C/2026/3795

16.7.2026

EUROOPA SÜSTEEMSETE RISKIDE NÕUKOGU HOIATUS,

25. juuni 2026,

eesliini tehisintellektimudelitest tulenevate süsteemsete küberriskide kohta

(ESRN/2026/3)

(C/2026/3795)

EUROOPA SÜSTEEMSETE RISKIDE NÕUKOGU HALDUSNÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Majanduspiirkonna lepingut ([1]), eelkõige selle IX lisa,

võttes arvesse Euroopa Parlamendi ja nõukogu määrust (EL) nr 1092/2010, 24. november 2010, finantssüsteemi makrotasandi usaldatavusjärelevalve kohta Euroopa Liidus ja Euroopa Süsteemsete Riskide Nõukogu asutamise kohta ([2]), eelkõige selle artikli 3 lõike 2 punkti c ning artikleid 16 ja 18,

võttes arvesse Euroopa Süsteemsete Riskide Nõukogu otsust ESRB/2011/1, 20. jaanuar 2011, millega võetakse vastu Euroopa Süsteemsete Riskide Nõukogu töökord ([3]), eelkõige selle artikleid 18 ja 19,

ning arvestades järgmist:

(1) Juhtivad tehisintellekti pakkujad on välja töötanud eesliini tehisintellektimudelid (*Frontier AI Models*, edaspidi FAIM), mis on küberturvalisuse valdkonnas väga võimekad ning võimelised korraldama täielikult automatiseeritud küberründeid keerukate süsteemide vastu, sealhulgas haavatavuste avastamise ning eksploitide välja töötamise ja relvana kasutamise kaudu, muutes seeläbi põhjalikult küberohtude keskkonda.

(2) FAIMid on märkimisväärselt paremad kui varasemad tehisintellektimudelid uute küberrünnete korraldamise viiside leidmisel, ületades varasemaid mudeleid nii hinna, kiiruse kui täpsuse poolest ning konkureerides nüüd inimestest tippekspertidega.

(3) FAIMid võivad ohustada info- ja kommunikatsioonitehnoloogia (IKT) keskkondade alussüsteeme, millele finantstaristu tugineb, suurendades süsteemse mõjuga küberintsidentide tõenäosust ja tõsidust.

(4) FAIMid on näidanud, et nad suudavad avastada haavatavusi ja töötada välja uudseid eksploite, seades seeläbi küberründe ohtu peamised operatsioonisüsteemid ja tarkvara, mida kasutatakse peaaegu kõikide organisatsioonide IKT-keskkondades.

(5) Ajalooliselt on selliseid haavatavusi avastatud harva, sageli turbevaldkonna töötajate poolt, mis on omakorda võimaldanud välja töötada sihtotstarbelisi parandusmeetmeid. Sellistel juhtudel antakse tarkvara pakkujatele sageli standardne tähtaeg – tavaliselt 90 päeva – haavatavuse parandamiseks enne selle avalikustamist. Samas suurendavad FAIMid tõenäoliselt tuvastatud haavatavuste mahtu.

(6) Finantssüsteemi praegused paikamistavad on valdavalt reageerivat laadi, tuginedes perioodilistele ajakohastustele ja *ad hoc* reaktsioonile avalikustatud haavatavustele. Selline lähenemine toimib ohukeskkonnas, kus haavatavuse avastamine on ajaliselt hallatav. Haavatavuste mahu kasvamisel võivad praegused tavad aga osutuda ebapiisavaks tegevuskerksuse säilitamisel.

(7) Samuti võib haavatavuste mahu kasv põhjustada praeguste paikamisprotsesside ülekoormamist, kuna nendes seatakse esikohale riskil põhinevad parandusmeetmed ja nõutakse tarkvaraparanduste testimist enne rakendamist, et tagada operatsioonide stabiilsus. Kui lühikese aja jooksul avastatakse liiga palju kriitilise tähtsusega haavatavusi ja vajalike kriitilise tähtsusega tarkvaraparanduste arv suureneb märkimisväärselt, võivad finantsasutused olla sunnitud otsustama, kas jätta end oluliste küberriskide meelevalda või vähendada paranduste testimise nõudeid, millega kaasneb operatiivintsidentide ja katkestuste oht.

([1]) EÜT L 1, 3.1.1994, lk 3, ELI: http://data.europa.eu/eli/agree_internation/1994/1/oj.
([2]) ELT L 331, 15.12.2010, lk 1, ELI: http://data.europa.eu/eli/reg/2010/1092/oj.
([3]) ELT C 58, 24.2.2011, lk 4.

(8) Varem meisterdati relvana kasutatavaid eksploite suuresti käsitsi ning selleks kulus inimekspertidel päevi või nädalaid; nüüd oskavad FAIMid seda teha mõne minuti või tunniga. See tähendab parandamise ajal kriitilise tähtsusega ja oluliste funktsioonide järjepidevuse säilitamiseks vajalike kaitseotstarbeliste ajaliste puhvrite kokkukuivamist.

(9) Tehisintellekti abil relvana kasutatavate eksploitidega kaasnevate kriitilise tähtsusega haavatavuste levik ja kaitseotstarbeliste ajaliste puhvrite kahanemine suurendab järsult ohtu üksikutele kriitilise tähtsusega või olulistele funktsioonidele ja asutustele. Kui asjaomased riskid realiseeruvad nende funktsioonide ja asutuste lõikes üheaegselt, võib see kaasa tuua süsteemse küberriski püsiva suurenemise, mille jaoks ei ole praegu tõhusat riskimaandamisraamistikku. Liidu finantssektori ning muude sektorite ja jurisdiktsioonide tugeva omavahelise seotuse tõttu kujutab selline olukord süsteemset riski ja võib tekitada süsteemset haprust.

(10) Lisaks töötavad FAIMe praegu välja vaid vähesed tehisintellekti pakkujad, kellest nii mõnigi on väljendanud muret, et tulevased FAIMid võivad olla piiramatuks avalikuks juurdepääsuks liiga võimsad.

(11) Juba praegu kasutavad pahatahtlikud tegutsejad tehisintellekti küberrünnete tõhustamiseks. On tõenäoline, et pahatahtlikele tegutsejatele muutuvad lõpuks kättesaadavaks – kas lekete, varguse, iseseisva arendustöö või avatud juurdepääsu kaudu – ka tehisintellektimudelid, mille võimekus on võrreldav praegu kontrollitud kaitsekeskkondades kasutatavate mudelitega.

(12) Kuigi FAIMid võivad märkimisväärselt suurendada ründevõimet ja keerukate küberrünnete tõenäosust, tugevdavad need ka kaitsevõimet, eelkõige tulenevalt haavatavuste avastamise, andmete korrelatsiooni ja parandusmeetmete rakendamisega üksikutes asutustes. Lühikeses ja keskpikas perspektiivis kaalub ründevõime kiiruse, ulatuse ja täpsuse suurenemine siiski tõenäoliselt üles sellest saadava kasu.

(13) FAIMide kiire arengu tõttu on vaja viivitamata käsitleda tuvastatud finantsstabiilsust ohustavaid riske, et vältida nende realiseerumist või vähemalt leevendada nende võimalikku mõju. Liidu finantsturgude finantsstabiilsuse tagamiseks peaksid kõik Euroopa Süsteemsete Riskide Nõukogu (ESRN) liikmed oma makrotasandi usaldatavusmeetmete ja mikrotasandi poliitikameetmete raames kaaluma FAIMide mõju finantsasutuste talitlus- ja vastupanuvõimele. See ei piira liidu keskpankade rahapoliitilisi volitusi. Näiteks on EKP teiste asutuste praeguste algatuste kõrval pangandusjärelevalve rollis palunud olulistel finantsinstitutsioonidel viivitamata hinnata muutuva ohuolukorra mõju ja töötada 31. oktoobriks 2026 välja põhjalik tegevuskava, milles kirjeldatakse konkreetseid meetmeid asjaomaste riskide käsitlemiseks ([4]).

(14) Tehisintellekti tehnoloogia levides on oluline tagada, et kogu elutähtis taristu ning eelkõige finantsasutused oleksid valmis toime tulema FAIMide abil läbiviidavate küberrünnetega ning tegema aja- ja asjakohaseid ettevalmistusi. Sellised üksikute üksuste kaitsepüüdlused ei ole siiski piisavad. Tulemuslikuks reageerimiseks ja riskide maandamiseks on vaja koordineeritud lahendust, mis hõlmab kõiki mõjutatud isikuid, sealhulgas tehisintellekti pakkujaid, tarkvarapakkujaid, turvaettevõtteid, avatud lähtekoodiga tarkvara hooldajaid, finantsasutusi ja ametiasutusi nii riikide kui ka liidu tasandil.

(15) Eelnimetatud küsimuste käsitlemisel on oluline meelde tuletada asjakohaseid liidu õigus- ja poliitikaraamistikke, eelkõige Euroopa Parlamendi ja nõukogu määrust (EL) 2022/2554 ([5]), Euroopa Parlamendi ja nõukogu määrust (EL) 2024/1689 ([6]), Euroopa Parlamendi ja nõukogu määrust (EL) 2024/2847 ([7]) ning Euroopa Süsteemsete Riskide Nõukogu soovitust (ESRN/2021/17) ([8]).

([4]) Olulistele finantsinstitutsioonidele adresseeritud kiri on avaldatud EKP pangandusjärelevalve veebilehel www.bankingsupervision.europa.eu.

([5]) Euroopa Parlamendi ja nõukogu määrus (EL) 2022/2554, 14. detsember 2022, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Euroopa Parlamendi ja nõukogu määrus (EL) 2024/1689, 13. juuni 2024, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ning muudetakse määruseid (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ning direktiive 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828) (tehisintellekti käsitlev määrus) (ELT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Euroopa Parlamendi ja nõukogu määrus (EL) 2024/2847, 23. oktoober 2024, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrusi (EL) nr 168/2013 ja (EL) 2019/1020 ning direktiivi (EL) 2020/1828 (küberkerksuse määrus) (ELT L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Euroopa Süsteemsete Riskide Nõukogu soovitus, 2. detsember 2021, seoses üleeuroopalise süsteemsete küberintsidentide koordineerimisraamistikuga asjaomastele asutustele (ESRN/2021/17) (ELT C 134, 25.3.2022, lk 1).

(16) Määrusega (EL) 2022/2554 on finantsasutustele ette nähtud terviklik raamistik IKT-riskide, sealhulgas küberrünnetest tulenevate riskide tuvastamiseks, juhtimiseks, jälgimiseks ja maandamiseks. Võttes arvesse finantssektori omavahelist seotust ning sõltuvust IKT-süsteemidest ja kolmandast isikust teenuseosutajatest, võib edukal küberründel, mis mõjutab üht või mitut finantsasutust või nende kriitilise tähtsusega teenuseosutajaid, olla märkimisväärne süsteemne mõju. Finantsjärelevalveasutused peaksid pöörama asjakohast tähelepanu järelevalvetegevusele selles valdkonnas, võttes arvesse küberrünnete võimalikku mõju finantssüsteemi stabiilsusele, terviklikkusele ja usaldusväärsusele ning sellest tulenevat võimalikku tegevus-, finants- ja tarbijakahju.

(17) Määrusega (EL) 2024/1689 on kehtestatud tehisintellektisüsteemide ja üldotstarbeliste tehisintellektimudelite liidus turule laskmise, kasutusele võtmise ja kasutamise ühtlustatud normid, sealhulgas teatavatel asjaoludel süsteemid ja mudelid, mida pakuvad kolmandates riikides asutatud tehisintellekti pakkujad, kui tehisintellektisüsteemi toodetud väljundit kasutatakse liidus või tehisintellektimudel on integreeritud liidu turule lastud süsteemi. Kõnealuse määrusega sätestatakse ka erinormid – sealhulgas rangem regulatiivne kord – süsteemse riskiga üldotstarbelisteks tehisintellektimudeliteks liigitatud mudelite jaoks.

(18) Määrusega (EL) 2024/2847 kehtestatakse tootjatele kohustuslikud küberturbenõuded, mis hõlmavad liidu turule lastud digielemente sisaldavate riist- ja tarkvaratoodete kavandamist, projekteerimist, arendamist ja hooldust. Samuti nõutakse selles, et tootjad käsitleksid haavatavusi oma toodete olelusringi jooksul. Kui määrust 2027. aasta detsembris täielikult kohaldama hakatakse, peavad selliseid tooteid liidu turule laskvad finantssektori ettevõtjad ka tagama, et need tooted vastavad kohaldatavatele nõuetele.

(19) Soovituses ESRN/2021/17 soovitati Euroopa järelevalveasutustel koostöös ühiskomiteega ning Euroopa Keskpanga (EKP), ESRNi ja asjaomaste riiklike asutustega välja töötada tõhus liidu tasandi koordineeritud reageerimine suure piiriülese küberintsidendi või sellega seotud ohu korral, millel võib olla süsteemne mõju liidu finantssektorile. Selle tulemusena loodi üleeuroopaline süsteemne küberintsidentide koordineerimisraamistik (EU-SCICF), mis on väärtuslik ja operatiivne platvorm teabevahetuseks ja koordineerimiseks finantsasutuste vahel.

(20) Seda arvesse võttes annab ESRN käesolevaga üldise hoiatuse, milles käsitletakse olulisi finantsstabiilsuse riske, mida FAIMide areng võimendab. Hoiatus tugineb analüüsidele, mis on esitatud ESRNile 2026. aasta juunis avaldatud teatises kübersuutlikkusega eesliini tehisintellektimudelite käsitlemise kohta finantsstabiilsuse seisukohast ([9]),

ON VASTU VÕTNUD KÄESOLEVA HOIATUSE:

1. JAGU

Hoiatus

Uus riskikeskkond

Kübersuutlikkusega eesliini tehisintellektimudelite (*Frontier AI Models*, edaspidi FAIMid) kiire areng muudab oluliselt liidu finantssüsteemi riskikeskkonda. Praegused tõendid näitavad, et FAIMid on võimelised avastama haavatavusi, töötama välja toimivaid eksploite ning iseseisvalt toime panema täiemahulisi küberründeid kiiruse, ulatuse ja täpsusega, mis kõrgelt ületab varasemaid tehisintellektimudeleid. Tegemist on paradigma muutusega küberturbe valdkonnas ja pöördepunktiga tehisintellekti võimekuse valdkonnas.

ESRN on seisukohal, et asjaomased arengud põhjustavad finantssüsteemile süsteemseid riske, mis võivad avaldada märkimisväärset kahjulikku mõju küberturvalisusele, tulenevalt kiiremast haavatavuste avastamisest ning reageerimiseks ja tõhusa kaitse loomiseks eraldatava aja lühenemisest, küberrünnete suuremast ulatusest ja keerukusest ning uute sõltuvuste ja kontsentratsiooniriskide tekkimisest finantssüsteemis. Kuigi ESRN on täheldanud ka FAIMidest tulenevat finantsasutuste kaitsevõime tugevnemist, realiseerub see võimekus lähiaastatel tõenäoliselt järk-järgult, nõudes finantsasutustelt tegutsemist üleminekuperioodil, mida iseloomustavad kõrgendatud risk, suur ebakindlus ja kiiresti arenev tehnoloogiline keskkond. Finantssüsteemi digitaalset ja läbipõimunud olemust arvestades võib kahjulik mõju küberturvalisusele kiiresti levida, mõjutades kriitilise tähtsusega ja olulisi funktsioone kõikides finantsasutustes, põhjustades lõppkokkuvõttes süsteemseid häireid ja usalduse kaotust finantssüsteemi vastu.

([9]) Avaldatud ESRNi veebilehel www.esrb.europa.eu.

Uued FAIMid suurendavad olemuslikku IKT-riski, mis nõrgendab finantssektori tegevuskerksust, eelkõige neljas valdkonnas: a) aeg, sealhulgas võime kiiresti ja talitlushäiret põhjustamata paigata keerukaid süsteeme, võttes arvesse kaitseotstarbeliste ajaliste puhvrite kokkukuivamist haavatavuse avastamise ja eksploidi relvana kasutamise vahel; b) kaitsjate suutlikkus, sealhulgas nende võime viia FAIMi abil läbi automatiseeritud ja manuaalseid turvateste ning kaitsta ja avastada FAIMi pahatahtlikust kasutamisest tulenevaid ohte ja neile reageerida; c) kontsentratsioon, sealhulgas sõltuvus piiratud arvust tehisintellekti pakkujatest, kes omakorda sõltuvad pilveteenuste pakkujatest, avatud lähtekoodiga komponentidest ja muust laialdaselt kasutatavast tarkvarast; ja d) ametiasutuste võimekus, sealhulgas FAIMide arengule vastav ootuste kalibreerimine, stressitestimine ja valmisolekumeetmed, et talitlushäired ei muutuks laiema ebastabiilsuse allikaks.

Lisaks on keeruline tagada ja säilitada tehisintellekti kasutuselevõtmise nähtavust mis tahes finantsasutuses, sealhulgas täielikult mõista, kus ja kuidas tehisintellekti kasutatakse, arvestades, et seda kasutatakse kliendiliidestes, siseagentides, äriprotsessides ja integreerimisel kolmandate isikutega.

Süsteemne hindamine

Tuvastatud arengud võivad oluliselt muuta nii küberriski ulatust kui ka struktuuri, suurendades nii otseseid kui ka kaudseid riske finantsstabiilsusele. FAIMi võimekus võib seada olemasolevad kerksusraamistikud märkimisväärse surve alla, eriti kui intsidendid levivad laialt ja toimuvad üheaegselt. Intsidendid võivad kiiresti levida ka finantsasutustes ja -turgudel, kui need mõjutavad kriitilise tähtsusega kolmandast isikust teenuseosutajaid, ühiseid tehnoloogilisi ökosüsteeme või laialdaselt kasutatavaid avatud lähtekoodiga komponente, suurendades sellega kaasnevate süsteemse mõjuga häirete ohtu.

FAIMid muudavad finantssektoris kolme asümmeetria allikat: esiteks asümmeetria jurisdiktsioonide vahel, teiseks asümmeetria kaitsjate ja ründajate vahel ning kolmandaks asümmeetria suuremate ressursside ja vähemate vahenditega varustatud finantsasutuste vahel.

Esiteks tekitab juhtivate tehisintellekti pakkujate praegune geograafiline koondumine väljapoole liitu strateegilist sõltuvust ja geopoliitilist riski. Jurisdiktsioonide vaheliste teadmiste ja tehnoloogilise asümmeetria leevendamiseks on vaja võtta meetmeid, et hõlbustada liidu ja selle liikmesriikide piisavat ja proportsionaalset juurdepääsu hiljuti välja töötatud FAIMidele. Asjaomased meetmed peaksid olema õigeaegsed, sidusad ja tõhusad nii poliitika kujundamise kui ka rakendamise seisukohast ning neis tuleks piisavalt arvesse võtta liidu erinevaid finantssektoreid, kasutades ära vastavate Euroopa järelevalveasutuste eksperditeadmisi. See leevendaks mitte ainult asümmeetriat liidu ja kolmandate riikide jurisdiktsioonide vahel, vaid ka eri liikmesriikides asutatud finantsasutuste vahel, säilitades võrdsed tingimused liidus ja liiduväliselt ning vähendades süsteemset riski. Kord, mis hõlbustab juurdepääsu FAIMidele ainult teatavate finantsinstitutsioonide kategooriate jaoks või valitud jurisdiktsioonides, tekitaks ühtse rahandusturu killustumist, vähendades selle likviidsust ja sügavust.

Teiseks, mis puudutab ründajate ja kaitsjate vahelist asümmeetriat, siis FAIMid vähendavad ründajate juurdepääsukulusid. Pahatahtlikud tegutsejad sõltuvad ründeoperatsioonide tehniliselt arenenumate ja töömahukamate osade elluviimisel tõenäoliselt üha enam FAIMidest, mis aitavad vähendada kulusid. Kaitsjaid seevastu pärsivad tegevusnõuded, sõltuvus ja regulatiivsed kohustused, mis piiravad FAIMide mõju ja ulatust lühikeses kuni keskpikas perspektiivis ning millest tulenevalt on lõppkokkuvõttes vaja pikemat kohanemisperioodi.

Kolmandaks on finantsasutustel erinevad ressursid ja vahendid FAIMidest tulenevate väljakutsete lahendamiseks. Need erinevused võivad tuleneda fikseeritud (mitte-skaleeritud) kuludest, piiratud ressurssidest ja piiratud juurdepääsust spetsialistidele. Kui asjaomaste väljakutsetega toimetulemise võimekus on asümmeetriline, võib ahela nõrgim lüli mõjutada kogu süsteemi stabiilsust.

Mõju

Oluline on tagada, et süsteemselt olulised makse- ja arveldussüsteemid ning finantsturutaristud oleksid jätkuvalt kaitstud FAIMide kasutamisest ja arendamisest tulenevate haavatavuste eest. Nii avaliku kui erasektori üksused peaksid oma küberturvalisuse raamistikud põhjalikult läbi vaatama ja neid ajakohastama, et selliseid haavatavusi arvesse võtta. Järelevalve eest vastutavad asutused peaksid võtma meetmeid, et tagada süsteemide piisav kaitse. Seal, kus see on vajalik liidu finantssüsteemi turvalisuse ja vastupidavuse suurendamiseks, tuleb edendada ametiasutuste ja eraõiguslike finantsasutuste vahelist koostööd.

Oma 2020. aasta süsteemse küberriski aruandes ([10]) nimetas ESRN süsteemse riski võimaliku allikana küberohtude kiirust, ulatust ja pahatahtlikku tegutsemist. Ametiasutused peaksid olema teadlikud, et FAIMid kujutavad endast uut levikuallikat, kuid ka võimendavad varem tuvastatud allikaid, ning integreerima asjaomase teabe oma poliitikameetmetesse. Võttes arvesse kõiki finantsstabiilsuse riske, mis tulenevad finantssektori avatusest küberriskile, on oluline tagada, et käesolevas hoiatuses välja toodud murekohad kajastuksid järelevalve- ja järelevaatamistegevuses ning poliitilistes seisukohtades, mille asjaomased asutused oma vastavate volituste piires vastu võtavad.

Asjaomased asutused peaksid oma pädevuse piires ning määrusega (EL) 2022/2554 kehtestatud raamistiku alusel olema teadlikud kolmest eespool nimetatud asümmeetria allikast, mida FAIMid finantssektoris on tekitanud. Asümmeetria vähendamiseks tuleks lisaks olemasolevatele testimisraamistikele kaaluda koostöökokkuleppeid ja valdkondlikku koordineerimist ([11]). Samuti peaksid finantsasutused tagama, et erasektori finantsasutuste juhatused on täielikult pühendunud FAIMi-põhiste küberriskide maandamisele, et kehtestatud on selged juhtimis- ja vastutusraamistikud ning et õigeaegne reageerimine koos vastavate majasiseste investeeringutega on asjakohaselt kavandatud.

Hoiatuses käsitletud võimalikud arengud – olgu see süsteemne mõju, geopoliitiline risk või ründajate ja kaitsjate vahelise tasakaalu muutumine – võivad mõjutada finantssüsteemi toimimist ja usaldust selle vastu. Järjepideva hindamise läbiviimiseks kaalub ESRN vajadust kajastada selliseid arenguid riskihindamistes, testimisraamistikes ja järelevalvealastes ootustes ning tulevaste stsenaariumide väljatöötamisel. Samuti jälgib ESRN FAIMide kasutamist ja arendamist ning nende mõju finantssektorile süsteemse riski seisukohast. Lisaks hindab ESRN iga kvartali riskihinnangus neid arenguid haldusnõukogu tasandil ja kaalub vajaduse korral muid meetmeid.

2. JAGU

Mõisted

Käesolevas hoiatuses kasutatakse mõisteid järgmises tähenduses:

1) „tehisintellekti pakkuja“ – määruse (EL) 2024/1689 artikli 3 punktis 3 määratletud pakkuja;

2) „eesliini tehisintellektimudelid (*Frontier AI Models*, FAIM)“ – täiustatud üldotstarbelised tehisintellektimudelid, mis on võimelised oluliselt mõjutama ründe- või kaitseotstarbelisi küberoperatsioone;

3) „küberrünne“ – küberrünne nõukogu määruse (EL) 2019/796 artiklis 1 määratletud tähenduses, sealhulgas juhul ([12]), kui see algab liidust;

4) „haavatavus“ – määruse (EL) 2022/2554 artikli 3 punktis 16 määratletud nõrkus;

5) „eksploit“ – vahend, tehnika või meetod, mida kasutatakse ühe või mitme haavatavuse ärakasutamiseks, et saada volitamata juurdepääs süsteemidele, neid muuta või häirida või muul viisil põhjustada IKT-riski või IKTga seotud intsidente;

6) „relvana kasutamine“ – eksploidi ettevalmistamine või kohandamine, et see võimaldaks haavatavusi süstemaatiliselt või skaleeritavalt ära kasutada;

7) „kriitilise tähtsusega või oluline funktsioon“ – kriitilise tähtsusega või oluline funktsioon määruse (EL) 2022/2554 artikli 3 punktis 22 määratletud tähenduses;

8) „üldotstarbeline tehisintellektimudel“ – määruse (EL) 2024/1689 artikli 3 punktis 63 määratletud tehisintellektimudel;

9) „süsteemse riskiga üldotstarbeline tehisintellektimudel“ – üldotstarbeline tehisintellektimudel, mis on liigitatud süsteemset riski tekitavaks vastavalt määruse (EL) 2024/1689 artikli 51 lõikele 1;

10) „IKTga seotud intsident“ – määruse (EL) 2022/2554 artikli 3 punktis 8 määratletud intsident;

([10]) Vt *Systemic cyber risk*, ESRN, veebruar 2020, avaldatud ESRNi veebilehelwww.esrb.europa.eu.

([11]) Nt ohuteabel põhinev eetiline ründetestimine (TIBER), ohuteabel põhinev läbistustestimine (TLPT), täiustatud ründetestimine (ART) ja küberkerksuse stressitestimine (CyRST).

([12]) Nõukogu määrus (EL) 2019/796, 17. mai 2019, piiravate meetmete kohta, millega takistada liitu või selle liikmesriike ähvardavaid küberrünnideid (ELT L 129 I, 17.5.2019, lk 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11) „IKT-risk“ – määruse (EL) 2022/2554 artikli 3 punktis 5 määratletud risk;

12) „tegevuskerksus“ – digitaalne tegevuskerksus määruse (EL) 2022/2554 artikli 3 punktis 1 määratletud tähenduses.

Frankfurt Maini ääres, 25. juuni 2026

ESRNi haldusnõukogu nimel
ESRNi sekretariaadi juhataja
Francesco MAZZAFERRO