary AI*), mille ülesanne on süsteemi turvameetmete ülekavaldamine või uute ründestrateegiate välja töötamine. Lisaks saab tehisintellekti algoritme kasutada keerukamate sotsiaalse manipuleerimise rünnakute jaoks, näiteks sihistatud rünnakute (ingl *spear phishing*) või muude kindla sihtmärgiga rünnakute puhul, mis kasutavad infot konkreetse isiku kohta, et petta teda tundlikku teavet avaldama. Sarnaselt süsteemi ründavate meetmetega saab tehisintellekti vahendeid rakendada ka (küber)süsteemi valvamiseks (ingl *automated defense*) ja ka selline kasutusviis on kasvutrendis. Ohtudele keskendudes ei tähenda tehisintellektile delegeeritud tegevus aga mitte seda, et süsteem on turvalisem, vaid hoopis seda, et üha enam ollakse (tehnoloogiliste süsteemide turvalisuse võtmes) sõltuvad tehnoloogiast ja selle töökindlusest.

[3] Tehisintellekt on tehnoloogia, mis sisendiks saadud andmeid analüüsides jäljendab/kordab ülesannete täitmise loogikat ja täitmise tavapärast mustrit. Generatiivne tehisintellekt loob aga sisendiks saadud andmete analüüsi ja sünteesi alusel uue tulemuse ja sisu, nt tekst, pilt, audiovisuaalne materjal, aga ka (programmeerimiseks vajalik) kood.

- Tehisintellekti, eriti generatiivset tehisintellekti, kasutatakse üha enam (ka kübersõja kontekstis) pettuste ja valeinfo, sh süvavõltsingute (ingl *deepfake*) loomiseks (Mahmudov, 2023). Üks märgilisemaid süvavõltsinguid on 2022. aasta märtsis levitatud video Ukraina president Zelenskist, kes kaasmaalasi allaandmisele kutsub (Burgess, 2022). Enne USA presidendivalimisi novembris 2024 hindasid eksperdid selliseid süvavõltsinguid suureks ohuks ka demokraatlikule valimisprotsessile (Taylor, 2024). Olgugi, et see oht USA presidendivalimistel ei realiseerunud, peab arvestama järjest suureneva võimalusega, et paljud riigid ja huvigrupid üle ilma kasutavad võltsinguid ühiskondade meelsuse aktiivseks mõjutamiseks, kerksuse vähendamiseks ja demokraatlikesse protsessidesse sekkumiseks.

Tehisintellekti, sh generatiivset tehisintellekti, kasutavad ja arendavad ettevõtted keskenduvad kaitsetööstusele või laienevad kaitsetööstusesse.

Praegu on tehisintellekti kasutuselevõtt maailmas küll kiirelt kasvanud (nt suurtel andmeja keelemudelitel toimivad ettevõtte Open AI tehisintellekt ChatGPT, Microsofti Copilot või Hiina ettevõtte Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd. DeepSeek), kuid sellel sektoril ei ole õnnestunud toodete populaarsusest hoolimata leida veel viisi, kuidas selliseid tooteid pakkudes ettevõtte kasumlikkust suurendada. Kuigi paljudes eluvaldkondades on tehisintellekt mitmeid protsesse hõlbustanud, ei ole veel välja kujunenud seesugust toodet, mis tehisintellekti arendamise kulusid ettevõttele tasa teenida võimaldaks.

Samal ajal on tehisintellekti arendavad ettevõtted ja suurkorporatsioonid üha sagedamini kaasatud riikide julgeolekut tagavatesse protsessidesse, näiteks piirivalve, teabe kogumine jms julgeoleku tagamise protsessid. Riikliku võimekuse arendamine on kulukas, kuid eraettevõttest partner aitab väiksema kulu ja vaevaga riigi kaitsevõimet tõsta.[4] Järjest suurenev surve riikidele oma kaitsevõimekust tõsta – eriti Euroopa riikidele – on hea võimalus kaitsetööstuse ettevõtetele, nagu Palantir ja Anduril, kasutada salastatud sõjaväeandmeid oma tehisintellekti mudelite treenimiseks. Selleks on riigikaitsesektori näol leitud ka ostujõuline teenuse tellija.

Ühendades tehisintellekti ettevõtete sooviga leida kasutoovaid projekte ning riikide järjest suureneva vajadusega kaitsevõimet parandada, hinnatakse, et üha enam tehisintellekti ettevõtteid on sisenemas kaitsetööstusesse. Lähiaastatel on kaitsetööstuses oodata tehisintellektil põhinevate lahenduste arvu hüppelist kavu, kuid sellega kasvavad ka riiklike andmete jagamisel eraettevõtetega kaasnevad riskid, sh protsesside läbipaistvus ja turvalisus. Esmalt on riskiks koostöö või teenuse hankimine ebasõbralikelt riikidelt ja riiklikelt ettevõtetelt. Näiteks teevad mitmed Euroopa riigid jõulisi samme Hiina toodete otsese kasutamise tõkestamiseks riigikaitse ja turvalisuse valdkonnas, sh uuendatakse riigihanke protsesse. Tehnoloogia arendamise protsessid on aga keerukad ning osapooli ja allhankijaid mitmeid, mistõttu on näiteks ka Hiina osalusega ettevõtete, sh Euroopa ettevõtete, välistamine keerukas.

Teine suur risk on tehisintellekti lahendusi arendavate ettevõtete töökorralduse üha suurem sõltuvus generatiivsest tehisintellektist. Riigi ja eraettevõtte partnerlus digilahenduste arendamisel ei ole uudne. On juba tuvastatud, et tehisintellekti lahendusi arendavad ettevõtted kasutavad süsteemide loomisel kontrollimatult generatiivset tehisintellekti

[4] USA sõjavägi on alustanud mitme projektiga, mis viitavad suurele huvile kasutada ja integreerida tehisintellekti laiaulatuslikult nii lahinguvälja otsustusprotsessidesse kui ka logistikasse. Samalaadsete arendustega tegeleb aktiivselt ka Hiina RV.

(küll veel kontrollitud tingimustes), mis etteantud reegleid eirab või petab (Kantrowitz, 2025). Lisaks on süsteemide arendamisel tavapärane praktika avalikes foorumites jagatavate programmeerimiskoodide ja viipade (ingl *prompt*) kasutamine, mis võimaldab automatiseerimisel põhineva programmeerimise puhul pahatahtliku koodi integreerimist süsteemi juba selle arendamise käigus (Marcus & Hamiel, 2025).

Tehisintellektil, sh generatiivsel tehisintellektil, põhinev suurandmete analüüs võimestab kaitsetööstuse innovatsiooni.

Tehisintellekti suurandmete töötlemise võimekus on olnud suureks abiks juba nii farmakoloogias kui ka materjaliteadustes ning hinnatakse, et lähiaastatel võimestab tehisintellekt innovatsiooni veel paljudel elualadel. Siin ei saa kindlasti tähelepanuta jätta tehisintellekti võimekust toetada kaitsetööstust uudsete heidutusmeetmete väljatöötamisel, aga kahjuks ka ründemeetmete arendamisel. (O'Donnell *et al*., 2025) Kui tehisintellektil on võimekus toetada näiteks farmaatsiatööstust, siis võib sarnast võimekust eeldada ka massihävitusrelvade tootmisel. Niisuguste võimaluste kasv võimaldab (ostujõulistel) riikidel oma sõjalist võimekust kiiresti suurendada ja mitmekesistada.

Pikaajalised operatsioonid võimaldavad süsteemselt riiki ja selle elutähtsaid teenuseid nõrgestada ning (füüsilisi) rünnakuid planeerida.

Pikaajaliste küberspionaaži operatsioonide ning riiklikult toetatud toimijate kontekstis on Eestit lähiajal enim mõjutavaks trendiks eelkõige see, et küberründeid viiakse läbi riigi toel (st piisab küberründeks rahalise ressursi olemasolust) ning rünnete eesmärk on jääda võimalikult pikaks ajaks märkamatuks, et informatsiooni koguda ja süsteemi haavatavusi tuvastada. Sagedasti teostavad riiklikult toetatud küberründeid riiklikud eriteenistused (nt Venemaa GRU, Hiina Rahvavabastusarmee), kuid ründevektorite mitmekesistumine, rünnete kavandamine tehisintellekti toel ning ründed kui organiseeritud kuritegevuse uus tegevusvaldkond (mida järgnevas alapunktis selgitatakse) võib ka riigi heaks töötavate toimijate ringi muuta oluliselt mitmekesisemaks ja toimijate tuvastamise keerukamaks. Lisaks võib distantsi hoidmine toetatud toimijast olla ka riigi taotluslik valik, et rahvusvahelisi diplomaatilisi suhteid hoida.

Eesti riigiasutused ja ettevõtted on pidevalt küberrünnakute surve all. Seda survet suurendas Venemaa täiemahulise agressioonisõja algus Ukrainas 2022. aasta veebruaris. 2024. aastal registreeris Riigi Infosüsteemi Amet (RIA) Eestis seni rekordilised 6515 mõjuga küberintsidenti. Kogu maailmas registreeriti 2024. aastal 40 287 turvanõrkust, mida saab ära kasutada küberrünnakuteks. Võrdluseks, et 2015. aastal oli maailmas registreeritud turvanõrkuste arv 6487 (Riigi Infosüsteemi Amet, 2025, lk 6, 35). Seega on nii küberrünnete arv kui ka haavatavuste hulk küberruumis iga aastaga üha kasvanud, mistõttu on nii riigil, ettevõtetel kui ka eraisikutel järjest rohkem vaja küberkaitsemeetmetesse investeerida.

Viimastel aastatel on tuvastatud, et üha enam viivad küberspionaaži läbi riigi poolt toetatud toimijad. Küberspionaaž omandab järjest enam küberkuritegevuse võtteid. (Deloitte, 2025; Hitachi Cyber, 2025) Pikaajalised ja keerukad ründed (ingl *Advanced Persistent Threats, APTs*) on järjest intelligentsemad ja neid on keeruline tuvastada. Kasvanud on süsteemile omaste turvanõrkuste ekspluateerimine (ingl *zero-day exploits*) ja tarneahela ründed. Toimijate eesmärk on hankida pikaaegsete ja sihistatud võrku infiltreerumiste abil tundlikku infot, aga ka saboteerida ja halvata kriitilist taristut. Kuna info hõivamisel kasutatakse lisaks tehisintellekti võimalusi, on küberspionaaži lisandunud võimekus

kiirelt töödelda ja analüüsida suurt hulka andmeid. Andmete (sh riiklike andmete) digiteerimise maht ja avalike (ka elutähtsate) teenuste digitaalne olemus on muutnud need kübersõja kontekstis oluliseks spionaaži- ja ründesihiks. Lisaks asutuste või ettevõtete ründamisele on teabe kogumise eesmärgil küberspionaaži objektiks järjest rohkem ka üksikisikud.

RIA küberturvalisuse aastaraamatus (Riigi Infosüsteemide Amet, 2025) tõdetakse, et Hiina küberoperatsioonide võimekus ületab Venemaa oma ning Hiinaga seotud rühmitused on ilmselt kõige võimekamad ja keerulisemaid küberoperatsioone läbi viivad läänevastased jõud, mille omapäraks on nende varjatus ja laiaulatuslikkus. Hiina küberrünnakute võimekust näitab tema massiivne tegevus Taiwani vastu, kus toimub hinnanguliselt 15 000 rünnakut sekundis (vt Kaljula, 2024). Lisaks hoiatatakse, et riiklikule kontrollile alluvate ja riigi dotatsioone kasutavate Hiina ettevõtete tooted on küberrünnakute potentsiaalseks platvormiks.

Küberrünnakutest on saanud organiseeritud kuritegevuse kasvav osa.

Küberkuritegevusega saadava tulu kasv ja küberkuritegevuse valdkondade laienemine on meelitanud traditsioonilisi organiseeritud kuritegelikke grupeeringuid küberkuritegevuse turule sisenema, sh on kasvutrendis inimkaubanduse abil küberrünnakuid läbi viivate valeinfot tootvate ning levitavate rühmituste mehitamine ja jõustamine. Traditsioonilise organiseeritud kuritegelike gruppide sisenemine küberkuritegevuse valdkonda muudab ka küberkuritegevuse olemust. Näiteks grupid, kes on harjunud füüsilise kahju tekitamisega, ei pruugi heituda elutähtsa taristu ründamisel või võivad valida teenuse tellijat ideoloogilistel kaalutlustel.

Tehisintellektil põhineva uue tehnoloogia rutakas integreerimine ja küberturbespetsialistide kasvav puudus.

Tehisintellekti rutaka integreerimisega seonduvalt on Eestit lähiajal tõenäoliselt kõige enam mõjutavaks trendiks tehisintellekti integreerimisel ebapiisav ohukohtadega arvestamine. Samuti napib täiendavate turbemeetmete rakendamiseks vajalike oskustega tööjõudu.

Tehisintellektil, sh generatiivsel tehisintellektil, põhinevaid tööriistu on nende kasutusmugavuse tõttu kiirelt mitmetesse töövoogudesse integreeritud ning paljud näevad laiatarbe generatiivses tehisintellektis (nt ChatGTP, Copilot, DeepSeek) suurt tuge igapäevaste tööülesannete kiiremal täitmisel. Kuigi kasutuselevõtt on kiire, toob Maailma Majandusfoorumi raporti „Golbal Cybesecurity Outlook 2025" (World Economic Forum, 2025) kübereksperte küsitlus välja, et vaid ligikaudu kolmandikul ettevõtetest on enne tehisintellekti süsteemide integreerimist kasutusel ka turvaprotokoll, mis tehisintellekti tehnoloogia integreerimise turvalisust hindab. Teatud tööriistade, näiteks Hiina ettevõtete pakutavate teenuste puhul, on maailmapraktikas ja ka Eestis välja toodud võimalikud turvariskid, ent üldiselt ei ole tehisintellekti tööriistade kasutamine veel reguleeritud. Reguleerimine võib tunduda vähem vajalik, kui tehisintellektipõhist teenust pakub tarkvaraettevõte, mille tarkvara on niikuinii riigis, asutuses või ettevõttes juba kasutusel. Liigne usaldus tehisintellekti süsteemide kasutuselevõtul võib viia tuvastamata ja uute ohtude realiseerumiseni. Seda enam, et üheks oluliseks tulevaseks haavatavuseks peetakse justnimelt pilvetehnoloogiaid, millel põhinevad ka mitmed tehisintellekti tööriistad.

Spetsialistide koolitamine ja tööturg ei jõua järele tehnoloogia kiirele arengule ning seetõttu on nii Euroopas kui ka Eestis järjest suurem küberturbespetsialistide puudus (Euro-

pean Commission, 2024a). Eurobaromeetri 2024. aasta uuring tõi välja, et Eestis on üle kolmveerandi küberturbega tegelevatest töötajatest kasvanud sellesse rolli oma teiste tööülesannete kaudu, mitte pole palgatud spetsiifiliselt küberturbega seotud ametikohale (Euroopa keskmine on 57%). Euroopa keskmisest jääb tulemus samuti alla nii küberturbega seotud töökoha vahetuse kui ka esimese erialase töökoha näitajates (European Commission, 2024b). Lühidalt, sageli täidavad Eestis küberturbega seotud rolle inimesed, kellel ei ole selleks vastavat formaalset kvalifikatsiooni. Järjest keerukamaks muutuval küberturbemaastikul on see digitaalselt võimestatud riigis muret tekitav trend.

KÜBERSÕDA

Riikliku sidetaristu halvamine invasiivseks rünnakuks või infooperatsiooni võimestamiseks.

Kuigi ekspertide eeldatud suuremahuline sidekatkestus Ukrainas jäi 2022. aastal Venemaa invasiooni alguses ära, on Venemaa senistest taktikatest see Eestile võimalikku mõju avaldav tegevus. Nimelt oli Krimmi annekteerimisel korraldatud sidevahendite halvamine võtmetähtsusega, et Venemaa saaks samal ajal piirkonnas kontrolli haarata ja rahvusvahelise inforuumi valeinformatsiooniga üle külvata. (Pickle, 2024) Kuna see taktika on Venemaa arsenalis, tuleb Läänemeres kulgeva sidetaristu toimepidevust ning Venemaa (ja Venemaale sõbralike riikide) varilaevastiku tegevust Põhja-Balti regioonis valvsalt jälgida ja tõkestada (Loik, 2024; Muuga *et al.*, 2025).

Oluline on toonitada, et Vene eriteenistuste eesmärk on pääseda juurde riigile olulisele infole, mistõttu tuleb info kaitseks kasutada metoodiliselt hinnatud tugevaid krüptograafilisi lahendusi (Välisluureamet, 2025, lk 9). Kaitsepolitseiamet (2025, lk 38) rõhutab samuti, et küberluurega tegelevad Vene eriteenistuste üksused otsivad aktiivselt ligipääsu Eesti riigi- ja erasektori võrkudele, sh ennustavad trendid vargvõrgustike ehk kompromiteeritud seadmete kasvavat kasutamist vahelülirünneteks.

Venemaa kasutas intensiivselt eri tüüpi infooperatsioone ja kübervõimestatud infooperatsioone olulise osana hübriidsest vaenutegevusest Ukraina vastu konventsionaalset kallaletungi eskaleerivas faasis, et mõjutada strateegilist ja sõjalist-operatsioonilist keskkonda endale soodsamas suunas. Selleks viidi läbi erinevaid „häki ja avalikusta" tüüpi küberoperatsioone. Eriti ohtlikuks osutusid hävitusvara kasutamine ning rünnakud riigi oluliste teenuste, andmebaaside ja kriitilise infrastruktuuri või nende osade vastu (Savimaa ja Loik, 2023, lk 38). Samalaadsete küberoperatsioonide tõrjumiseks peab valmis olema ka Eesti nii riigi- kui ka olulist mõju omavates erasektori ettevõtetes. Väga olulise riskina on viimastel aastatel üles kerkinud merealuste ühendustega seotud kriitilise taristu haavatavus (Muuga *et al.,* 2025), sh sabotaažioht infokommunikatsiooni ja energiasüsteemide turvalisusele.

Küber-füüsiline rünne riikliku (elutähtsa) taristu halvamiseks ja tsiviilkriisi esilekutsumiseks.

Kuigi energiasõltuvus digitaalselt võimestatud Eestis ei ole uudne oht, tuleb pidevalt kasvava riskina pidada silmas ohtu energiataristule, mis ühiskonna jätkuvalt suureneva ja elektrienergial toimiva tehnoloogiasõltuvuse tõttu võib halvata digitaalselt võimestatud riigi toimimise. Ka teised elutähtsad taristud – vee- ja kanalisatsioonivõrk, transport jms – sõltuvad elektrienergia olemasolust. Tehnoloogiline suutlikkus küberrünnete

läbiviimiseks kasvab tehnoloogia arenedes, mistõttu suureneb ka taristuvastaste rünnete võimalus. Taristu rikkest tingitud tsiviilkriisi võidakse kasutada invasiooniks või (küber) sõjas edu saavutamiseks ja jõuvahekordade muutmiseks.[5]

Ründavale kübersõjale vastukaaluks on luurav kübersõda oma kübermeetmetega võimestamas konventsionaalset sõda.

Jätkuv sõjategevus Ukrainas on avanud võimaluse täpsemalt analüüsida (küber)sõja taktikaid ja domeene Venemaa tegevuse näitel. Nähtub, et kübersõda ei ole mitte niivõrd rünnakule orienteeritud, vaid peamine valdkond on luureandmete kogumine. Mõne eksperdi hinnangul on see küberruumi võimaluste „parim" kasutusviis. (Pickle, 2024) Arvestades eespool välja toodud küberspionaaži arenguid, on riiklike teenuste ja andmete küberturvalisus tulevikus veel olulisem. Spionaaži tulemusel võib lekkida informatsioon, mis ohustab otseselt riigi toime- ja kaitsevõimet ning mida on sihistatult võimalik toime- ja kaitsevõime nõrgestamiseks kasutada.

Suurtel tehnoloogiaettevõtetel, nagu Starlink, Google ja Amazon, on (küber)sõdades üha suurem roll.

Kriisiolukordades ja riikliku taristu tõrgete korral võivad suurettevõtted pakkuda riigile ja selle taristu toimimisele vajalikku abi. Partnerlus globaalsete suurettevõtetega võib olla lausa hädavajalik, et pakkuda elutähtsaid teenuseid ning toetada sõjaväge, majandust ja riigi funktsioone. Oluline on märkida, et eraettevõtted ja nende teenused on kättesaadavad kõikidele osapooltele, kelle maksejõud ja ideoloogia ettevõttega sobib, mistõttu tuleb partnerluse loomisel ja hoidmisel võtmetähtsusega ressursside ja taristule ligipääsu tagamiseks kaaluda ja maandada riske, mis selliste partnerlustega kaasnevad. See tähendab, riik võib sõltuda teenusepakkuja reeglitest, hinnapoliitikast, aga ka võimalikust teenuse katkestamisest, kui ettevõttel peaks selleks soov tekkima. Tegemist on nn võtmemaastikega (ingl *key terrain*) kübermaastikul. Riiklikud partnerlused ja kokkulepped rahvusvaheliste IT-ettevõtetega muutuvad üha olulisemaks, mistõttu tuleks ka Eestil lähiajal hoolikalt hinnata teiste riikide tegevust ja enda positsioon kindlustada.

Tehnoloogilise arengu tõttu on kübersõja olemus muutumas üha komplekssemaks ja keerulisemalt tuvastatavaks ning on läbiviimise lihtsustumise tõttu järjest tõenäolisem, mistõttu on Eestil vaja sellekohast kriitilist analüüsivõimekust tõsta.

Küber- ja füüsiliste meetmete kasutamine sõjategevuses ei ole seni vastanud analüütikute prognoosile (vt Pickle, 2024), kus tegevus ühes domeenis võimestab otseselt teist, mistõttu on oluline analüüsida, missugused võiksid olla alternatiivsed kübersõja viisid (sh kübertegevus võimestamas füüsilist domeeni või kübertegevus ette valmistamas füüsilise domeeni rünnakut). Kübersõdade täiendav analüüs on Eestile kriitilise tähtsusega, sest naaberriik Venemaa on korduvalt näidanud küberrünnete abil (demokraatliku) ühiskonna stabiilse toimepidevuse ohustamise võimekust. Kübermeetmete kasutamise motivatsiooni analüüsides tuleb silmas pidada peamiselt kaht senist trendi.

- Ukraina sõjast nähtub, et kübertegevustega üritatakse inforuumis sihtgruppide meelsust muuta ja kontrollida ning strateegilist initsiatiivi saavutada ja hoida.

---

[5] Maailma Majandusfoorumi uuringu andmetel hindas vaid 50% vastanud ekspertidest, et on kindlad või väga kindlad, et nende organisatsioon või koduriik on hästi ette valmistatud kriitilist infrastruktuuri ründavate suuremate küberintsidentide ennetamiseks ja nendega hakkama saamiseks (World Economic Forum, 2025, p. 6).

- Kübertegevused ilma füüsilise ründeta ei ole osutunud piisavaks, et territooriumi üle füüsiline kontroll saavutada. Küberründe ja füüsilise ründe koordineerimine on aga osutunud Ukraina sõja näitel väga keerukaks.

Kübersõjas ei toimu sõjategevus ainuüksi kahe riigi vahel, vaid kübrrünnakutesse kaasatakse ka teisi osapooli.

Kui konventsionaalses sõjas on vastasseis riikide relvajõudude vahel peamine, siis kübersõjas on tõenäoliselt võimalikke osapooli ja toetavaid või palgatud jõude rohkem. Riigi sõjalise võimekuse suurendamine teiste osapoolte kaasamise abil on trend, mis võib Eestit lähiaastatel mõjutada. Riiklikku võimekust (küber)sõja pidamiseks ei saa hinnata pelgalt riiklike üksuste suuruse alusel, vaid arvestada tuleb ka võimalike kaastöötajatega. See omakorda tähendab, et küberründeid riigi ja taristu vastu tuleb sarnaselt hinnata: tegemist ei pruugi olla eri toimijate eraldiseisvate rünnakutega, vaid süsteemse ja koordineeritud riigi vastu suunatud rünnakuga, mille viivad läbi ründavat riiki toetavad ja värvatud toimijad (Pickle, 2024).

VÄÄRINFO JA DESINFORMATSIOON

Teiseks kõige suurema võimaliku mõjuga riskiks Eesti jaoks hindasid Eesti eksperdid väärinfo ja desinformatsiooni levikuga seonduvaid ohte. Selle riski all on silmas peetud pidevat laialdast meediavõrgustike kaudu manipuleeriva teabe levitamist nii riiklike kui ka mitteriiklike toimijate poolt, et kallutada avalikku arvamust olulisel määral faktide ja autoriteedi usaldamatuse suunas, sealhulgas valeinformatsiooni ja fabritseeritud sisu kaudu.

Karistusseadustikuga (seisuga 25.07.2025) on Eesti inforuumis kriminaliseeritud sõjale või muul viisil relvajõu kasutamisele üleskutsumine, kui sellega eiratakse rahvusvahelise õiguse üldtunnustatud põhimõtteid (KaRS § 92, Sõjapropaganda). Samuti on kriminaliseeritud vaenu õhutamine (KaRS § 151), st tegevused, millega on avalikult kutsutud üles vihkamisele, vägivallale või diskrimineerimisele seoses rahvuse, rassi, nahavärvi, soo,

FOTO: MICROSOFT COPILOT, 2025

keele, päritolu, usutunnistuse, seksuaalse sättumuse, poliitiliste veendumuste või varalise või sotsiaalse seisundiga, kui sellega on põhjustatud oht isiku elule, tervisele või varale. Kriminaalkorras karistatav on ka rahvusvahelise kuriteo toetamine ja õigustamine (KaRS § 151[1]), st agressiooniakti, genotsiidi, inimsusevastase kuriteo või sõjakuriteo toimepanemisega seotud sümboli avalik eksponeerimine neid tegusid toetaval või õigustaval viisil ja avalik üleskutse kuriteo toimepanemisele Eesti Vabariigi vastu (KaRS § 236). Nende koosseisude künnisest allapoole jääva halli ala vaenulikud mõjutusoperatsioonid, sh Eesti ja Euroopa Liidu jurisdiktsioonist väljapoole jäävad mõjutustegevuse allikad, nõuavad üha rohkem tähelepanu ning aktiivseid vastumeetmeid, nagu infooperatsioonide sisu ja allikate avalikustamine, meediasanktsioonide arendamine ning jõustamine.

Võimaliku vaenuliku mõjutustegevuse olulisem negatiivne mõju Eestile on järgmine:

- väheneb ühiskonna usaldus demokraatlike institutsioonide legitiimsuse ja teovõime suhtes;
- süveneb ühiskonna polariseerumine, mis loob omakorda soodsa pinnase teatud gruppide radikaliseerumiseks;
- kahaneb usaldusväärsus Eesti välis- ja julgeolekupoliitika rahvusvahelise edukuse ja teovõime suhtes.

Hübriidohtude käsitlustes on hakatud üha enam tähelepanu pöörama demokraatlike poliitiliste süsteemide ja otsustusprotsesside haavatavustele vaenulike manipulatsioonikatsete suhtes, eriti inforuumis (Savimaa *et al.,* 2024, lk 8). Venemaa praegune režiim on teinud inforuumi sihipärasest mõjutamisest olulise osa oma strateegilisest ründerelvastusest. Seda kasutatakse aktiivselt nii riigisiseselt kui ka rahvusvahelisel tasandil, sh demokraatlikesse valimistesse sekkumisel (vt Duffy, Harbath, 2024; Zygar, 2024). Praeguse poliitilise süsteemi jätkudes Venemaal oleks naiivne eeldada, et tema agressiivne mõjusfääride strateegia naabrite ja nende liitlaste suhtes muutuks (Loik, 2022). Pigem on vastupidi, Kremli desinformatsioonivõtted muutuvad üha mitmekesisemaks. Selline areng eeldab lääneriikidelt ja demokraatlikelt institutsioonidelt suuremat strateegilist tähelepanu, vastupanuvõime tugevdamist ning selgeid poliitikasuundi, et säilitada demokraatlike otsustusprotsesside usaldusväärsus ja vastupanuvõime intensiivse infosõja tingimustes. Oluline on tugevdada ka Euroopa Liidu ja NATO koostööd hübriidohtude valdkonnas (Zandee *et al*., 2022).

Väärinfo ja desinformatsiooni leviku kontekstis loovad tehisintellekti rakendamisvõimaluste innovatsioonid hübriidsete operatsioonide planeerimisel (disainimisel) ja infokeskkonnas läbiviimisel üha uusi strateegilisi eeliseid, dilemmasid ja julgeolekuprobleeme. Kaitsepolitseiamet (2025, lk 43) prognoosib tehisintellekti üha suuremat rolli manipuleerivates mõjutusoperatsioonides, mis on suunatud valimiste jt demokraatlike protsesside häirimisele. Sellised infooperatsioonid muutuvad üha keerukamateks ja laialdasemateks. **Tehisintellekti kasutamisel infooperatsioonides avarduvad riskid sattuda nii massiivsemate, kiiremate kui ka täpsemini disainitud vaenulike mõjutusoperatsioonide ja kübervõimestatud infooperatsioonide sihtmärgiks**. Ühtlasi suureneb vaenulike toimijate luure- ja analüüsivõime keerukate süsteemide haavatavuste tuvastamiseks ning eskaleerivate kaskaadiefektide esilekutsumiseks.

Eesti julgeolekuasutuste (Kaitsepolitseiamet ja Välisluureamet) viimaste aastate raportites ja aastaraamatutes on järjekindlalt tähelepanu pööratud ka Hiinast lähtuvatele julgeolekuohtudele. Kaitsepolitsei aastaraamatutes tõstetakse ohutegurina esile Hiina RV saatkonna ja Hiina kogukondade esindajate tegevust Eesti avaliku arvamuse mõjutami-

seks ja Hiinale soodsamate hoiakute loomiseks. Aastaraamatus 2023–2024 juhitakse seejuures tähelepanu, et võrreldes Venemaaga on Hiina luure laiapõhjalisem ja intensiivsem (Kaitsepolitseiamet, 2024, lk 21), see hõlmab kõiki valdkondi, alates sõjaväe-, tehnilisest ja teadusspionaažist küberspionaaži ja -rünnakute ning pehme jõu (kultuurikoostöö) vahenditeni. Olulisel kohal on aktiivne ja passiivne mõjutustegevus ning mõjuagentide värbamine kohalike elanike seast.

Hiina on ehitanud üles ülemaailmse luurevõrgustiku, mis rakendab Hiina Kommunistliku Partei käepikendusena tegutsevat ja selle rahvusvaheliste suhete osakonna juhitud Ühisrinnet (ingl *United Front*) ning millega teevad koostööd paljud välismaal viibivad Hiina RV kodanikud. Austraalia analüütiku Alex Joske sõnul keskendub see muu hulgas „… mõjupositsioonidel olevatele isikutele või neile, kes väidavad, et esindavad ühiskonna peamisi segmente – rahvuskogukondade liidreid, ärimagnaate, usutegelasi jne“ (Joske, 2022, lk 31; Läänemets, 2024, lk 21–22). Ka Eestis on selline mõjutustegevus olnud üsna aktiivne, nagu näitab oma uurimuses Frank Jüris, kes väidab, et „kuigi Hiina edu on olnud osaline, on tema mõjutustegevus jõudnud Eesti poliitika kõrgeimatele tasanditele“ (Jüris 2023, lk 3).

2024. aastal pälvis Eestis enim tähelepanu Riigikogu Eesti-Hiina parlamendirühma osaliselt Hiina rahastatud visiit Hiinasse ja sellele järgnenud ühiskondlik debatt, millesse sekkus ka Hiina suursaatkond (Madsen, 2024). Kuna Eesti avalikkuse teadlikkus ja kriitiline suhtumine Hiina mõjutustegevusse on kasvanud, on Hiina saatkond suunanud oma tegevuse maakondadesse, korraldades seal kohtumisi ja kultuuriüritusi kohalikele omavalitsustele ja haridusasutustele ning ettevõtjatele, mis teenivad eeskätt propagandaeesmärke (Lomp, 2025). Ka Kaitsepolitseiamet on seisukohal, et kuna Hiina ei ole sõbralik riik ja on orienteeritud pigem koostööle meile vaenuliku Venemaaga, tuleb kõiki Hiina tegevusi Eestis vaadelda läbi julgeolekuprisma, „kuna ka Hiina ise vaatab kõiki eluvaldkondi just nimelt julgeoleku- ja parteiaparaadi võimulpüsimise vaatenurgast“ (Kaitsepolitseiamet, 2025, lk 33).

RIIKIDEVAHELISED RELVASTATUD KONFLIKTID

Kolmandaks kõige suurema võimaliku mõjuga riskiks Eesti julgeolekule hindasid Eesti eksperdid riikidevahelise relvastatud konflikti ohtu. Selle riski all on silmas peetud kahe- või mitmepoolse jõu kasutamist riikide vahel ja/või riigi ja valitsusväliste osalejate vahel, sageli ideoloogiliste, poliitiliste või religioossete eesmärkidega, mis väljendub sõjana ja/või organiseeritud, kestva vägivallana (sh aktiivne sõjategevus, sissisõjad, kodusõjad, terrorism, genotsiidid ja atentaadid).

Selliste riskide võimaliku realiseerumise suurim mõju Eestile võib olla järgmine:

- poliitiline polariseerumine ja konfliktide kiire eskaleerumine;
- vaenuliku mõjutustegevuse kasv;
- ohu kasv riigi põhiseaduslikule korrale ja territoriaalsele terviklikkusele.

Riikidevaheliste või riikide ja mitteriiklike struktuuride vaheliste sõjaliste konfliktidega kaasnevad ohud Eestile on erinevad. Eesti julgeolekukontekstis on jätkuvalt ohuks nii

FOTO: STOCKCAKE.COM

Venemaa agressioonisõda Ukrainas kui ka Lähis-Idas toimuvad relvakonfliktid, mis on toonud kaasa polariseerumist ja radikaliseerumist ka Eestis. Riikidevahelise relvastatud konflikti, aga samuti muu relvastatud konflikti mõju Eesti sisejulgeolekule sõltub konfliktiga seotud kogukonna suurusest ning välistegutseja mõjust sellele. Kõige suurema mõjuga stsenaariumiks Eesti jaoks võib pidada niisuguste konfliktide esinemist meie lähipiirkonnas.

Relvastatud konfliktid on tänapäeval sageli osa laiemast hübriidkonfliktist, kus lisaks vahetule kineetilisele kontaktile osapoolte vahel toimub varisõda kolmandate riikide territooriumil, kus kasutatakse muu hulgas kohalikke kuritegeliku taustaga isikuid või internetis värvatud äärmuslasi. Oma eesmärkide saavutamiseks kolmandates riikides on Iraani, Venemaa ja Hiina luureasutused kasutanud üha enam kuritegelikku maailma nii füüsiliste kui ka küberrünnakute ja desinformatsioonikampaaniate läbiviimisel (DOJ, 2023; Kaitsepolitseiamet, 2024; Kaitsepolitseiamet, 2025; Europol SOCTA, 2025; ISCP, 2025; Jones, 2025; PST, 2025).

Eesti olukorda puudutavas ohuhinnangus on oluline jälgida arenguid Lähis-Idas ja Euroopas.

Araabia Kevade ja Süüria kodusõjaga kaasnenud rändekriis aastatel 2015–2016 näitas, et ka suhteliselt lühiajalistel vägivallalainetel Lähis-Idas või Põhja-Aafrikas on pikaajaline mõju Euroopa Liidu liikmesriikidele. Eelkõige langeb väga suure surve alla piiriturvalisus ja võime tulla toime suuremahulise irregulaarse rändesurvega. Lisaks võivad need tähendada ka reisimist konfliktipiirkondadesse, et osaleda sõjategevuses terroristlike režiimide ridades, samuti konfliktis osalevate terroristlike režiimide ja rühmituste rahalist toetamist või terroristlikku propagandat. Ohuallikaks on ka võimalikud terroristlikud üksikründajad. On suur tõenäosus, et Venemaa kasutab sõjalise konflikti situatsioone nii Läänemaailma kui ka Eesti ühiskonna lõhestamiseks.

Riiklike osalejatega konfliktid suurendavad terrorismiohtu ka Euroopas.

Riikidevahelised relvastatud konfliktid mõjutavad sageli terrorismitrende: need võivad kujundada äärmuslikke ideoloogiaid, soodustada uute liitude tekkimist ja mõjutada rünnakutaktikaid. Sõjalised konfliktid võivad toimida päästikuna radikaliseerumisele, pakkuda soodsat pinnast äärmuslike vaadete levikuks ja soodustada välisvõitlejate liikumist konfliktipiirkondadesse. Samuti võivad need konfliktid tekitada ühiskondlikku polariseerumist ka nendes riikides, mis asuvad sõjategevusest geograafiliselt kaugel ega ole otseselt sõjategevusest mõjutatud.

Riikidevaheliste relvastatud konfliktidega kaasneb sageli ka uudsete sõjatehnoloogiate kiirenenud kasutuselevõtt ja levik. See dünaamika tekitab näiteks droonisõjas märkimisväärseid julgeolekuprobleeme seoses teadmiste ja võimete võimaliku jõudmisega valitsusväliste osalejateni. Praeguseks on terroristlikud organisatsioonid ja rahvusvahelised kuritegelikud kartellid näidanud üles kasvavat huvi droonisõja oskusteabe omandamise vastu lahinguväljal (Altman, 2025; Höller, 2025). Vägivaldsete äärmuslaste (sh üksiktegutsejate) võimalikud rünnakud laiatarbedroonidega on kasvav terrorismioht (Hambling, 2025; Rassler & Veilleux-Lepage, 2025).

Terrorismivastased meetmed lääneriikides ja mujal ning regionaalne koostöö riikide vahel on oluline terroristlike rünnakute ja nende mahitamise tõkestamisel. See on vähendanud rahvusvaheliste terroristlike organisatsioonide võimekust viia läbi rünnakuid riigipiirideüleselt. Piiriülene on ka terroristlik ja terrorismi õigustav propaganda internetis,

mille kättesaadavus püsib probleemina terrorismivastases võitluses ka järgnevatel aastatel. Seda võimendavad uued tehnoloogilised lahendused, mis muudavad sellise propaganda suhtes haavatavamaks üha enam varateismelisi.

Venemaa sõjaga Ukraina vastu on kaasnenud Venemaa ja Hiina laiem läänevastane hübriidsõda.

Lisaks desinformatsioonile ja mõjutustegevusele on selles oma koht ka Venemaa eriteenistuste või kuritegeliku maailma poolt nn allhankena läbiviidud operatsioonidel Euroopas, sh rünnakutel Venemaa-kriitiliste poliitikute ja poliitiliste oponentide vastu, vandaalitsemistel, süütamistel ja muudel sabotaažiaktidel, sh oluliste infrastruktuuriobjektide vastu (Edwards & Seidenstein, 2025). Selles sõjas on olnud oma roll ka Hiinal, kes on Venemaa toetaja ning deklareerinud ennast varjamatult tema strateegilise partnerina ja võimendanud nii siseriiklikult kui ka rahvusvahelisel tasandil Venemaa agendat. Hiina majanduslik ja poliitiline toetus Venemaale ning sõjaline koostöö Venemaaga võimaldab Venemaal sõda jätkata, mis on otsene ja käegakatsutav Hiinast lähtuv julgeolekuoht Eestile ja kogu Euroopale. Venemaa partnerluse ja oma varasema näilise neutraalsusega Venemaa-Ukraina sõjas peab Hiina eeskätt silmas enda huvisid mõjuvõimu suurendamiseks kogu maailmas (vt Läänemets, 2023). Samas on Hiina välisminister avalikult väljendanud seisukohta, et Hiina ei saa lubada Venemaa kaotust Ukraina sõjas (Walsh, 2025).

Kui Hiina peaks lähiajal tegelikult ründama Taiwani ja vallandama India-Vaikse ookeani regioonis uue sõja (mis vaatamata pingete tõusule regioonis ja Pekingi sõjakale retoorikale on paljude ekspertide arvates siiski pigem vähetõenäoline; vt Läänemets, 2022; Adlakha, 2023; Roy, 2024), millesse sekkuksid USA ja tema liitlased, põhjustaks see ettearvamatuid tagajärgi kogu maailmas, sh sõjaolukorra eskaleerumist kogu India-Vaikse ookeani (Indo-Pacific) regioonis ja sellest tingitud Venemaa surve tõenäolist suurenemist Euroopas. Eesti julgeolekuolukorrale avaldaks see kindlasti mõju, eelkõige sõjast tingitud tarneahelate võimaliku katkemise tõttu, mis võivad tekitada teatud tarbekaupade puuduse ning katkestusi seadmete ja tehnoloogiate tarnetes strateegiliselt olulistele rajatistele (päikese- ja tuulepargid energia tootmiseks jm).

Laiemas terrorismitrendis võib eeldada, et vägivaldne islamiäärmuslus püsib suurima globaalse terrorismi ohuna.

Järgnevatel aastatel jäävad terrorismi mõjutama poliitilised ja sõjalised arengud Lähis-Idas. Lähitulevik näitab, milliseks kujuneb Süüria uus islamistlik režiim ja selle piirkondlik positsioon ning milline saab olema Türgi roll Süüria sündmustes. Seniste trendide põhjal võib eeldada, et järgnevatel aastatel kujutab suurimat terrorismiohtu nii Euroopas kui ka globaalselt džihadism, vägivaldne islamism/islamiäärmuslus (Europol TESAT, 2025; GTI, 2025). Terrorismioht Euroopas võib kasvada, kui mõni terroristlik rühmitus kehtestab end mingil territooriumil riigina, mis võib kujuneda terrorismi tõmbekeskuseks ka Euroopa elanike jaoks (vrdl ISIS aastatel 2014–2019) (Europol TESAT, 2025). Eeldada võib, et läääneriikides viivad terroristlikke rünnakuid läbi üksiktegutsejad, kes on radikaliseerunud internetis ning saavad innustust terroristlikust ideoloogiast ja propagandamaterjalidest, ilma ametliku või vahetu sidemeta terroristliku rühmaga (Europol TESAT, 2024).

GEOÖKONOOMILINE VASTASSEIS

Neljas kõige suurema võimaliku mõjuga risk Eesti jaoks oli Eesti ekspertide hinnangul geoökonoomilise vastasseisu oht. Selle riski all on silmas peetud majanduslike mõjutusvahendite kasutamist globaalsete või piirkondlike võimude poolt, et kujundada ümber riikidevahelist majanduslikku suhtlust, piirates kaupade, teadmiste, teenuste või tehnoloogiate liikumist ja levikut, et suurendada iseseisvust, piirata geopoliitilisi konkurente ja/või tugevdada mõjusfääri (näiteks valuutameetmed, investeeringute kontroll, sanktsioonid, riigiabi ja subsiidiumid ning kaubanduskontroll).

Selliste riskide võimaliku realiseerumise suurim mõju Eestile on järgmine:

- Ameerika Ühendriikide raskesti ennustatava ja ebastabiilse välispoliitika negatiivne mõju Eesti majandusele;
- Eesti jaoks oluliste tarneahelate häired;
- Euroopa Liidu ja Ameerika Ühendriikide poolt Venemaa (ja Valgevene) vastu kehtestatud sanktsioonide otsene ja kaudne mõju Eesti majandusele.

FOTO: MICROSOFT COPILOT, 2025

Geoökonoomiline vastasseis süveneb ja kujundab ümber globaalset jõutasakaalu.

Järgnevatel aastatel seavad jõudude tasakaalu maailmas paika kontrollihoovad maailma majanduse vereringe üle: andmekeskused, kiibitehased, koobalti leiukohad, transpordikoridorid ning eeskätt reeglid, mis nende kasutamist suunavad. Washington (koos EL-i) ja Peking (koos pidevalt laieneva BRICS-i blokiga) kindlustavad juba praegu eraldiseisvaid tehnoloogia- ja ressursisfääre. Ülemvõim saab kuuluma koalitsioonile, kes suudab tarneahelaid, standardirežiime ja turupositsioone kõige osavamalt ära kasutada. Teisalt olukorras, kus tehisintellektist on saamas peamine majandusarengu vedur, on sõjaline jõud selle väärtuspõhiselt jaotuva majandussüsteemi kaitsmisel samuti oluline.

Ameerika Ühendriigid annavad regulaarselt mitmetähenduslikke majanduspoliitilisi sõnumeid.

USA president Donald Trump käsitleb USA kehtestatavaid tariife kui karistuslikku meedet, kuid tema algatused on küsitavad. Praktikas on selline tegevus juba toonud kaasa segaduse globaalses majanduses, mille vastumeetmena püüavad kõik riigid, sh (endised) liitlased jõuda parimate individuaalsete kokkulepeteni, kuid selle taustal soovitakse oma majanduselu muuta Ameerika Ühendriikidest võimalikult vähem sõltuvaks (Manak, *et al.,* 2025; Puri, 2025). Selle tagajärjeks on muu hulgas Ameerika dollari kui rahvusvahelise majanduselu baasvaluuta tähtsuse vähenemine ja naftahindade suur kõikumine.

Ameerika Ühendriikide poolt president Trumpi initsiatiivil kehtestatud kaitsetollide otsene mõju Eesti majandusele tuleneb eelkõige meie sõltuvusest rahvusvahelise kaubanduse ja kaubanduspartnerite käekäigust. Kuigi Eesti ja USA kaubanduslikud otsesidemed, v.a kaitsetööstus, on suhteliselt marginaalsed, on maailmaturul valitseva ebastabiilsuse negatiivne mõju nii Euroopa Liidu kui ka Eesti majandusele olemas. Seda aitavad kompenseerida Euroopa Liidu kehtestatavad vastumeetmed, mille maht ja ulatus selgub siis, kui saavad selgeks Ameerika konkreetsed sammud. Samas on oluline teadvustada EL-i üldist sõltuvust impordist ja globaalsetest tarneahelatest ning jälgida Hiina mõju võimalikku suurenemist Euroopas.

Hiina kasutab majandus- ja kaubandussõltuvust üha enam teiste riikide poliitilise mõjutamise vahendina.

Hiinast lähtuv julgeolekurisk geoökonoomika valdkonnas seisneb eelkõige selles, kui suures sõltuvuses ollakse edaspidi Hiina strateegilistest toorainetest, tehnoloogiatest, investeeringutest ja tarbekaupadest. Hiina impordi maht võib hakata sõltuma Hiina ja USA omavahelise kaubavahetuse tariifidest. Kui Hiina ei saa kõrgete tariifide tõttu enam endises mahus USA-sse kaupu eksportida, hakkab ta otsima uusi turge oma kaupade jaoks, eelkõige küll Aasias, aga tõenäoliselt ka Euroopas, sh Eestis. Eesti võib sellises olukorras eelistada odavamate Hiina kaupade sissevoolu suurenemisest, sest kõrgema hinnaga lääne kaubad ei ole konkurentsivõimelised. Seda eelkõige just Eesti järsult kasvanud elukallidusest tingitud ostujõu vähenemisest ja suurenenud sotsiaal-majanduslikust lõhest, mis tuleneb suuresti maksukoormuse kasvust ning vajadusest suunata ressurssi pikemaajaliste majandusprioriteetide asemel kiires tempos riigi sõjalise kaitsevalmiduse suurendamiseks.

Teatud piirist alates võib selline kaubandussõltuvus suurendada ka poliitilist sõltuvust: populistidest poliitikud võivad rahva toimetuleku parandamist ettekäändeks tuues hakata ajama praegusest märksa Hiina-sõbralikumat poliitikat, nagu see on toimunud mitmes Ida- ja Kagu-Euroopa riigis (näiteks Ungaris ja Serbias), mille valitsus on olnud läbivalt

Hiina-sõbralik ja kuhu viimane on teinud suuri investeeringuid (Rohac, 2024, lk 3–4). Just need riigid eristuvad Kesk- ja Ida-Euroopa riikide seas oma Hiina-sõbralikkuse poolest, mis on ilmselgelt korrelatsioonis ka nende Vene-sõbralikkusega.

Eestil on selles vallas väike mänguruum, sest sõltume liiga palju suurriikide omavahelisest kaubanduspoliitikast. Kui USA ja Hiina jõuavad kaubandustollide osas kokkuleppele (mis on tõenäoline) nii, et see ei muuda liiga palju üleilmseid tarneahelaid, siis Eesti olukord eksportkaupadega varustatuse osas meile vastuvõetavate hindadega ei pruugi palju muutuda.

Euroopa Liidu ja USA sanktsioonid Venemaa suhtes vajavad tõhusamat jõustamist.

Euroopa Liit kehtestas 18. juulil 2025 Venemaa vastu 18. sanktsioonipaketi (19. on kehtestamisel), mille keskse meetmena langetatakse Venemaa nafta hinnalagi 60 dollarilt 47,6 dollarile barreli kohta. Hinnalae ülevaatus hakkab toimuma iga kuue kuu tagant, et see oleks alati 15% madalam keskmisest turuhinnast (Eesti Vabariigi Välisministeerium, 2025). Euroopa Liit on võtnud vastu põhimõttelise otsuse loobuda täielikult Venemaalt pärit energiakandjate (nafta, gaas, uraan) kasutamisest 2027. aastaks.

Eesti majandust puudutab 2027. aasta muutus otseselt suhteliselt vähe, sest Eesti otsesed majandussidemed Venemaaga olid juba enne aktiivse vastasseisu teket aasta-aastalt vähenenud. Venemaa naftat ja gaasi ei ole Eesti turule otse juba aastaid imporditud (näiteks Lukoil lahkus siinselt jaemüügiturult juba aastal 2003), kuid Euroopa Liidu turuolukorda arvestades on alust uskuda, et endiselt võib siinsetest naftatoodetest mingi osa olla algselt pärit Venemaalt (Suzan & Bounfour, 2023). Laiemas plaanis on Euroopa Liidu tasandil teadvustatud vajadust tõhustada sanktsioonide jõustamist, mis nõuab liikmesriikide pädevatelt ametkondadelt lisaressurssi. 24. aprillil 2024 võtsid Euroopa Parlament ja nõukogu vastu direktiivi (EL) 2024/1226 EL-i piiravate meetmete rikkumise eest määratavate karistuste määratlemise kohta, mis sätestab liikmesriikide kohustuse kriminaliseerida direktiivis määratud tegevused oma siseriikliku õiguse alusel. Peaasjalikult tuleb harmoneerida kriminaalkaristused varade külmutamata jätmise, reisikeeldude ja relvaembargode rikkumise, keelatud või piiratud majandus- ja finantsteenuste osutamise ning sanktsioneeritud varade kohta valeandmete esitamise eest (Bonifassi & Bastien, 2025).

Kokkuvõttes tuleb nentida, et maailm on sisenenud geoökonoomilises tähenduses ebamäärasuse ja ebastabiilsuse etappi. Euroopa ja Ameerika vaheline kasvanud majanduslik vastuolu on loodetavasti ajutine ja mööduv ning toob pikemas perspektiivis kaasa hoopis liitlassuhete uuenemise ja tugevnemise. Eesti on enda valiku läänemaailma kuulumise kasuks teinud juba ammu ja praegu pole vähimatki põhjust selle ümbervaatamiseks. Samas tuleks praeguseid tendentse käsitleda mitte niivõrd probleemidena, vaid hoopis väljakutsete ja võimalustena Eesti ja läänemaailma (eeskätt Euroopa Liidu riikide) majanduselu paremaks integreerimiseks, mis peaks tagama edaspidise stabiilse sotsiaal-majandusliku arengu Eestis. Eesti majanduse suhteline väiksus ja sellest tulenev paindlikkus peaks võimaldama kiiret kohanemist ning sujuvat ümberorienteerumist muutuvate turgude ja tootmise puhul.

ÜHISKONNA POLARISEERUMINE

Viiendaks kõige suurema võimaliku mõjuga riskiks Eesti jaoks hindasid Eesti eksperdid ühiskonna polariseerumisega seonduvaid ohte. Selle riski all on silmas peetud ideoloogilisi ja kultuurilisi lahkarvamusi kogukondades ja kogukondade vahel, mis toovad kaasa sotsiaalse stabiilsuse languse, otsuste langetamise võimetuse, majanduslikud häired ja kasvava poliitilise polariseerumise.

Selliste riskide võimaliku realiseerumise suurim mõju Eestile on järgmine:

- poliitilisest polariseerumisest tulenev otsustusvõimetus riigi majandusliku stabiilsuse tagamisel;
- suurenenud lõhestumine kogukondade vahel, tekitades sotsiaalse ebastabiilsuse kasvu;
- investeerimiskeskkonna ja tarbijakäitumise negatiivsed muutused ning ebakindluse kasv.

FOTO: MICROSOFT COPILOT, 2025

Maailmavaateline polariseerumine, kasvav kärepopulism ja tegeliku kaasatuse vähenemine on lääne demokraatiate 21. sajandi esimesel veerandil struktuurne väljakutse (Borbáth *et. al*., 2023; Serani, 2025). Polariseerumine on väärtuskonflikt, mida on ühtlasi võimendanud sotsiaalmeedia (Yarchi, *et al*., 2020; Kubin & von Sikorski, 2021) ja eeldatavalt üha enam ka tehisaru manipulatiivsed rakendused. Viimase kümnendi jooksul on lääne ühiskonnad liikunud läbi erinevate kriiside, millega on kaasnenud ühiskondlik ja poliitiline polariseerumine. Rändekriisid, kliimaärevus, pandeemia, Venemaa agressioonisõda Ukrainas, Hamasi ja Iisraeli vastasseis Gazas ning identiteediõigused on vaid lai pintslitõmme vastandumist võimendavatest teemadest nii poliitilisel, ühiskondlikul kui ka kultuurilisel tasandil.

Lähiaastatel on põhjust eeldada seisukohtade, hoiakute ja väärtuste äärmuslikuks muutumist ja vastandumist eri valdkondades.

Prognoosida võib, et järgnevatel aastatel süveneb lääne demokraatiates ühiskondlik-poliitiline polariseerumine nii globaalsete kui ka lokaalsete kriiside tõttu. Kiired tehnoloogilised, geopoliitilised ja ühiskondlik-kultuurilised muutused on võimendanud väärtuskonflikti. Vaenulike riiklike ja mitteriiklike välistoimijate eesmärk on võimendada ühiskonnas olemasolevaid vastandumisi, vajaduse korral toetades ka vastanduvaid arvamusi ja äärmusrühmi.

Hübriidsõjas lääne ühtsuse õõnestamiseks kombineeritakse küber-, kuritegelikke ja kognitiivseid taktikaid. Demokraatlike instutsioonide ja meedia usaldusväärsust õõnestatakse tehisintellektipõhise desinformatsiooniga. Interneti kajakambrid ja algoritmid õõnestavad ühiskondlikku sidusust ning loovad või võimendavad polariseerumist ühiskonnas. Võimust ja rahvast võõrandumise protsesse (nt ääremaastumine) kasutavad ära (liberaalsele) demokraatiale vastanduvad erinevates maailmavaatelistes (sh poliitilistes) äärmustes tegutsejad. Populism on muutumas peavooluks kogu poliitilises spektris. Läänemaailmas püsivad polariseeriva tegurina arvamused sisserände ja integratsiooniga seotud küsimustes.

Prognoosi kohaselt süvendab tehisintellekti sihipärane kasutamine vaenulike tegutsejate poolt ühiskondlikku polariseerumist veelgi aastaks 2030.

Tehisintellekti kasutuselevõtt on toonud kaasa paradigma muutuse ka väärinfo levitamisel ja narratiivide kujundamisel. Süvavõltsingud, sünteetiline meedia ja algoritmipõhine hüperpersonaalne propaganda hägustavad piiri autentse ja manipuleeritud teabe vahel ning süvendavad juba olemasolevat polariseerumist. Infosõdades võivad isegi veenvad vastunarratiivid uppuda tehisintellekti loodud sisu massiivsesse kakofooniasse. Demokraatlike institutsioonide ja meedia usaldusväärsuse küsitavuse kaudu võib see ohustada olemasoleva avaliku diskursuse alustalasid.

Konfliktinarratiive (nt globaalne džihaad, lääne rõhumine, Venemaa vastupanu) tarbitakse kiiresti TikToki, YouTube Shortsi, Discordi ja Telegrami kaudu (Shin & Jitkajornwanich, 2024). Platvormid võimendavad emotsionaalselt laetud sisu, mis on sageli modereerimata. Internetikeskkonnad on jätkuvalt oluline radikaliseerumise kanal äärmuslikesse ideoloogiatesse. Kasvav probleem on varateismeliste radikaliseerumine vägivallaideoloogiatesse. Aastal 2024 oli Euroopas terrorismisüüdistusega kinnipeetutest 16% vanuses 12 kuni 17 eluaastat (Europol TESAT, 2025).

Üha nooremate elanike radikaliseerumine äärmuslikesse maailmavaadetesse jääb probleemiks veel järgnevateks aastateks. Noored on äärmuslike ideoloogiate suhtes haava-

tavad, kuna nad puutuvad reguleerimata veebipõhiste subkultuuride kaudu üha enam kokku äärmusliku sisu ja vandenõuteooriatega (OECD, 2023). Haavatavust ja vastuvõtlikkust suurendavad noorte vaimse tervise probleemid ning eraldatus ja kuuluvustunde puudumine. Noori manipuleeritakse usaldamatuse ja vimma tekitamisega kas võltsitud uudiste, meemide või propagandat levitavate mõjutajate kaudu. Paremäärmuslikud meemid, džihadistlikud videod ja anarho-nihilistlikud subkultuurid võivad radikaliseeruda üksikisikuid mängu- ja meemikultuuri kaudu enne, kui nad puutuvad kokku võimalike institutsionaalsete kaitsemeetmetega.

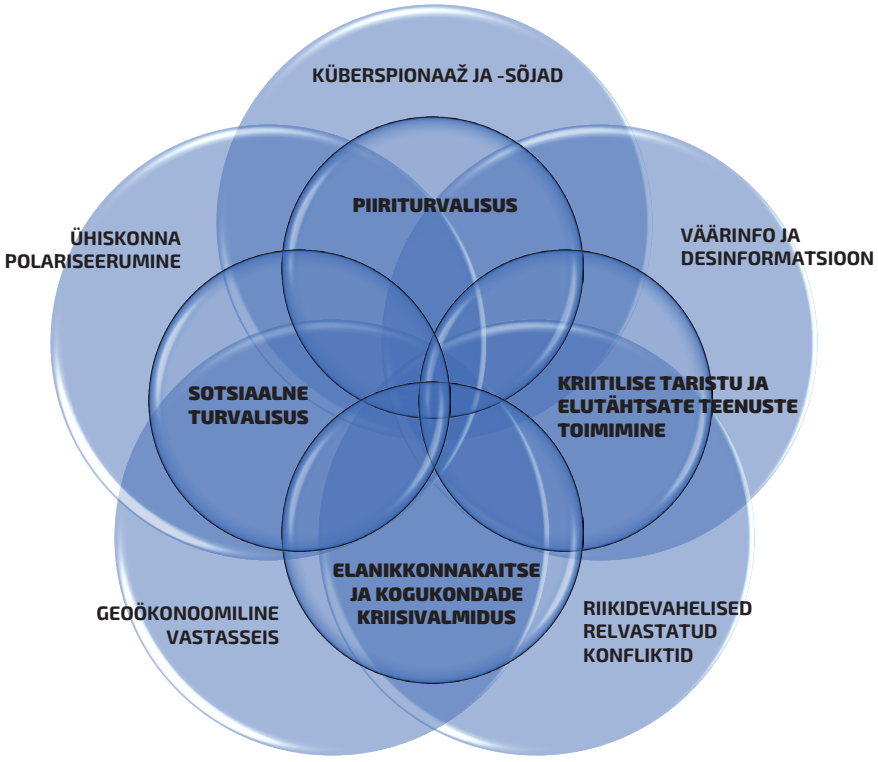
Nagu käesolev kümnend on näidanud, võib ühiskonna polariseerumine leida aset paljudes eluvaldkondades, kus soodsat pinnast pakuvad väärtuskonfliktidega laetud teemad. Erinevad äärmuslikud maailmavaated ja ideoloogiad – olgu poliitilised, religioossed või kultuurilised – kasutavad tundlikke valdkondi, et õõnestada usaldust riiklike institutsioonide ja demokraatliku otsustusprotsessi vastu. Tehisintellekt on muutnud desinformatsiooni loomise ja levitamise senisest kiiremaks, odavamaks ja raskemini tuvastatavaks, tekitades konkureerivaid tegelikkusi ja nõrgestades institutsionaalseid narratiive.

Ilma tõhusate ennetus- ja vastumeetmeteta on vaenulikud välistoimijad, nii riiklikud kui ka valitsusvälised, aga samuti kohalikud sisuloojad ja võrgustikud üha enam võimelised kasutama arenevaid tehnoloogiaid ning asümmeetrilisi taktikaid, et süvendada sihipäraselt ühiskondlikke lõhesid. Tõsise väljakutse ennetus- ja vastumeetmetele esitab tehnoloogiline areng, mh pahatahtlikud tehisintellektisülemid (ingl *malicious AI swarms*) (Schroeder *et al*., 2025), mis nõuab spetsiifiliste tarkvaraliste turvalahenduste väljatöötamist ja rakendamist.

VÕIMALIKE RISKIDE REALISEERUMISE KOOSMÕJU

Eesti eksperdid hindasid Eestit lähiaastatel kõige enam mõjutavate ohtudena (esitatud siinses raportis lk 14) küberspionaaži ja -sõdu, väärinfot ja desinformatsiooni, riikidevahelisi relvastatud konflikte, geoökonoomilist vastasseisu ning ühiskonna polariseerumist. Järgnevalt on Eestit kõige enam mõjutavaid ohte käsitletud nelja siseturvalisuse toimevaldkonna – piiriturvalisuse, kriitilise taristu ja elutähtsate teenuste toimimise, elanikkonnakaitse ja kogukondade kriisivalmiduse ning sotsiaalse turvalisuse – vaates (joonis 8).

Teadlased analüüsisid lisaks võimalikke kaskaadiefekte ja realiseerumise koosmõju nendele neljale toimevaldkonnale. Ülevaates on arvestatud ka eespool esitatud Maailma Majandusfoorumi hinnanguid suurima mõjuga riskidele (siinses uuringuraportis lk 7) –



JOONIS 8. EESTIT KÕIGE ENAM MÕJUTAVATE OHTUDE KÄSITLEMINE NELJAS TOIMEVALDKONNAS

kuigi need (näiteks ekstreemsed ilmastikunähtused) ei pruugi Eesti ekspertide hinnanguid arvestades olla Eesti jaoks lähiperioodil suurima ja vahetu mõjuga, võivad need siiski mõjutada Eesti sisejulgeolekut ja -turvalisust kaudselt.

Globaalsete riskide samaaegne realiseerumine ja omavaheline sünergia võivad põhjustada kaskaadiefekte, mis eskaleerivad kriise ulatuslikumateks ja raskemini hallatavateks ühiskondlikeks probleemideks. Mitme üheaegse kriisi avaldumisel ei pruugi olla piisav, kui riigi ja ühiskonnana ollakse seni hästi valmis ühe või teise kriisi eraldi vallandumiseks. Tavapäraselt planeeritud ja varutud ressursid võivad olla ebapiisavad juhul, kui häiritud on korraga mitmed elutähtsad teenused. Niisuguste kriiside võimalik eskaleeruv mõju suurendab kogukondade haavatavust: sageli kaasnevad sellega majanduslik ebastabiilsus, süvenev sotsiaalne lõhenemine ning kasvav usalduskriis riiklike institutsioonide suhtes. Seetõttu on tähtis, et siseturvalisuse asutustel, aga ka teistel riigisektori institutsioonidel oleks vajalik ettevalmistus, strateegiad ja riskihalduse protsessid, milles on ettevaatavalt arvestatud tavapärasest ressursimahukamate ja ootamatu dünaamikaga olukordadega. Samuti on oluline, et siseturvalisust puudutav õigusloome hoitaks ajakohasena ja vastavuses kiiresti areneva tehnoloogia ja muutuva (majandus)keskkonna tingimustega.

PIIRITURVALISUS

Venemaa ja Hiina, ent ka võimalike teiste riikide või huvigruppide küberspionaaž ja potentsiaalsed kübersõjad võivad endaga kaasa tuua küberrünnakuid, mis on suunatud piirivalves kasutatavate süsteemide vastu, nagu seirevõrgustikud, biomeetrilised andmebaasid, rändekontrolli platvormid. Selle tulemusena võivad need põhjustada piirikontrolli seiskumist, seiresüsteemide valehäireid ja/või edastatava teabe moonutusi, mis võib pärssida olukorrateadlikkust. Näiteks võib kübermanipulatsioon automatiseeritud piiriületuspunktides (nt eGate-süsteemides) põhjustada kontrollijärjekordade pikenemist, usaldusväärsuse langust tehniliste süsteemide ning ka Politsei- ja Piirivalveameti vastu ning suurendada ebaseaduslike piiriületuste riski rohelisel piiril. Küberspionaaži kaudu on võimalik hankida tundlikku teavet piirihalduse ja piirikaitse taktikalise korralduse kohta (nt sensorite paiknemine, patrulli korraldamine, reageerimine häiringutele), mida saab hiljem kasutada salakaubaveo, diversiooniaktide ja füüsiliste rünnete planeerimiseks. Täiendavaks riskiks võivad olla Hiinas valmistatud tehnoloogialahendused, näiteks jälgimisteenuste platvormid, mis ilma korrektse administreerimiseta võivad osutuda varjatud ebaseaduslikuks ligipääsukanaliks süsteemidele ja teabele. Küberrünnakud võivad ka kasutatava piirivalvetehnoloogia (nt droonid, jälgimissüsteemid, andmebaasid) otseselt halvata, kui selle riski maandamiseks ei ole rakendatud asjakohaseid turbemeetmeid.

Väärinfo, desinformatsiooni ja Venemaa strateegilise mõjutustegevuse tulemusena nii meedia vahendusel kui ka ametkondlike või muude otsekanalite kaudu kolmandates riikides, EL-i liikmesriikides ja ka Eestis leviv valeinfo, mis käsitleb „avatud piiride“ poliitikat, pagulaste õigusi või piiriületuse tingimusi, võib õhutada ebaseaduslikku rändevoogu, mida saab kasutada hübriidsurve meetmena (sarnaselt Valgevene ja Euroopa Liidu piirikriisiga 2021). Venemaa mõjutusoperatsioonid võivad levitada narratiive, mis õõnestavad avalikkuse usaldust Politsei- ja Piirivalveameti suhtes, mh kujutades neid pagulaste suhtes ebainimlike või kallutatuna. Desinformatsiooni abil on võimalik eskaleerida pinget piirialadel, luues mulje näiteks elanike kiusamisest piiriäärsete maade võõrandamisel või piiritsooni rakendamisel. Piiriäärsete kogukondade polariseerimine valeinfo kaudu võib vähendada kohalike elanike koostöövalmidust piirivalvega, mis omakorda nõrgestab varajast ohutuvastust. Valeinfo ja desinformatsioon võivad õõnestada avalikkuse usaldust piirivalve ja rändepoliitika vastu.

Venemaa agressioon Ukrainas on tekitanud pagulaste voolu, kus taotlejaid tuleb ka läbi Venemaaga loodud piiripunktide. See suurendab Eesti piirikontrolli koormust ja nõuab ühelt poolt paindlikkust rändehalduse mehhanismides, teisalt aga võimalike julgeolekuohtude pidevat tuvastamist. Võimalik, kuigi seni massiliselt fikseerimata, on ka terrorirühmituste või -võitlejate imbumine massiimmigratsiooni käigus kolmandatest riikidest, mis seab surve alla nii biomeetrilise tuvastuse kui ka riskiprofiilide filtreerimise süsteemid. Kuigi hinnangud Venemaa sõjalisele võimekusele on erinevad, siis Ukraina konflikti eskaleerudes nii Venemaale soodsas kui ka ebasoodsas suunas võib Venemaa tekitada diversiooniakte piiril Balti riikidega, näiteks selleks, et katsetada NATO reageerimisvõimekust piiri läheduses, või selleks, et tekitada Balti riikide ühiskonnas ebamugavustunnet ja hirmu.

Venemaa agressioonisõda Ukrainas, NATO riikide toetus Ukraina iseseisvusele ja territoriaalsele terviklikkusele ning Venemaa senised väljaütlemised, et soovitakse NATO eemalolekut Venemaa piiride vahetust lähedusest, kujutavad potentsiaalset otsest ohtu Eesti piiriturvalisusele, tähendades võimalikku vaenulikku tegevust Venemaa poolt Euroopa Liidu, sh Eesti piiril. Ühe otseselt vaenuliku tegevusena võib käsitleda varem kahepoolselt kokkulepitud märgistuspoide ühepoolset eemaldamist Narva jõelt. Samuti toimuvad Venemaa poolt mahukad GPS-süsteemide segamised Peterburi ja Pihkva ümbruses Ukraina droonide võimalikuks segamiseks, mille käigus ei huvituta rahvusvahelisest mõjust tsiviillennunduse turvalisusele teistes riikides. Laieneda ja süveneda võib ka sihilike drooniintsidentide probleem, mis nõuab droonitõrjemeetmete kiiret arendamist ja rakendamist.

Kolmanda riski, geoökonoomilise vastasseisu (Venemaa *vs*. EL ja selle liikmesriigid) mõju piiriturvalisusele ilmneb selles, et sanktsioonide laiendamisel võivad kasvada piiridel salakaubavõrgustikud ja tekkida korruptsioonirisk. Ebaseaduslik kaubavahetus on muutunud majandusliku surve tagajärjel atraktiivsemaks. Kui Eesti piiriäärsete elanike majanduslik haavatavus Kagu-Eestis ja Ida-Virumaal kasvab, võib see suurendada varimajanduse toetamist ja piirületusi puudutavate seaduste eiramist. Venemaa otsene tegevus, nähes Euroopa Liidus ja selle liikmesriikides oma geoökonoomilist ja geopoliitilist vastast, võib samuti mõjutada piiripunktide tööd ning Venemaalt saabuva piiriülese salakauba ebatõhusat kontrollimist Venemaa poolel. Lisaks, sarnaselt 2021. aastal Valgevene–EL-i piiril toimunud ulatuslikule organiseeritud ebaseaduslikule rändesurvele ning samaaegsele ebaseadusliku rände intensiivistumisele Venemaa–Eesti ja Venemaa–Soome piiril võib ka Venemaa–Eesti piiril kasvada ebaseadusliku rände maht.

Neljas risk, ühiskonna polariseerumine, võib mõjutada piiriturvalisust ühiskondliku killustumise ja vastandumise kaudu, õõnestades ühiskondlikku konsensust rändepoliitika ja piirikontrolli osas, näiteks seoses varjupaigataotlejate vastuvõtuga või piirikaitse intensiivsuse reguleerimisega. Kui osa elanikkonnast tajub piirikontrolli ideoloogiliselt motiveerituna (nt liiga leebe või liiga karm), siis võib see põhjustada ühiskondliku arvamuse varasemast intensiivsemat avaldumist. Infokeskkonna fragmenteerumine võib takistada ühtse avaliku arusaama tekkimist reaalsetest piiriohtudest, mis omakorda vähendab koostööd kriisiolukorras. Lisaks võib väljastpoolt juhitud radikaliseerumine (näiteks Venemaa või Hiina poolt) kasutada ühiskonna lõhesid sihipäraselt ära, et mobiliseerida piiriäärset elanikkonda EL/NATO-vastaseks infokampaaniaks. Näiteks võivad ekstreemselt meelestatud Venemaad toetavad elanike rühmitused Venemaa organisatsioonide eestvedamisel korraldada väiksemaid diversiooniakte ja meeleavaldusi, et häirida piiripunktide tööd ja turvalisust.

Globaalsed ohud võivad mõjutada Eesti piiriturvalisust. Ekstreemsed ilmastikunähtused, riikidevahelised relvastatud konfliktid eri regioonides väljaspool Euroopat ja terrorism

suurendavad oluliselt rändesurvet, eeskätt Lähis-Idast ja Aafrikast. See võib tekitada logistilise ja operatiivse ülekoormuse Eesti piirihaldussüsteemile.

Soovitused siseturvalisuse valdkonna riskidega toimetulekuks järgmisel viiel aastal.

- Tugevdada piiri- ja rändesüsteemide digitaalset ja füüsilist vastupidavust ning tagada nende pidev ajakohastamine.
- Hoida kriisiohjeplaanid pidevalt ajakohasena ning täiendada neid rändesurve ja infooperatsioonide võimalikuks koosmõjuks.
- Hinnata piiriturvalisuse süsteemide toimepidevuse sõltuvust ja haavatavust kolmandate riikide tehnoloogiapakkujatest. Riskianalüüsi põhjal rakendada tehnilisi ja organisatsioonilisi meetmeid.
- Arendada kiiresti välja ja rakendada droonitõrjemeetmed.

KRIITILINE TARISTU JA ELUTÄHTSAD TEENUSED

Süsteemne küberspionaaž ja sihipärased küberrünnakud suudavad halvata mitmeid elutähtsaid teenuseid ja taristut üheaegselt, põhjustades kaskaadiefekte kogu teenuseahelas (näiteks elektrivõrgu, sidevõrkude, veemajanduse ja andmetaristu samaaegsed rikked). Registreeritud küberintsidentidest suur osa on seotud teenuste katkestustega avalikus sektoris ja energiavaldkonnas. Tehisintellektil põhinevad tööriistad võimaldavad rünnata sihtotstarbeliselt just süsteemseid sõlmpunkte (nt SCADA-süsteemid, varuhalduse platvormid), mis halvavad kogu taristuvõrgu töö. Teisalt sõltub taristu töökindlus järjest enam infosüsteemide terviklikkusest, mistõttu on ohuallikaks nii füüsiline kui ka digijuurdepääs süsteemidele.

Desinformatsioonikampaaniad, mis seavad kahtluse alla avaliku sektori võimekuse ja legitiimsuse, võivad vähendada elanikkonna valmisolekut järgida hädaolukorras antavaid juhiseid või tekitada paanikat ja teenuste ülekoormust. Valeinfo levik (näiteks seoses veevarustuse „mürgitamisega“, elektrikatkestuste „varjamisega“ või ravimite „mõjuga“) võib põhjustada ebamõistlikku tarbimiskäitumist, mis omakorda destabiliseerib teenuste planeerimist ja toimimist. Seetõttu võib isegi psühholoogiline või informatsiooniline rünne ilma füüsilise või tehnilise rünnakuta viia teenuste ajutise katkestuse või usalduskriisini, mis seab ohtu nende toimepidevuse.

Elutähtsad teenused, nagu elektrivarustus, side, transport ja tervishoid, on muutunud strateegilisteks sihtmärkideks riikidevaheliste konfliktide raamistikus. Ukrainas toimunud massiivsed küberrünnakud (näiteks NotPetya, 2017; energia- ja sidevõrkude sihtimine 2022–2024) on näidanud, et riiklikult juhitud kübertegevus võib olla otseselt seotud sõjalise surve avaldamisega kriitilise taristu kaudu. Eesti kontekstis tähendab see, et näiteks Läänemere merealuste kaablite, gaasiühenduste või sideühenduste kahjustamine võib katkestada teenuste toimimise mitte päevadeks, vaid nädalateks, eriti kui kriis mõjutab samal ajal mitut sektorit.

Geoökonoomiline vastasseis (Venemaa ja EL-i vahel) mõjutab samuti kriitilise taristu ja elutähtsate teenuste toimimist. Sanktsioonide ja tarnepiirangute tõttu võivad katkeda toormaterjalide, varuosade või tehnoloogiliste komponentide tarneahelad, mis on kriitilise taristu hoolduse ja arenduse eeltingimus. Näiteks toorainest sõltuvate imporditud seadmete (nt kõrgepingelülitid, generaatorite komponendid, ravimid) tarnete katkemine või kallinemine võib pikendada hooldetsükleid ja suurendada seisakute riski. Eriti tundlikud on energiataristu, meditsiinitaristu ja IT-süsteemid, mille tarnelogistika sõltub rahvusvahelistest turuosalistest ja makrotasandi stabiilsusest. Kriitilise taristu toimepide-

vuse tagamine nõuab paindlikke tarneahelaid ning strateegilisi varusid, sh kodumaiseid täiendavaid reservvõimsusi.

Sotsiaalne lõhestumine ja institutsiooniline usalduskriis võivad polariseeruvas ühiskonnas põhjustada saboteerivat käitumist (näiteks teenuste tahtlik blokeerimine, sabotaaž, sabotaaži toetav propaganda). Teenuste toimimine sõltub sageli ühiskondlikust koostööst ja normikuulekusest nii tavaolukorras kui ka kriisi ajal (näiteks evakuatsioonikorralduste järgimine, kriisitarbimise mõistlikkus), mida polariseerumine õõnestab. Radikaliseerunud indiviidide või rühmituste tegevus võib sihtida just neid sümboolseid või ühiskondlikult nähtavaid taristuobjekte, mis esindavad riiklikku autoriteeti. Seetõttu peaks kriitilise taristu kaitse hõlmama mitte ainult tehnilist turvet, vaid ka sotsiaalset vastupanuvõimet, kogukondlikku usaldust ja ennetavat kommunikatsiooni.

Koosmõju ja kaskaadiefektid kriitilisele taristule ja elutähtsatele teenustele võivad avalduda küberrünnakute kaudu, kui samal ajal katkevad side-, energia- ja veeteenused, millel on laiaulatuslik mõju kogu ühiskonna toimimisele. Kaitseta jäänud info- ja andmetaristu võib halvata riigi mõne olulise valdkonna juhtimisvõime ja operatiivotsustusvõime. Suurenev sõltuvus eraettevõtetest (näiteks pilveteenused, kommunikatsioon) tähendab, et ka teenust pakkuvad eraettevõtted peavad soovima ja suutma tagada nende teenuste toimepidevuse, et elutähtsad teenused ei muutuks tururiskide ja geopoliitiliste konfliktide pantvangiks.

Soovitused siseturvalisuse valdkonna riskidega toimetulekuks järgmisel viiel aastal.

- Tagada mitmekihiline kaitse elutähtsatele teenustele (sh füüsiline ja digitaalne).
- Töötada välja võtmeteenuste autonoomia- ja dubleerimismehhanismid.
- Tagada küberturbespetsialistide ja küberkriisi plaanide olemasolu ning ajakohasus.
- Luua operatiivsed riskide kooskõlastusmehhanismid erasektori partneritega, eriti side-, energia- ja andmetaristu haldajatega.

ELANIKKONNAKAITSE JA KOGUKONDADE KRIISIVALMIDUS

Nagu eelmises alajaotuses käsitletud, on küberspionaaži ja küberrünnete kaudu võimalik halvata elutähtsaid taristuid, nagu energiavarustus, sidesüsteemid ja andmekogud. See omakorda mõjutab otseselt elanikkonna füüsilist turvalisust ja kriisile reageerimise võimet. Küberrünnetega võivad kaasneda teabe lekkimine, volitamata muutmine ning süsteemide ja teenuste katkestused. See aeglustab kriisile reageerimist ja halvendab elanikkonnakaitse tegevuste operatiivset suutlikkust. Kogukondliku kriisivalmiduse vaates võib usaldus e-riigi ja digitaalse teavituse kanalite vastu kahaneda, kui inimesed kogevad teenuste katkemist või kahtlustavad andmeleket. Üksikisikute digitaalsed haavatavused suurendavad riski, et kogukondlikud võrgustikud jäävad kriisis informeerimata või saavad manipuleeritud teavet, mis vähendab sotsiaalset kohanemisvõimet.

Väärinfo ja desinformatsiooni mõju elanikkonnakaitsele ja kogukondade kriisivalmidusele seisneb selles, et süsteemne valeinfo levik (sh süvavõltsingud ja manipuleeritud narratiivid) õõnestab riigi ametlikke kriisiteavituse mehhanisme, mis on elanikkonnakaitse seisukohalt kriitilise tähtsusega. Desinformatsiooni sihtrühmaks on sageli venekeelne elanikkond ja noored, kes võivad digikeskkonnas sattuda massiivsete mõjutusoperatsioonide sihtmärgiks. Kriisiolukorras võib valeinfo põhjustada ebaühtlast riskitajumist, mille tulemusel eri kogukonnad reageerivad vastuoluliselt või ei järgi ametlikke juhiseid.

Ukrainas toimunud sõjategevus on näidanud, et elanikkonna kaitsmiseks mõeldud taristu (näiteks varjendid, evakuatsiooniplaanid, kommunikatsioonivõrgud) muutub kergesti sihtmärgiks. Eestis tähendab see vajadust taastada ja katsetada erinevaid varjumisvõimekusi, tagada hajutatud kriisivarud ning korraldada realistlikke õppusi kogukondlikul tasandil. Sõja mõju on kasvatanud pinget ja hirmu kogukondades, eriti piirkondades, kus esineb rahvuslikke ja ideoloogilisi lõhesid. See võib takistada usaldusel põhinevat koostööd kriisiolukordades. Samas on sõda aktiveerinud kogukondlikku solidaarsust ja kriisivalmidust.

Geoökonoomilise vastasseisu mõju elanikkonnakaitsele võib ilmneda juhul, kui Venemaa mõjutustegevuse tulemusena suudetaks häirida Euroopa Liidu siseseid tarneahelaid või tarneahelaid Euroopa Liidu liikmesriikide ja partnerriikide vahel. See võib kaasa tuua tarneahelate ebakindluse või katkemise, mis mõjutab ravimite, kütuse või toidu kättesaadavust. Kogukonnad, kus sotsiaal-majanduslik haavatavus on juba suur (näiteks äärealade elanikud, eakad, üksikvanemad), võivad kaotada motivatsiooni kriisivalmiduseks, kuna esmased ellujäämisvajadused võtavad kogu tähelepanu. Raskused võivad süvendada kõrvalseisja tunnet riigi- ja turvastruktuuridest, mis vähendab usaldust koostööks kriisis.

Eesti ühiskonna polariseerumise, sh ideoloogilise ja väärtuspõhise killustumise mõju elanikkonnakaitsele ilmneb neil juhtudel, kui riiklikud ohuteavitused ja kriisiinfo võetakse vastu läbi ideoloogiliste filtrite. Siis võib tekkida või süveneda olukord, kus osa elanikkonnast keeldub uskumast ametlikke juhiseid või isegi vastandub neile aktiivselt, mis toimus näiteks COVID-19 pandeemia ajal. Valeinfo leviku ja äärmusrühmituste mõjul võivad tekkida ka tõrked evakuatsioonis, koostöös kohaliku omavalitsusega või hädaolukorra juhtimises. Sotsiaalmeedias süvenevad kajakambrid ja vandenõuteooriad murendavad kogukondade ühtsust ning takistavad ühist arusaama ohtudest ja vastutusest. Noorte varajane kokkupuude äärmusliku sisuga (näiteks sotsiaalmeediakanalites nagu TikTok, Discord, Telegram) suurendab vägivallaideoloogiate ja sotsiaalse vastandumise levikut, mis võib muutuda ohuallikaks kriiside käigus.

Mitme kriisi, näiteks massiivne valeinfo levik, energiakatkestus ja rändevood, samaaegne esinemine võib muuta kogukonnad järsult väga haavatavaks. Poliitiline ja institutsionaalne usalduskriis võib pärssida kriisiteavitust ja vastupanuvõimet. Radikaliseerumine ja sotsiaalne polariseerumine võivad vallanduda kriisikommunikatsiooni ebaõnnestumisel.

Soovitused siseturvalisuse valdkonna riskidega toimetulekuks järgmisel viiel aastal.

- Arendada välja integreeritud elanikkonnakaitse strateegiad multikriiside jaoks.
- Laiapindse riigikaitse raames tugevdada selge ühiskondliku rollijaotusega kogukondlikku valmisolekut ja sotsiaalset sidusust.
- Kasutada kriisiteavituse planeerimisel infotarbimise psühholoogiat ja digitaalse kirjaoskuse meetmeid.

SOTSIAALNE TURVALISUS

Vaenulike organisatsioonide või riikide korraldatud süsteemsed küberrünnakud sihivad sotsiaalseid teenuseid, identiteedihaldust ja finantsinfrastruktuure. Sellised rünnakud võivad põhjustada teenuste katkemist ja isikuandmete lekkimist, mis omakorda vähendavad inimeste turvatunnet ja usaldust riigi võimekusse neid kaitsta. Küberrünnakud, mille tagajärjel häiritakse näiteks toetuste maksmist, meditsiiniandmeid või rahvastikuregistrit, võivad vallandada ebavõrdsuse ja sotsiaalse stressi, eriti haavatavates elanikegruppides, nagu eakad ja erivajadustega inimesed.

Väärinfo ja desinformatsioon mõjub samuti sotsiaalsele turvalisusele. Süsteemne väärinfo levik tekitab vastandlikke tõlgendusi ühiskondlikest probleemidest, õõnestab sotsiaalset sidusust ja soodustab grupipõhist stigmatiseerimist. Narratiivid, mis esitavad riigiasutusi korrumpeerununa või erinevaid ühiskonnagruppe ohuna (juhul, kui see ei ole põhjendatud), võivad viia vastanduvate leerideni ja toita vastastikust vaenu. Näiteks Ida-Virumaa venekeelset elanikkonda mõjutavad Eesti-vaenulikud narratiivid võivad aktiveerida ühiskondlikke konflikte, eriti kui need leiavad tuge kohalikes kogukondades ja virtuaalsetes foorumites.

Sõja jätkumine Ukrainas ning selle visuaalne ja emotsionaalne kajastus meedias ning Ukraina vabastamise venimine on väsitanud ühiskonda moraalselt ja psühholoogiliselt, eriti madalama sissetulekuga elanike seas, kelle jaoks igapäevane toimetulek on peamiseks murekohaks. Sõjategevuse eskaleerumine Ukrainas võib vähendada turvatunnet ja tekitab mõnel juhul psühhosotsiaalset stressi, mis võib ilmneda tõrjuva käitumise ja vaenukõnena (vt ka KAPO 2024, 2025).

Rahvusvahelise geoökonoomilise vastasseisu mõjul tõusevad hinnad ja langeb ostujõud, mis eriti madala sissetulekuga elanikkonnale tähendab raskusi esmatarbekaupade soetamisel ja teenuste kättesaamisel. Kui elukalliduse kasv on tajutav ja põhjused keerulised või geopoliitilised, siis projitseeritakse rahulolematus tihti sisepoliitikale või konkreetsetele elanikerühmadele, suurendades nii sotsiaalset pinget. Riskirühmadeks on piirkonnad, kus tööpuudus on kõrge ning on palju üksikvanemaid, töötuid ja eakaid, kelle toimetulek võib järsult halveneda majandussurutise või tarnehäirete korral.

Ühiskonna polariseerumise mõjul tugevnevad ideoloogilised lõhed (näiteks liberaalsed *vs*. konservatiivsed väärtused, rahvuslased *vs*. globalistid) võivad killustada sotsiaalset keskkonda, kus erinevad kogukonnad kaotavad võime üksteist usaldada või koostööd teha. Kuigi vaadetepõhine polariseerumine on Eestis üldiselt rahulik, võib näiteks vaktsineerimise, pagulaste, Ukraina sõja, rohepöörde või hariduse teemal vastandumine muutuda siiski madala intensiivsusega konfliktideks töökohtades, haridusasutustes või kogukondlikes võrgustikes. Laste ja noorte haavatavus on eriti kriitiline, kuna nad puutuvad varakult kokku polariseeritud ja radikaliseeriva sisuga, mille tulemusel võib väheneda usaldus ühiskondlike institutsioonide vastu või suureneda tõrjutus ja vägivaldsus.

Sotsiaalset turvalisust mõjutavate ohtude kaskaadiefektid, nagu valeinfo, tööpuudus, toimetulekuraskused ja identiteedikriisid, võivad esile kutsuda ühiskondlikke pingeid ja massirahutusi, eriti majanduslanguse või geopoliitilise kriisi ajal. Noorte radikaliseerumine sotsiaalmeedia ja modereerimata keskkondade kaudu võib süvendada vägivaldset ekstremismi. Sotsiaalne vastandumine võib muutuda julgeolekuprobleemiks, kui see ohustab põhiseaduslikku korda.

Soovitused siseturvalisuse valdkonnas riskidega toimetulekuks järgmisel viiel aastal.

- Kujundada pikaajaline sotsiaalse vastupanu strateegia, mis vähendab ühiskondlikku killustatust.
- Suurendada üldist teadlikkust ja luua riskigruppidele suunatud sekkumismehhanismid (sh digitaalses ruumis).
- Suurendada demokraatlike institutsioonide legitiimsust ja kaasatust usaldusväärse kriisikommunikatsiooni ja hariduse kaudu.

MITME OHU ÜHEAEGSE REALISEERUMISE VÕIMALIK MÕJU EESTI SISEJULGEOLEKULE

Eeltoodust ilmnes, et mitme ohu üheaegne realiseerumine võib mõjutada kõiki nelja fookusvaldkonda (piiriturvalisus, kriitiline taristu ja elutähtsad teenused, elanikkonna kaitse ja kogukondade kriisivalmidus ning sotsiaalne turvalisus) teisiti ja mahukamalt kui neist ühe ohu eraldi realiseerumine. Võimalik sünergiline multikriis – näiteks kübersõda, valeinfo, rändesurve ja majanduslik ebastabiilsus – võib mõjutada kõiki fookusvaldkondi korraga.

Selle paremaks ilmestamiseks võib luua hüpoteetilise olukorra, mille kohaselt tekib Eestis samal ajal mitu erinevat kriisi, millest mõned on sihilikult esile kutsutud välise huvigrupi poolt – näiteks halvab vaenuliku välisriigi korraldatud ja toetatud küberrünnak ajutiselt side- ja energiataristu, sealhulgas piiri seiresüsteemid ja andmehaldusteenused. Samal ajal levib valeinfokampaania, mis esitab kriisi Eesti valitsuse poolt lavastatuna ühiskonna paremaks allutamiseks ning kutsub seetõttu üles kodanikuallumatusele. Lähis-Idas puhkenud relvastatud konflikt toob kaasa olulise rändesurve Euroopa Liidu idapiiridele. Aasia ja lääne geopoliitiliste pingete eskaleerumine katkestab osa tarneahelaid ning põhjustab hinnatõusu ja kaupade nappust.

Niisuguse abstraktse näitliku stsenaariumi rakendumisel on mõju fookusvaldkondadele järgmine.

- Mõju piiriturvalisusele. Küberrünnete tõttu talvel oluliste miinuskraadide või suvel kuumalaine ajal lakkab töötamast osa idapiiri elektroonilistest seiresüsteemidest ning dokumendikontrollisüsteemid idapiiril ja Tallinna lennujaamas. See põhjustab segadust piiriületuste haldamises ja täiendavat ajakulu piiriületusel. Desinformatsioon, mille kohaselt Eesti piir on avatud või piiriületus katkestatud, kutsub esile piirikogukondade rahutuse ja usaldamatuse piirivalve vastu. Samal ajal eskaleeruv rändesurve ja kolmandatest riikidest pärit haavatavate demograafiliste rühmade (lapsed, eakad) arvukas viibimine Venemaa ja Eesti piiripunktide vahelisel alal või rohelisel piiril suurendab survet vastuvõtuvõimekusele ja siseneva liikluse kontrollimisele. See omakorda raskendab Politsei- ja Piirivalveameti operatiivset toimimist, eriti kui ka Maksu- ja Tolliametil puudub asukohas toetav võimekus ning puudub toetav koostöö kogukondadega. Olukorra eskaleerudes võivad piiriäärsed piirkonnad jääda vastuolulise ja manipuleeriva infovälja mõjualasse, mis vähendab institutsioonide autoriteeti.
- Energia- ja sidesüsteemide sihitud rünnakud halvendavad elutähtsate teenuste kättesaadavust üle riigi (näiteks katkeb side häirekeskuse ja meditsiiniasutuste vahel, lakkavad töötamast makseterminalid). Pilvepõhiste teenuste (näiteks digiretsept, rahvastikuregister) katkemine või andmekao risk halvab logistikavood ja tarneahelad. Tarnekriisi tõttu (näiteks ravimite või varuosade puudus) võib sulguda osa esmatasandi tervishoiuteenuseid, mis kasvatab haavatavust. Toimub teenuste ajutine ümberjaotus prioriteetidele, mis põhjustab rahulolematust ja tajutavat ebavõrdsust eri piirkondades.
- Vaenulike organisatsioonide või mõne välisriigi orkestreeritud valeinfo kriisijuhtimise kohta, nagu näiteks „valitsus varjab tõde“, „ajutine evakuatsioon on lõks“, õõnestab elanikkonna valmisolekut järgida kriisihalduse juhiseid. Küberrünnakute tõttu katkestatud teavituskanalid takistavad hädaolukorra kommunikatsiooni, sh sireenide ja SMS-hoiatussüsteemide tööd. Kohalikud kriisivarud (näiteks toidujagamine, varjumisvõimalused) osutuvad ebapiisavaks, kuna seni pole arvestatud

multikriisi stsenaariumiga. Vähem usaldust avalike võimude vastu viib selleni, et inimesed pöörduvad ebausaldusväärsete allikate või radikaliseerunud võrgustike poole, kahjustades sotsiaalset ühtekuuluvust kogukondlikul tasandil.

- Tarneahelate katkestusest tulenev kriitiliste kaupade nappus võib põhjustada Venemaa infoväljas olevates kogukondades rahutusi ja vaenulike toimijate poolt suunatud proteste, mida võimendavad sotsiaalmeedias levivad äärmusnarratiivid. Valeinfo ja desinformatsioon loovad teatud rahvusgruppidest või ametnikest vaenlasekujusid, kutsudes esile sotsiaalset pinget ja polariseerumist. Majanduslikult haavatavatele rühmadele langeb ebaproportsionaalne kriisikoormus, mis süvendab tajutavat ebaõiglust ja õhutab sotsiaalset konflikti. Usaldus sotsiaalkaitsesüsteemide vastu väheneb.

Kuigi selline stsenaarium on pigem hüpoteetiline, võtab see näitlikult arvesse lähiaastate geopoliitiliste pingete, tehnoloogiliste ohtude ja sotsiaalsete probleemide võimalikku koostoimet. Eesti kontekstis näitab see, et kriisivalmidus ei tohi toetuda lineaarsele riskijuhtimisele, vaid vajab süsteemipõhist, ristsõltuvusi arvestavat strateegilist planeerimist. Elutähtsate teenuste, kogukondliku vastupanuvõime ja kommunikatiivse vastupanu tugevdamine on vältimatu, kui soovitakse hoida Eesti ühiskonda stabiilsena ka komplekssete julgeolekušokkide korral. Eesti sisejulgeoleku vastupanuvõime eeldab, et kriiside lahendamine ei tugine üksikutele reageerimisvõimekustele, vaid integreeritud ja ennustatavale riskijuhtimisele. Seetõttu on soovituslik liikuda prognoosivalt kohaneva ja laiapõhjalise julgeoleku poole, kus tehnoloogia, sotsiaalne sidusus ja usaldus institutsioonide vastu üksteist toetavad.

KOKKUVÕTE

Riskijuhtimise võtmeks on võimekus näha ette võimalikke tulevikustsenaariumeid ja teadusel on selles ülioluline roll. Kindlasti on tähtis ka teadvustada, et pelgalt teaduslikest ja tehnoloogilistest läbimurretest ei piisa tänapäevaste kriiside ületamiseks. Igast kriisist on oluline õppida ning käsitleda saadud õppetunde kui võimalust toetada ühiskondlikke muutusi, tegeledes sellega järjepidevalt ka siis kui otseseid ohte parasjagu ei esine.

Olukordades, kus ühiskondlik surve nõuab kiiret poliitilist sekkumist, kasvab vajadus põhjendada langetatavaid otsuseid teadusliku lähenemise kaudu – eriti siis, kui tegemist on ebapopulaarsete ja vähese avaliku toetusega meetmetega või nende mõju ei avaldu vahetult. Samas tuleb rõhutada, et teadus saab pakkuda üksnes informeeritud tegevusvalikuid, samal ajal kui vastutus lõplike otsuste eest lasub poliitilistel otsustajatel. Ka kriiside ajal on oluline neid rolle selgelt eristada ning tagada ühiskonnale arusaam teadlaste ja poliitikute usalduslikust ja läbipaistvast koostööst.

Eesti erialaekspertide hinnangul peetakse Eesti sisejulgeolekut aastatel 2026–2030 kõige enam mõjutavateks globaalseteks riskideks:

- küberspionaaži ja -sõdu;
- väärinfo ja desinformatsiooni levikut;
- riikidevahelisi relvastatud konflikte;
- geoökonoomilist vastasseisu;
- ühiskonna polariseerumist.

Samas hinnati suureks riskiks ka võimalikku talentide ja oskustööjõu puudust ning kriitilise infrastruktuuri ja oluliste tarneahelate häireid. Oskustööjõu võimalik puudus ei ähvarda pelgalt tehnoloogiaga seotud valdkondi, vaid on ohuks ka realiseeruda võivate riskide ohjamisel, seda eriti sisejulgeoleku tagamiseks vajalike funktsioonide täitmisel, kui samal ajal on haavatud mitmed elutähtsad teenused. Samuti on oluline pöörata senisest rohkem tähelepanu võimalike tarneahelate katkemisega tekkivatele ohtudele ja ühiskonna toimimiseks vajalike varude tagamisele.

Tehisintellekti, eriti generatiivse tehisintellekti, kiire areng suurendab küberspionaaži ja -rünnete keerukust. Süveneb kriitilise taristu haavatavus. Eestis registreeriti 2024. aastal rekordiline arv mõjuga küberintsidente. Tehisintellektipõhised manipulatsioonitehnikad (nt süvavõltsingud) suurendavad usaldamatust demokraatlike institutsioonide suhtes ja süvendavad ühiskondlikku lõhestatust. Eriti ohustatud on noored sotsiaalmeedias ja reguleerimata infokeskkondades. Tehnoloogiline areng ja hübriidohud (sh väärinfo, käre-

populism ja äärmuslus) süvendavad lõhet kogukondade vahel. Kasvab poliitiline otsustusvõimetus ja ühiskondlik usalduskriis.

Venemaa agressioon Ukrainas ning pinged Lähis-Idas ja Aasias võivad põhjustada eskaleeruvat rändesurvet, terrorismiohu suurenemist ja sotsiaalset destabiliseerumist ka Eestis. Radikaliseerumise risk kasvab eriti seoses globaalsete konfliktidega. Eesti majandus on haavatav USA ja Hiina kaubanduskonflikti mõjule.

Tõenäoline on mitmete riskide samaaegne realiseerumine ehk multikriisid, mis võib üle koormata traditsioonilised kriisihaldusmehhanismid. Eriti suur mõju võib kaasneda, kui korraga katkeb juurdepääs infole, energiale ja kriitilistele (elutähtsatele) teenustele. Analüüsis on hinnatud, et strateegilise valmisoleku suurendamiseks on vaja tõhustada laiapindset riigikaitset, arendada ühiskonna küberhügieeni ja teabekriitikat, suurendada investeeringuid küberturbe spetsialistide koolitusse ning maandada sõltuvust ebastabiilsetest tarneahelatest.

Uuringu tulemusena on poliitikakujundajatele kokkuvõtvalt esitatud järgmised soovitused.

- Integreerida teaduspõhised prognoosid kriisijuhtimisse ja strateegilisse planeerimisse.
- Suurendada investeeringuid küberturvalisusse ja -teadlikkusse ning droonitõrjemeetmetesse.
- Luua lisamehhanismid valeinfo leviku tõkestamiseks ja ühiskondliku polariseerumise leevendamiseks.
- Tagada kriitilise taristu mitmekordne kaitse peatähelepanuga side-, energia- ja andmetaristule.
- Jälgida süsteemselt globaalsete konfliktide mõju Eesti sisejulgeolekule ning arendada sellekohaseid prognoosivaid metoodikaid ja mudeleid.

VIIDATUD ALLIKAD

Adlakha, H., 2023. 10 Reasons Xi Won't Attack Taiwan Anytime Soon. The Diplomat, 20.01.2023. [Võrgumaterjal] Leitav: https://thediplomat.com/2023/01/10-reasons-xi-wont-attack-taiwan-anytime-soon/ [Kasutatud 13.05.2025].

Altman, H., 2025. "Cartel Members Fought in Ukraine to Learn FPV Drone Skills: Report." *The War Zone*, July 30. Leitav: https://www.twz.com/news-features/cartel-members-fought-in-ukraine-to-learn-fpv-drone-skills-report [Kasutatud 22.08.2025].

Anghel, V., 2025. *Global Risks to the EU*. European University Institute. [Võrgumaterjal] Leitav: https://cadmus.eui.eu/server/api/core/bitstreams/bf016066-0244-5253-9c9a-6229fa318598/content [Kasutatud 21.03.2025].

Bonifassi, S., & Bastien, J., 2025. *A closer look at EU sanctions enforcement following adoption of new directive*. Global Investigations Review, 30.06.2025. [Võrgumaterjal] Leitav: https://globalinvestigationsreview.com/guide/the-guide-sanctions/sixth-edition/article/closer-look-eu-sanctions-enforcement-following-adoption-of-new-directive [Kasutatud 12.09.2025].

Borbáth, E., Hutter, S., & Leininger, A., 2023. Cleavage politics, polarisation and participation in Western Europe. *West European Politics*, Vol. 46(4), pp. 631–651. https://doi.org/10.1080/01402382.2022.2161786

Burgess, S., 2022. Ukraine war: Deepfake video of Zelenskyy telling Ukrainians to 'lay down arms' debunked. SkyNews, 17.03.2022. [Võrgumaterjal] Leitav: https://news.sky.com/story/ukraine-war-deepfake-video-of-zelenskyy-telling-ukrainians-to-lay-down-arms-debunked-12567789 [Kasutatud 03.06.2025].

Data Guardian Hub, 2024. How Cyber Espionage Threats Have Evolved: A Look at 5 Key Trends in 2024. Data Guardian Hub, 20.05.2024. [Võrgumaterjal] Leitav: https://www.es.consulting/blog/cybersecurity-trends-for-2024-a-look-into-the-future [Kasutatud 03.06.2025].

Deloitte, 2025. Global Cyber Threat Intelligence (CTI). Annual Cyberthreat Trends Report – 2024. [Võrgumaterjal] Leitav: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-annual-cyber-threat-trends-report-2025.pdf [Kasutatud 03.06.2025].

DOJ, 2023. Press Release: U.S. Attorney Announces Charges And New Arrest In Connection With Assassination Plot Directed From Iran. Press release, U.S. Attorneys Office, Southern District of New York, U.S Department of Justice. Leitav: https://www.justice.gov/usao-sdny/pr/us-attorney-announces-charges-and-new-arrest-connection-assassination-plot-directed [Kasutatud 22.08.2025].

Duffy, K. & Harbath, K., 2024. Defending the Year of Democracy: What It Will Take to Defend 2024's 80-Plus Elections From Hostile Actors. *Foreign Affairs,* 04.01.2024. [Võrgumaterjal] Leitav: https://www.foreignaffairs.com/united-states/defending-year-democracy [Kasutatud 24.08.2025].

Eesti Vabariigi Välisministeerium, 2025. Euroopa Liit võttis vastu uue sanktsioonipaketi Venemaale. 18. juuli 2025. [Võrgumaterjal] Leitav: https://vm.ee/uudised/euroopa-liit-vottis-vastu-uue-sanktsioonipaketi-venemaale [Kasutatud 12.08.2025].

Edwards, C. & Seidenstein, N., 2025. *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*. The International Institute for Strategic Studies (August 2025). [Võrgumaterjal] Leitav: https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/ [Kasutatud 12.09.2025].

Euroopa Parlamendi ja nõukogu direktiiv (EL) 2024/1226, 24. aprill 2024, mis käsitleb liidu piiravate meetmete rikkumisega seotud kuritegude määratlemist ja nende eest mõistetavaid karistusi ning millega muudetakse direktiivi (EL) 2018/1673. ELT L, 2024/1226, 29.4.2024.

European Commission, 2024a. Eurobarometer 547. Cyberskills. [Võrgumaterjal] Leitav: https://europa.eu/eurobarometer/surveys/detail/3176 [Kasutatud 03.06.2025].

European Commission, 2024b. Eurobarometer 547. Cyberskills. Facktsheet – Estonia. [Võrgumaterjal] Leitav: https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=93205 [Kasutatud 03.06.2025].

Europol SOCTA, 2025. Europol, *European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime*, Publications Office of the European Union, Luxembourg, 2025. Leitav: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf [Kasutatud 22.08.2025].

Europol TESAT, 2024. *European Union Terrorism Situation and Trend Report 2024*, Luxembourg: Publications Office of the European Union. Leitav: https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf [Kasutatud 22.08.2025].

Europol TESAT, 2025. European Union Terrorism Situation and Trend Report 2025, Luxembourg: Publications Office of the European Union. Leitav: https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf [Kasutatud 22.08.2025].

GTI, 2025. *Global Terrorism Index 2025: Measuring The Impact of Terrorism,* Sydney: Institute for Economics & Peace. Leitav: https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf [Kasutatud 22.08.2025].

Hambling, D., 2025. "Moving Targets: Implications of the Russo-Ukrainian War for Drone Terrorism." *CTC Sentinel Combating Terrorism Center at West Point* 18 (7). Leitav: https://ctc.westpoint.edu/wp-content/uploads/2025/07/CTC-SENTINEL-072025_cover-article.pdf [Kasutatud 22.08.2025].

Hitachi Cyber, 2025. Cyber Threat Landscape in 2025: Trends and Challenges. [Võrgumaterjal] Leitav: https://hitachicyber.com/cyber-threat-landscape-in-2025-trends-and-challenges/ [Kasutatud 21.05.2025].

Höller, L., 2025. Drug cartel operatives snuck into Ukraine for drone training: report. Defence News, July 30. Leitav: https://www.defensenews.com/global/

the-americas/2025/07/30/drug-cartel-operatives-snuck-into-ukraine-for-drone-training-report/ [Kasutatud 22.08.2025].

ISCP, 2025. Intelligence and Security Committee of Parliament. Iran. HC 1116. London: UK Parliament. Leitav: https://isc.independent.gov.uk/wp-content/uploads/2025/07/Intelligence-and-Security-Committee-of-Parliament-Iran.pdf [Kasutatud 22.08.2025].

Jones, Seth G., 2025. Russia's Shadow War Against the West. CSIS Briefs. March. Center for Strategic and International Studies. Leitav: https://www.csis.org/analysis/russias-shadow-war-against-west [Kasutatud 22.08.2025].

Joske, A., 2022. Spies and Lies. How China's Greatest Covert Operation Fooled the World. Berkeley, CA: Hardie Grant Books.

Jüris, F., 2023. Making friends, making inroads: The CCP's influence activities in Estonia. Sinopsis. Aca Media. [Võrgumaterjal] Leitav: https://sinopsis.cz/en/making-friends-making-inroads-the-ccps-influence-activities-in-estonia/ [Kasutatud 24.07.2025].

Kaitsepolitseiamet, 2024. Aastaraamat 2023-2024. [Võrgumaterjal] Leitav: https://kapo.ee/sites/default/files/content_page_attachments/Aastaraamat%202023-2024.pdf [Kasutatud 14.05.2025].

Kaitsepolitseiamet, 2025. Kaitsepolitsei aastaraamat 2024-2025. Tallinn: Kaitsepolitseiamet. [Võrgumaterjal] Leitav: https://kapo.ee/sites/default/files/content_page_attachments/aastaraamat-2024-2025_0.pdf [Kasutatud 25.04.2025].

Kaljula, R., 2024. Väike Taiwan – tehnoloogiline suurriik. Postimees AK, 13.01.2024. [Võrgumaterjal] Leitav: https://maailm.postimees.ee/7936785/ak-vaike-taiwan-tehnoloogiline-suurriik [Kasutatud 14.05.2025].

Karistusseadustik. RT I, 05.07.2025, 9.

Kantrowitz, A., 2025. AIs Deceive Human Evaluators. And We're Probably Not Freaking Out Enough. CMSWire, 27.02.2025. [Võrgumaterjal] Leitav: https://www.cmswire.com/ai-technology/ais-deceive-human-evaluators-and-were-probably-not-freaking-out-enough/ [Kasutatud 12.09.2025].

Kubin, E. & von Sikorski, C., 2021. The role of (social) media in political polarization: a systematic review. *Annals of the International Communication Association*, *45*(3), pp. 188–206. https://doi.org/10.1080/23808985.2021.1976070

Loik, R., 2022. Venemaa „infomürsud" Ukraina vastu valmistasid ette konventsionaalset kallaletungi. Diplomaatia, Nr. 211, lk. 16–20. [Võrgumaterjal] Leitav: https://diplomaatia.ee/venemaa-infomursud-ukraina-vastu-valmistasid-ette-konventsionaalset-kallaletungi/ [Kasutatud 16.05.2025].

Loik, R., 2024. Undersea Hybrid Threats in Strategic Competition: The Emerging Domain of NATO–EU Defense Cooperation. Journal on Baltic Security, 10 (2), pp. 1–25. [Võrgumaterjal] Leitav: https://journalonbalticsecurity.com/journal/JOBS/article/126/text [Kasutatud 24.08.2025].

Lomp, L-E., 2025. Peeter Tali: Kohtla-Järve sotsidest juhid on poliitiliselt kurdid ja pimedad. Postimees, 28. jaanuar. [Võrgumaterjal] Leitav: https://www.postimees.ee/8181083/peeter-tali-kohtla-jarve-sotsidest-juhid-on-poliitiliselt-kurdid-ja-pimedad [Kasutatud 24.07.2025].

Läänemets, M., 2022. Miks Hiina pelgab Taiwanit rünnata? Postimees, 28.07.2022. [Võrgumaterjal] Leitav: https://arvamus.postimees.ee/7572702/mart-laanemets-miks-hiina-pelgab-taiwanit-runnata [Kasutatud 13.05.2025].

Läänemets, M., 2023. Russo-Ukrainian war and China's global interests. *Security Spectrum. Procedings of the Academy of Security Science*s, 22, pp. 177 – 189. [Võrgumaterjal] Leitav: https://digiriiul.sisekaitse.ee/handle/123456789/3154 [Kasutatud 14.05.2025].

Läänemets, M., 2024. Hiina „suur plaan" ja selle mõju Eesti julgeolekule. Turvalisuskompass, 7 (2), lk 9-32.

Madsen, T., 2024. Hiina suursaadik parlamendiliikmete visiidist: ma ei nõustu sõnaga «skandaal». Postimees, 19. detsember. [Võrgumaterjal] Leitav https://www.postimees.ee/8155755/intervjuu-hiina-suursaadik-parlamendiliikmete-visiidist-ma-ei-noustu-sonaga-skandaal [Kasutatud 24.07.2025].

Mahmudov, N., 2023. Cyber warfare: understanding the elements, effects, and future trends of cyber-attacks and defences. Security & Defense, 2, pp. 37–54.

Manak, I., Patterson, R., Liu, Z., O'Neil, S.K., Setser, B.W., Alden, E., Steil, B., Hillman, J.E., Goodman, M.P., & Freeman, W., 2025. What Trump Trade Policy Has Achieved Since 'Liberation Day'. Greenberg Center for Geoeconomic Studies at the Council on Foreign Relations. [Võrgumaterjal] Leitav: https://www.cfr.org/article/what-trump-trade-policy-has-achieved-liberation-day [Kasutatud 12.08.2025].

Marcus, G., & Hamiel, N., 2024. LLMs + Coding Agents = Security Nightmare. *Marcus on AI,* 17.08.2025. [Võrgumaterjal] Leitav: https://garymarcus.substack.com/p/llms-coding-agents-security-nightmare [Kasutatud 12.09.2025].

Muuga, E., Loik, R., Kaup, G.-H., Savimaa, R., & Koort, E. 2025. Julgeolekuohud Balti riikide merealuste ühendustega seotud kriitilisele taristule: Läänemeri hübriidsõja tulipunktis. Tallinn: Sisekaitseakadeemia. [Võrgumaterjal] Leitav: https://digiriiul.sisekaitse.ee/handle/123456789/3579 [Kasutatud 16.05.2025].

O'Donnell, J., Heaven, W. O. & Heikkilä, M., 2025. What's next for AI in 2025. MIT Technology Review, 08.01.2025. [Võrgumaterjal] Leitav: https://www.technologyreview.com/2025/01/08/1109188/whats-next-for-ai-in-2025/ [Kasutatud 03.06.2025].

OECD, 2023. *OECD Digital Education Outlook 2023: Towards an Effective Digital Education Ecosystem*, OECD Publishing, Paris. https://doi.org/10.1787/c74f03de-en

Pickle, C., 2024. The Changing Character of Cyber Warfare. U.S. Naval Insisute Proceedings, 150/6/1456. [Võrgumaterjal] Leitav: https://www.usni.org/magazines/proceedings/2024/june/changing-character-cyber-warfare [Kasutatud 03.06.2025].

PST, 2025. Norwegian Police Security Service (PST). National Threat Assessment 2025. Oslo: Politiets Sikkerhetstjeneste. Leitav: https://www.pst.no/globalassets/2025/nasjonal-trusselvurdering-2025/_nasjonal-trusselvurdering-2025_uu-engelsk.pdf [Kasutatud 22.08.2025].

Puri, S., 2025. *President Trump's tariffs increase pressure on allies to reduce security dependence on the US*. Chatham House, 15. April 2025. [Võrgumaterjal] Leitav: https://www.chathamhouse.org/2025/04/president-trumps-tariffs-increase-pressure-allies-reduce-security-dependence-us [Kasutatud 12.08.2025].

Rassler, D. & Veilleux-Lepage, Y., 2025. „On the Horizon: The Ukraine War and the Evolving Threat of Drone Terrorism" *CTC Sentinel Combating Terrorism Center at West Point 18 (3).* Leitav: https://ctc.westpoint.edu/wp-content/uploads/2025/03/CTC-SENTINEL-032025_cover-article.pdf [Kasutatud 22.08.2025].

Riigi Infosüsteemi Amet, 2025. *Küberturvalisuse aastaraamat 2025*. [Võrgumaterjal] Leitav: https://www.ria.ee/kuberturvalisuse-aastaraamat-2025 [Kasutatud 16.05.2025].

Rohac, D., 2024. Chinese Influence in Central and Eastern Europe. American Enterprise Institute, September 11, 2024. [Võrgumaterjal] Leitav: https://www.aei.org/wp-content/uploads/2024/09/20240906-Testimony-Europe-subcommittee-DR-reviewed-final-edits-1.pdf?x85095 [Kasutatud 24.07.2025].

Roy, D., 2024. Why China remains unlikely to invade Taiwan. The Lowy Institute, 17.04.2024. [Võrgumaterjal] Leitav: https://www.lowyinstitute.org/the-interpreter/why-china-remains-unlikely-invade-taiwan [Kasutatud 13.05.2025].

Savimaa, R., Loik, R., 2023. Kogemused Eesti siseturvalisusele 2022. aastal Ukrainale konventsionaalset jätkuinvasiooni ettevalmistavast faasist. Tallinn: Sisekaitseakadeemia. [Võrgumaterjal] Leitav: https://digiriiul.sisekaitse.ee/handle/123456789/2990 [Kasutatud 16.05.2025].

Savimaa, R., Puusalu, J., Loik, R., Ringvee, R., Läänemets, M., Tammel, K., Kont, K-R. & Saar, J., 2024. *Sisejulgeoleku väliskeskkonna trendid ja prognoos*. Sisekaitseakadeemia. [Võrgumaterjal] Leitav: https://doi.org/10.15158/kkn4-nd47 [Kasutatud 15.03.2025].

Schroeder, D. T. et al., 2025. „How Malicious AI Swarms Can Threaten Democracy". https://doi.org/10.48550/arXiv.2506.06299

Serani, D., 2025. Affective polarization, political mistrust and populist attitudes: longitudinal evidence from Italy. *Contemporary Italian Politics*, pp. 1–22. https://doi.org/10.1080/23248823.2025.2475631

Shin, D. & Jitkajornwanich, K., 2024. How Algorithms Promote Self-Radicalization: Audit of TikTok's Algorithm Using a Reverse Engineering Method. *Social Science Computer Review,* Vol. 42 (4), pp. 1020–1040. https://doi.org/10.1177/08944393231225547

Suzan, S., & Bounfour, A., 2023. New oil map: Impact of Russia's war on Ukraine on supply and demand. European Federation for Transport and Environment AISBL. [Võrgumaterjal] Leitav: https://www.transportenvironment.org/uploads/files/202307_oil_imports_report_compressed.pdf [Kasutatud 12.08.2025].

Zandee, D., van der Meer, S., & Stoetman, A., 2022. Countering Hybrid Threats: Steps for Improving EU-NATO cooperation. Clingendael Report. Netherlands Institute of International Relations. [Võrgumaterjal] Leitav: https://www.clingendael.org/pub/2021/countering-hybrid-threats/ [Kasutatud 24.08.2025].

Zygar, M., 2024. "Russia's War on Woke: Putin Is Trying to Unite the Far Right and Undermine the West." Foreign Affairs, 02.01.2024. [Võrgumaterjal] Leitav: https://www.foreignaffairs.com/russian-federation/russias-war-woke [Kasutatud 24.08.2025].

Taylor, M., 2024. An AI Deepfake Could Be This Election's November Surprise. Time, 03.10.2024. [Võrgumaterjal] Leitav: https://time.com/7033256/ai-deepfakes-us-election-essay/ [Kasutatud 03.06.2025].

Vlassov, J., 2025. The Iron House: Geopolitical Stakes of the US-China AGI Race. [Võrgumaterjal] Leitav: https://www.convergenceanalysis.org/fellowships/international-security/the-iron-house-geopolitical-stakes-of-the-us-china-agi-race [Kasutatud 12.09.2025].

Välisluureamet, 2024. Eesti rahvusvahelises julgeolekukeskkonnas 2024. [Võrgumaterjal] Leitav: https://www.valisluureamet.ee/doc/raport/2024-et.pdf [Kasutatud 13.05.2025].

Välisluureamet, 2025. Eesti rahvusvahelises julgeolekukeskkonnas 2025. Tallinn: Välisluureamet. [Võrguteavik] Leitav: https://www.valisluureamet.ee/doc/raport/2025-et.pdf [Kasutatud 12.04.2025].

Walsh, N. P., 2025. China tells EU it can't accept Russia losing its war against Ukraine, official says. CNN, 04.07.2025. [Võrgumaterjal] Leitav: https://edition.cnn.com/2025/07/04/europe/china-ukraine-eu-war-intl [Kasutatud 12.09.2025].

World Economic Forum, 2020. *The Global Risks Report 2020*. [Võrgumaterjal] Leitav: https://www.weforum.org/publications/global-risks-report-2020 [Kasutatud 21.02.2025].

World Economic Forum, 2024. *The Global Risks Report 2024*. [Võrgumaterjal] Leitav: https://www.weforum.org/publications/global-risks-report-2024 [Kasutatud 21.02.2025].

World Economic Forum, 2025. Global Cybersecurity Outlook 2025. [Võrgumaterjal] Leitav: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ [Kasutatud 03.06.2025].

World Economic Forum, 2025. *The Global Risks Report 2025*. [Võrgumaterjal] Leitav: https://www.weforum.org/publications/global-risks-report-2025 [Kasutatud 21.02.2025].

Yarchi, M., Baden, C. & Kligler-Vilenchik, N., 2020. Political Polarization on the Digital Sphere: A Cross-platform, Over-time Analysis of Interactional, Positional, and Affective Polarization on Social Media. *Political Communication*, Vol. 38(1–2), pp. 98–139. https://doi.org/10.1080/10584609.2020.1785067

LISAD

LISA 1. METOODIKA

Arengutrendide ülevaate koostamisel (kuni aastani 2030) on arvestatud pika ajahorisondi prognoosimisega kaasnevat suurt ebakindlust, mistõttu kombineeriti analüüsi kvaliteedi tagamiseks nelja täiendavat meedet: diskussioonipõhine tööprotsess (sh erialaekspertide küsitlus), tunnustatud prognooside sisendina kasutamine, erinevate kategooriate eristamine ja riskide avaldumise tõenäosuse hindamine.

Siinse uuringu põhialuseks on Maailma Majandusfoorumi GLOBAL RISK PERCEPTION SURVEY (GRPS) (*Globaalne riskide aruanne 2024)* riskihinnangud viies põhivaldkonnas, mida on täiendatud European University Institute (EUI) poolt koostatud dokumendi „Global Risks to the EU 2025" mõjuhinnangutega, mille realiseerumisest tulenevat võimalikku mõju Eestile hinnati eraldiseisvalt. Selleks et koostada võimalikult adekvaatne riskide ja nende realiseerumise mõju koondpilt, viidi mõjude hindamiseks lisaks läbi täiendav küsitlus, millele vastasid Eesti eri valdkondade eksperdid. Ekspertide valikul lähtuti põhimõttest, et kaasatud oleksid keskkonna, tehnoloogia, majanduse, sotsiaalteaduste ja geopoliitiliste teadmistega spetsialistid. Sihipärase valimiga kaasatud akadeemilise, era- ja avaliku sektori taustaga 24 Eesti erialaeksperti hindasid 2025. aasta aprillis 29 eelnevalt kindlaks määratud globaalset riski kahest aspektist: riski realiseerumise tõenäosust ja selle eeldatavat mõju Eesti jaoks 5–7 aasta perspektiivis. Keskkonnaga seonduvaid riske ja realiseerumise tõenäosust paluti lisaks 5–7 aasta perspektiivile hinnata ka 10–50 aasta perspektiivis.

29 määratletud riski jagunesid järgmistesse valdkondadesse (vt täpsemalt lisa 2):

- sotsiaalsed ja ühiskondlikud riskid;
- majanduslikud riskid;
- geopoliitilised riskid;
- keskkonnaga seotud riskitegurid;
- tehnoloogilised riskid.

Iga valdkonna trendide/riskide realiseerumise tõenäosust ja selle võimalikku mõju Eestile hinnati järgmisel skaalal:

MINIMAALNE	VÄHENE	KESKMINE	SUUR	VÄGA SUUR

Valdkondade trendide kajastamisel lähtuti eelkõige riigi sisejulgeolekut mõjutavatest aspektidest ja raportis kirjeldati saadud tulemuste põhjal detailsemalt Eesti jaoks potentsiaalselt kõige suurema mõjuga viie globaalse riski hindamise tulemusi.

LISA 2. GLOBAALSETE RISKIDE MÄÄRATLUSED

(GLOBAL RISK PERCEPTION SURVEY 2024 järgi)

SOTSIAALSED JA ÜHISKONDLIKUD RISKID

Tervise ja heaolu langus
Regulaarne või krooniline mõju füüsilisele ja vaimsele tervisele ning heaolule, mis eeldab arstiabi ja/või piirab igapäevaelu tegevusi. Siia kuuluvad muu hulgas vananemisega seotud seisundid, liigsed tarbimisharjumused, kliimamuutused (sealhulgas kuumalained) ja saaste.

Inimõiguste ja/või kodanikuvabaduste kahjustamine
Kõigile inimestele, olenemata nende staatusest, omaste õiguste ja/või kodanikuvabaduste kaitse puudumine. Siia kuuluvad muu hulgas õigus elule ja vabadusele, tööle ja haridusele, sõnavabadus, rahumeelsed rahvakogunemised, mittediskrimineerimine soo, rassi, etnilise päritolu ja muude tunnuste alusel ning eraelu puutumatus.

Ebavõrdsus (jõukus, sissetulek)
Olulised erinevused varade, jõukuse või sissetuleku jaotuses riikide sees või riikide vahel, mille tulemuseks on erinevused majandustulemustes. Siia kuuluvad muu hulgas kasvav või püsiv vaesus ja majanduslik polariseerumine.

Nakkushaigused
Viiruste, parasiitide, seente või bakterite levik, mis põhjustab ulatuslikke inimkaotusi ja majandushäireid. Siia kuuluvad muu hulgas zoonootilised haigused, looduslike või inimtekkeliste haigustekitajate levik, juba olemasolevate haiguste taastekkimine immuunsuse vähenemise tõttu, antimikroobse resistentsuse suurenemine ning kliimamuutuste ja keskkonnaseisundi halvenemise mõju haigustekitajatele.

Ebapiisav avalik infrastruktuur ja sotsiaalne kaitse
Olematu, ebapiisav või paratamatu avalik infrastruktuur, teenused ja sotsiaalne kaitse. Siia kuuluvad muu hulgas kättesaamatu või ebapiisav sotsiaalkindlustus ja -hüvitised, eluase, riiklik haridus, laste ja eakate hooldus, tervishoiu-, sanitaar-, transpordi- ja pensionisüsteemid.

Majanduslike võimaluste puudumine või tööpuudus
Tööalaste väljavaadete või tööstandardite halvenemine ja/või püsivad tõkked majandusliku potentsiaali ja turvalisuse realiseerimisel. Siia kuuluvad muu hulgas töötajate õiguste vähenemine, palgapoliitika stagneerumine, kasvav töötuse määr ja tööpuudus, automatiseerimisest või rohepöördest põhjustatud ümberasumine, stagneerunud sotsiaalsüsteem ning ebavõrdne juurdepääs hariduslikele, tehnoloogilistele ja majanduslikele võimalustele.

Sunniviisiline ränne või ümberasumine
Sunniviisiline riigisisene ja piiriülene ümberasumine, mis on tingitud muu hulgas pidevast diskrimineerimisest ja tagakiusamisest, majanduslike arenguvõimaluste puudumisest, inimtegevusest põhjustatud katastroofidest, loodusõnnetustest ja äärmuslikest ilmastikunähtustest (sh kliimamuutuste mõju), riigisisestest või riikidevahelistest konfliktidest.

Ühiskonna polariseerumine
Ideoloogilised ja kultuurilised lahkarvamused kogukondades ja kogukondade vahel, mis toovad kaasa sotsiaalse stabiilsuse languse, otsuste langetamise võimetuse, majanduslikud häired ja suurenenud poliitilise polariseerumise.

TEHNOLOOGILISED RISKID

Tehisintellektitehnoloogiate negatiivsed tagajärjed
Tehisintellekti edusammude ja sellega seotud tehnoloogiliste võimaluste (sealhulgas generatiivse tehisintellekti) arenguga kaasnevad tahtmatud või soovimatud negatiivsed tagajärjed üksikisikutele, ettevõtetele, ökosüsteemidele ja/või majandusele.

Kõrgtehnoloogiate negatiivsed tagajärjed (kvant-, bio-, geotehnoloogia)
Kõrgtehnoloogiate arengu kavandatud või soovimatud negatiivsed tagajärjed üksikisikutele, ettevõtetele, ökosüsteemidele ja/või majandusele. Siia kuuluvad muu hulgas aju/arvuti süsteemiliidesed, biotehnoloogia, geotehnoloogia ja kvantsüsteemid.

Tsensuur ja jälgimine
Koha või isiku ulatuslik ja kõikehõlmav jälgimine ja/või suhtluse, teabe ja ideede füüsiline või digitaalne mahasurumine, mis rikub oluliselt inim- ja kodanikuõigusi (nt eraelu puutumatust ja sõnavabadust).

Küberspionaaž ja -sõjad
Küberrelvade ja -vahendite kasutamine riiklike ja valitsusväliste osalejate poolt, et saavutada kontroll digitaalse kohaloleku üle, põhjustada häireid tegevuses ja/või kahjustada üksuse tehnoloogilisi- ja infovõrke ning infrastruktuuri. Siia kuuluvad kaitsvad ja ründavad küberoperatsioonid, mis toimuvad relvakonflikti ajal või vallandavad selle, ning küberrünnakud, millega varastatakse salastatud, tundlikke andmeid või intellektuaalomandit.

Väärinfo ja desinformatsioon
Pidev laialdane meediavõrgustike kaudu valeteabe levitamine, kallutades avalikku arvamust olulisel määral faktide ja autoriteedi usaldamatuse suunas. Siia kuuluvad muu hulgas valeinformatsioon, võltsitud, manipuleeritud ja fabritseeritud sisu.

Veebipõhised ohud
Kahjuliku käitumise kaitse nõrgenemine ja/või kahjuliku käitumise levik, mis kujutab endast digitaalset ohtu üksikisikute emotsionaalsele või vaimsele tervisele ja heaolule. Siia kuuluvad muu hulgas laste seksuaalne kuritarvitamine internetis, ahistamine internetis ja küberkiusamine.

GEOPOLIITILISED RISKID

Riikidevahelised relvastatud konfliktid (repressioonid, kodusõjad, riigipöörded, terrorism jne)
Kahe- või mitmepoolne jõu kasutamine riikide vahel ja/või riigi ja valitsusvälise(te) osaleja(te) vahel, sageli ideoloogiliste, poliitiliste või religioossete eesmärkidega, mis väljendub sõjana ja/või organiseeritud, kestva vägivallana. Siia kuuluvad muu hulgas aktiivne sõjategevus, sissisõjad, kodusõjad, genotsiidid, terrorism ja atentaadid.

Bioloogilised, keemia- ja tuumarelvad või ohud
Bioloogiliste, keemiliste, tuuma- või radioloogiliste ohtude tahtlik või juhuslik keskkonda viimine, mille tulemuseks on inimohvrid, hävitamine ja/või rahvusvahelised kriisid. Siia kuuluvad muu hulgas õnnetused või sabotaaž biolaboratooriumides, keemiatehastes ja tuumaelektrijaamades ning bioloogiliste, keemiliste ja tuumarelvade tahtlik või juhuslik keskkonda viimine.

Geoökonoomiline vastasseis (sanktsioonid, tariifid, investeeringute kontroll)
Majanduslike mõjutusvahendite kasutamine globaalsete või piirkondlike võimude poolt, et kujundada ümber riikidevahelist majanduslikku suhtlust, piirates kaupade, teadmiste, teenuste või tehnoloogiate liikumist ja levikut eesmärgiga suurendada iseseisvust, piirata geopoliitilisi konkurente ja/või tugevdada mõjusfääri. Siia kuuluvad muu hulgas valuutameetmed, investeeringute kontroll, sanktsioonid, riigiabi ja subsiidiumid ning kaubanduskontroll.

Riigisisene vägivald (rahutused, massitulistamised, jõukude vägivaldne käitumine jne)
Riigi või kogukonna sees toimuv jõu kasutamine, mille tulemuseks on inimohvrid, tõsised vigastused või materiaalne kahju. Hõlmab muu hulgas massitulistamisi ja kuritegusid, mis ähvardavad või põhjustavad kogukonnale füüsilist kahju, nagu jõuguvägivald, sooline vägivald ja inimröövid.

KESKKONNAGA SEOTUD RISKITEGURID

Bioloogilise mitmekesisuse vähenemine ja ökosüsteemi kokkuvarisemine
Tõsised tagajärjed keskkonnale, inimkonnale ja majandustegevusele, mis tulenevad liikide väljasuremisest või vähenemisest tingitud looduskapitali hävimise tõttu, hõlmates nii maismaa- kui ka mereökosüsteeme.

Kriitiline muutus planeedi toimesüsteemides
Pikaajalised, potentsiaalselt pöördumatud ja taastumatud muutused olulise tähtsusega planeedisüsteemides, mis tulenevad klimaatilise või ökoloogilise lävendi või murdepunkti ületamisest piirkondlikul või globaalsel tasandil. Hõlmab muu hulgas merepinna tõusu sulavate liustike tõttu, süsiniku vabanemist igikeltsa sulamisest ja ookeani või atmosfääri hoovuste ja voolude häirimist.

Äärmuslikud ilmastikunähtused (üleujutused, kuumalained jne)
Inimelude kaotus, ökosüsteemide kahjustamine, vara hävitamine ja/või rahaline kahju äärmuslike ilmastikunähtuste tõttu. Hõlmab muu hulgas maismaapõhiseid (nt metsatulekahjud), veepõhiseid (nt üleujutused) ning atmosfääri ja temperatuuriga seotud (nt kuumalained) sündmusi, sealhulgas neid, mida kliimamuutus süvendab.

Loodusressursside nappus (toit, vesi)
Toidu- või veepuudus inimeste, tööstuse või ökosüsteemi tarbeks, mis väljendub toidu- ja veepuuduses kohalikul, piirkondlikul või ülemaailmsel tasandil. Tuleneb muu hulgas järgmistest põhjustest: kriitiliste loodusvarade liigne kasutamine ja väärkasutus inimeste poolt, kliimamuutus (sealhulgas põud ja kõrbestumine) ja/või sobiva infrastruktuuri puudumine.

Ilmastikuga mitteseotud looduskatastroofid (maavärinad, vulkaanid, tsunamid, päikesepursked jne)
Inimelude kaotus, ökosüsteemide kahjustamine, vara hävimine ja/või rahaline kahju ilmastikuga mitteseotud loodusõnnetuste tõttu. Hõlmab muu hulgas maismaapõhiseid (nt maavärinad, vulkaanid), veepõhiseid (nt tsunamid) ja maaväliseid (nt asteroidi tabamused ja geomagnetilised tormid) sündmusi.

Reostus (õhk, pinnas, vesi jne)
Inimtegevusest tulenevate kahjulike materjalide sattumine õhku, vette ja pinnasesse, mille tagajärjeks on inimelude kaotus, rahaline kahju ja/või ökosüsteemide kahjustamine. Hõlmab muu hulgas majapidamis- ja tööstustegevust, keskkonnaõnnetusi, näiteks naftareostust ja radioaktiivset saastumist.

MAJANDUSLIKUD RISKID

Varahindade mulli lõhkemine
Eluaseme, investeerimisfondide, aktsiate ja muude varade hinnad kaotavad üha enam seose reaalmajandusega, mis toob kaasa nõudluse ja hindade tõsise languse. Siia kuuluvad muu hulgas krüptovaluutad, eluasemehinnad ja aktsiaturud.

Strateegiliste ressursside ja tehnoloogiate koondumine
Strateegiliselt oluliste ressursside (mineraalid, materjalid, tehnoloogiad) koondumine väikese arvu üksikisikute, ettevõtete või riikide kätte, kes saavad kontrollida juurdepääsu ja dikteerida hinnakujundust.

Kuritegevus ja ebaseaduslik majandustegevus (sh küberkuritegevus)
Organiseeritud kuritegevuse ülemaailmne levik või ettevõtete ja üksikisikute ebaseaduslik tegevus, mis õõnestab majanduslikku arengut ja kasvu (sh digitaalne). Siia kuuluvad muu hulgas ebaseaduslikud rahavood (nt maksudest ja sanktsioonidest kõrvalehoidumine, rahapesu), ebaseaduslik kaubandus ja salakaubandus (nt võltsimine, inimkaubandus, looduslike liikide ja relvadega kauplemine) ning küberkuritegevus (sh lunavara, andmevargused ja internetipettused).

Võlataseme kasv (avalik-õiguslik, ettevõtete ja kodumajapidamiste võlg)
Ettevõtetel, kodumajapidamistel või riigil on raskusi kuhjunud võlgade teenindamisega, mille tulemuseks on massilised pankrotid või maksejõuetus, likviidsuskriisid või makseviivitused ja riigivõlakriisid.

Olulise tarneahela häired
Süsteemselt olulise ülemaailmse tarneahela või tööstusharu tõsine häire või kokkuvarisemine, mis mõjutab maailmamajandust, finantsturge või ühiskonda ning põhjustab järsu šoki elutähtsate kaupade ja teenuste pakkumisele ja nõudlusele ülemaailmsel tasandil. Siia kuuluvad muu hulgas energia, tehnoloogiline riistvara, meditsiinitarbed ja kiirtarnet nõudvad tarbekaubad.

Kriitilise infrastruktuuri häired
Füüsilise ja digitaalse infrastruktuuri (sealhulgas satelliitide) või elutähtsate süsteemide, sealhulgas interneti, telekommunikatsiooni, kommunaalteenuste, finantssüsteemide või energiasüsteemide ülekoormus või seiskumine, mis tuleneb muu hulgas küberrünnakutest, tahtlikust või tahtmatust füüsilisest kahjustamisest, äärmuslikest ilmastikuoludest ja loodusõnnetustest.

Majanduslangus
Mitmeid aastaid kestev nullilähedane või aeglane ülemaailmne majanduskasv või ülemaailmne majanduslangus.

Inflatsioon
Kaupade ja teenuste hindade püsiv tõus. Hõlmab võimalust, et suur osa elanikkonnast ei suuda kahaneva ostujõu tõttu säilitada olemasolevat elustandardit.

Talentide ja/või tööjõu puudus
Ülemaailmne, geograafiline või tööstusharudevaheline ebakõla tööjõu ja oskuste pakkumise ja nõudluse vahel.

EDUKA RISKIJUHTIMISE VÕTMEKS ON VÕIMEKUS NÄHA ETTE VÕIMALIKKE TULEVIKUSTSENAARIUME JA TEADUSEL ON SELLES ÜLIOLULINE ROLL.

Eesti sisejulgeolekut mõjutavate globaalsete arengutrendide viie aasta (2026–2030) prognoosi eesmärk on pakkuda teaduspõhist strateegilist sisendit Eesti (sise)julgeolekupoliitika arendamiseks.

2025. aasta alguses viis Sisekaitseakadeemia sisejulgeoleku instituudi teaduskeskus läbi uuringu, mille käigus hinnati Eesti erialaekspertide abiga kõige tõenäolisemalt realiseeruda võivaid globaalseid riske ja nende võimalikku mõju Eestile. Riskide ja nende mõju hindamisel võeti ajahorisondina fookusesse kesk-pikk perspektiiv (5–7 aastat) ning need järjestati realiseerumise tõenäosuse ja Eesti jaoks võimaliku mõju ulatuse alusel. Uuringu tulemusena saadud viie kõige suurema mõjuga riski ja nende võimaliku koosmõju kohta lisasid Sisekaitseakadeemia teadlased omapoolse analüüsi ja selgitused.

sisekaitse.ee

ISBN 978-9985-67-530-4

9 789985 675304