Euroopan unionin
virallinen lehti

FI
C-sarja

C/2026/3795

16.7.2026

EUROOPAN JÄRJESTELMÄRISKIKOMITEAN VAROITUS,

annettu 25 päivänä kesäkuuta 2026,

etulinjan tekoälymalleista johtuvista systeemisistä kyberriskeistä

(EJRK/2026/3)

(C/2026/3795)

EUROOPAN JÄRJESTELMÄRISKIKOMITEAN HALLINTONEUVOSTO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon Euroopan talousalueesta tehdyn sopimuksen ([1]) ja erityisesti sen liitteen IX,

ottaa huomioon finanssijärjestelmän makrotason vakauden valvonnasta Euroopan unionissa ja Euroopan järjestelmäriskikomitean perustamisesta 24 päivänä marraskuuta 2010 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1092/2010 ([2]) ja erityisesti sen 3 artiklan 2 kohdan c alakohdan sekä 16 ja 18 artiklan,

ottaa huomioon Euroopan järjestelmäriskikomitean työjärjestyksen hyväksymisestä 20 päivänä tammikuuta 2011 annetun Euroopan järjestelmäriskikomitean päätöksen EJRK/2011/1 ([3]) ja erityisesti sen 18 ja 19 artiklan,

sekä katsoo seuraavaa:

(1) Johtavat tekoälyjärjestelmien tarjoajat ovat kehittäneet etulinjan tekoälymalleja (Frontier AI Models, FAIM), jotka ovat erittäin suorituskykyisiä kyberturvallisuuden alalla ja pystyvät tekemään täysin automatisoituja kyberhyökkäyksiä monimutkaisiin järjestelmiin, myös haavoittuvuuksien havaitsemisen sekä hyväksikäyttömenetelmien kehittämisen ja välineellistämisen kautta. Tämä kaikki muuttaa kyberuhkaympäristöä perusteellisesti.

(2) Etulinjan tekoälymallit ovat kyberhyökkäysten toteuttamisessa huomattavasti parempia kuin aiemmat tekoälymallit; lisäksi ne ovat kustannustehokkaampia, nopeampia ja tarkempia kuin aiemmat mallit ja tätä nykyä ne jo kilpailevat johtavien ihmisasiantuntijoiden kanssa.

(3) Etulinjan tekoälymallit pystyvät aiheuttamaan uhkia tieto- ja viestintäteknisiä ympäristöjä tukeville järjestelmille, joihin rahoitusmarkkinainfrastruktuuri perustuu, mikä lisää sellaisten kyberpoikkeamien todennäköisyyttä ja vakavuutta, joilla on järjestelmätason vaikutuksia.

(4) Etulinjan tekoälymallien on todettu pystyvän havaitsemaan haavoittuvuuksia ja luomaan uudenlaisia hyväksikäyttömenetelmiä, mikä altistaa yleisimmät käyttöjärjestelmät ja ohjelmistot, joita käytetään lähes kaikkien organisaatioiden tietojärjestelmäympäristöissä, kyberhyökkäysten riskille.

(5) Perinteisesti tällaisia haavoittuvuuksia on onnistuttu havaitsemaan vain harvoin, ja useimmiten niitä ovat löytäneet tietoturvatutkijat, joiden löydösten perusteella on voitu ryhtyä kohdennettuihin korjaustoimiin. Näissä tapauksissa ohjelmistoyhtiöille annetaan usein vakioitu määräaika – yleensä 90 päivää – haavoittuvuuden korjaamiseksi, ennen kuin siitä ilmoitetaan julkisesti. On todennäköistä, että havaittujen haavoittuvuuksien määrä kuitenkin kasvaa etulinjan tekoälymallien käytön myötä.

(6) Rahoitusjärjestelmän nykyiset korjauskäytännöt ovat pääasiassa reaktiivisia; ne perustuvat säännöllisiin päivityksiin ja tapauskohtaisiin toimiin, joilla havaitut haavoittuvuudet korjataan. Tämä lähestymistapa toimii sellaisessa uhkaympäristössä, jossa haavoittuvuuksien havaitseminen on hallittavissa sen takia, että siihen on aikaa. Haavoittuvuuksien määrän lisääntyessä nykyiset käytännöt voivat kuitenkin osoittautua operatiivisen häiriönsietokyvyn ylläpitämisen kannalta riittämättömiksi.

(7) Tämä määrän kasvu voi myös johtaa nykyisten korjausprosessien ylikuormittumiseen, koska niissä priorisoidaan riskiperusteisia korjaustoimenpiteitä ja edellytetään, että ohjelmakorjaukset testataan ennen järjestelmiin asentamista toiminnan vakauden varmistamiseksi. Jos lyhyessä ajassa havaitaan liian monta vaikutuksiltaan kriittistä haavoittuvuutta, jolloin tarvittavien kriittisten ohjelmakorjausten määrä kasvaa tuntuvasti, rahoituslaitokset voivat joutua päättämään, jättävätkö ne itsensä alttiiksi merkittäville kyberriskeille vai tinkivätkö ne korjauspäivitysten testausvaatimuksista, jolloin vaarana ovat toimintahäiriöt ja käyttökatkokset.

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

(8) Välineellistettyjä hyväksikäyttömenetelmiä luotiin aiemmin suurelta osin manuaalisesti ja ihmisasiantuntijoilta siihen kului päiviä tai viikkoja, mutta nykyään etulinjan tekoälymallit pystyvät tekemään sen jopa muutamassa minuutissa tai muutamassa tunnissa. Tämä tarkoittaa sitä, että ne suoja-aikapuskurit romahtavat, joita tarvitaan kriittisten ja tärkeiden toimintojen jatkuvuuden ylläpitämiseen korjaustoimien aikana.

(9) Kun tekoälyyn perustuvat kriittisiä haavoittuvuuksia hyödyntävät välineellistetyt hyväksikäyttömenetelmät lisääntyvät ja suoja-aikapuskurit vastaavasti pienenevät, yksittäisiin kriittisiin tai tärkeisiin toimintoihin ja laitoksiin kohdistuva riski suurenee jyrkästi. Jos tällaiset riskit toteutuvat samanaikaisesti kaikissa näissä toiminnoissa ja laitoksissa, systeeminen kyberriski voi jäädä pysyvästi suureksi, eikä sen pienentämiseksi ole tällä hetkellä tarpeeksi tehokkaita keinoja. Koska unionin rahoitussektorin toimijoiden, rahoitussektorin ja muiden sektoreiden sekä eri maiden väliset keskinäiset kytkökset ovat tiiviit, nykyinen tilanne aiheuttaa systeemisen riskin ja voi heikentää koko järjestelmää.

(10) Lisäksi etulinjan tekoälymalleja kehittävät tällä hetkellä vain muutamat tekoälyjärjestelmien tarjoajat, joista monet ovat jo ilmaisseet huolensa siitä, että tulevat etulinjan tekoälymallit voivat olla liian tehokkaita siihen, että ne voitaisiin asettaa rajoituksetta yleiseen käyttöön.

(11) Pahantahtoiset toimijat käyttävät tekoälyä jo nyt kyberhyökkäysten tehostamiseen. On todennäköistä, että tällaiset toimijat pääsevät jossain vaiheessa joko vuotojen, varkauksien tai riippumattoman kehitystyön kautta käsiksi sellaisiin tekoälymalleihin tai avoimesti saatavilla oleviin malleihin, joiden valmiudet ovat verrattavissa tällä hetkellä valvotuissa torjuntamekanismeissa käytettäviin valmiuksiin.

(12) Vaikka etulinjan tekoälymallit voivat yhtäältä lisätä hyökkäyskykyä ja kehittyneiden kyberhyökkäysten todennäköisyyttä tuntuvasti, toisaalta ne vahvistavat myös torjuntakykyä etenkin haavoittuvuuksien havaitsemisen, datan korrelaation ja yksittäisissä laitoksissa toteuttavien korjaustoimien osalta. Lyhyellä ja keskipitkällä aikavälillä hyökkäyskyvyn nopeus, laajuus ja tarkkuus todennäköisesti kuitenkin kasvavat edellä mainittuja hyötyjä enemmän.

(13) Etulinjan tekoälymallien nopean kehityksen vuoksi rahoitusvakauteen kohdistuviin havaittuihin riskeihin on puututtava viipymättä, jotta voidaan estää niiden toteutuminen tai ainakin lieventää niiden mahdollisia vaikutuksia. Jotta unionin rahoitusmarkkinoiden rahoitusvakaus voidaan taata, Euroopan järjestelmäriskikomitean (EJRK) kaikkien jäsenten on makro- ja mikrovakauspoliittisissa toimissaan otettava huomioon etulinjan tekoälymallien vaikutukset rahoituslaitosten toimintakykyyn ja häiriönsietokykyyn. Tämä ei kuitenkaan vaikuta keskuspankkien rahapolitiikkaa koskeviin tehtäviin unionissa. Pankkivalvojan roolissaan EKP on esimerkiksi pyytänyt merkittäviä laitoksia arvioimaan kehittymässä olevan uhkaympäristön vaikutukset viipymättä ja laatimaan 31. lokakuuta 2026 mennessä perusteellisen toimintasuunnitelman, jossa kuvataan konkreettisia toimenpiteitä, joilla tällaisia riskejä käsitellään, monien muiden viranomaisten tämänhetkisten aloitteiden tavoin ([4]).

(14) Tekoälyteknologian lisääntyessä on tärkeää varmistaa, että kaikki kriittinen infrastruktuuri ja erityisesti rahoituslaitokset ovat valmiita kohtaamaan etulinjan tekoälymalleihin perustuvat kyberhyökkäykset ja varautuvat niihin ajoissa ja asianmukaisesti. Yksittäisten laitosten torjuntatoimet eivät kuitenkaan riitä. Tehokas reagointi ja riskien lieventäminen edellyttävät koordinoituja vastatoimia, joihin osallistuvat kaikki asianomaiset osapuolet eli tekoälyjärjestelmien tarjoajat, ohjelmistoyhtiöt, tietoturvayhtiöt, avoimen lähdekoodin ylläpitäjät, rahoituslaitokset ja viranomaiset sekä kansallisella että unionin tasolla.

(15) Edellä mainittuja kysymyksiä käsiteltäessä on tärkeää palauttaa mieleen asiaankuuluvat unionin oikeudelliset ja toimintapoliittiset kehykset, erityisesti Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554 ([5]), Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689 ([6]), Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847 ([7]) ja Euroopan järjestelmäriskikomitean suositus (EJRK/2021/17) ([8]).

([4]) Merkittäville laitoksille osoitettu kirje on luettavissa EKP:n verkkosivustolla Pankkivalvonta-osiossa.

([5]) Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554, annettu 14 päivänä joulukuuta 2022, finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta (EUVL L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689, annettu 13 päivänä kesäkuuta 2024, tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta (tekoälysäädös) (EUVL L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847, annettu 23 päivänä lokakuuta 2024, digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös) (EUVL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Euroopan järjestelmäriskikomitean suositus, annettu 2 päivänä joulukuuta 2021, Euroopan laajuisesta systeemisten kyberpoikkeamien koordinointikehyksestä asiaan liittyviä viranomaisia varten (EJRK/2021/17) (EUVL C 134, 25.3.2022, s. 1).

(16) Asetuksessa (EU) 2022/2554 säädetään kattavasta kehyksestä, jonka avulla rahoituslaitokset voivat tunnistaa, hallita, seurata ja lieventää TVT-riskejä ja myös kyberhyökkäyksistä johtuvia riskejä. Kun otetaan huomioon rahoitussektorin tiiviit keskinäiset kytkökset ja sen riippuvuus tietojärjestelmistä ja kolmansista osapuolista eli palveluntarjoajista, yhteen tai useampaan rahoituslaitokseen tai niiden kriittisiin palveluntarjoajiin kohdistuvalla onnistuneella kyberhyökkäyksellä voisi olla merkittäviä järjestelmätason vaikutuksia. Valvontaviranomaisten on priorisoitava tämän osa-alueen valvontatoimia ja otettava huomioon sekä tällaisten kyberhyökkäysten mahdollinen vaikutus rahoitusjärjestelmän vakauteen, eheyteen ja luotettavuuteen että toimintaan liittyvät, taloudelliset ja kuluttajiin kohdistuvat vahingot, joita voi aiheutua.

(17) Asetuksessa (EU) 2024/1689 vahvistetaan yhdenmukaistetut säännöt, jotka koskevat tekoälyjärjestelmien ja yleiskäyttöisten tekoälymallien markkinoille saattamista, käyttöönottoa ja käyttöä unionissa, sekä tietyissä tilanteissa myös kolmansiin maihin sijoittautuneiden tekoälyjärjestelmien tarjoajien järjestelmiä ja malleja, kun tekoälyjärjestelmän tuotosta käytetään unionissa tai kun tekoälymalli on integroitu unionin markkinoille saatettuun järjestelmään. Kyseisessä asetuksessa säädetään myös erityisistä säännöistä ja tavallista tiukemmasta sääntelyjärjestelmästä, jotka koskevat systeemisiä riskejä aiheuttavia yleiskäyttöisiä tekoälymalleja.

(18) Asetuksella (EU) 2024/2847 otetaan käyttöön valmistajille pakolliset kyberturvallisuusvaatimukset, jotka koskevat unionin markkinoille saatettujen, digitaalisia elementtejä sisältävien laite- ja ohjelmistotuotteiden suunnittelua, kehitystä, tuotantoa, toimitusta ja ylläpitoa. Siinä edellytetään myös, että valmistajat käsittelevät haavoittuvuuksia tuotteidensa koko elinkaaren ajan. Kun asetusta aletaan soveltaa täysimääräisesti joulukuussa 2027, myös tällaisia tuotteita unionin markkinoille saattavien rahoituslaitosten on varmistettava, että kyseiset tuotteet täyttävät nämä vaatimukset.

(19) Suosituksessa EJRK/2021/17 annettiin suositus, että Euroopan valvontaviranomaiset yhteiskomitean välityksellä ja yhdessä Euroopan keskuspankin (EKP), EJRK:n ja asiaan liittyvien kansallisten viranomaisten kanssa alkavat kehittää unionin tason tehokkaita ja koordinoituja toimia sellaisia mahdollisia tilanteita varten, joissa rajat ylittävillä merkittävillä kyberpoikkeamilla tai niihin liittyvällä uhkalla voi olla systeeminen vaikutus unionin finanssialaan. Suosituksen pohjalta perustettiin yleiseurooppalainen systeemisten kyberpoikkeamien koordinointikehys (EU-SCICF), josta on tullut finanssialaa valvoville viranomaisille tärkeä ja operatiivinen tiedonvaihto- ja koordinointimekanismi.

(20) Edellä esitetyn perusteella EJRK antaa yleisluonteisen varoituksen, jossa käsitellään merkittäviä rahoitusvakauteen liittyviä riskejä, joita etulinjan tekoälymallien kehitys kasvattaa. Varoituksessa otetaan huomioon analyysi, joka on esitetty kesäkuussa 2026 julkaistussa EJRK:n muistiossa Addressing Frontier AI Models with cyber capabilities from a financial stability perspective ([9]),

ON ANTANUT TÄMÄN VAROITUKSEN:

1 JAKSO

Varoitus

Uudenlainen riskiympäristö

Etulinjan tekoälymallien, joilla on kybervalmiuksia, nopea kehitys muuttaa unionin rahoitusjärjestelmän riskiympäristöä merkittävästi. Tämänhetkinen näyttö osoittaa, että etulinjan tekoälymallit pystyvät havaitsemaan haavoittuvuuksia, luomaan toimivia hyväksikäyttömenetelmiä ja toteuttamaan itsenäisesti täysimittaisia kyberhyökkäyksiä, joiden nopeus, laajuus ja tarkkuus ylittävät aiempien tekoälymallien kyvyt selvästi. Tämä tarkoittaa paradigman muutosta kyberturvallisuuden alalla ja käännekohtaa tekoälymallien kyvykkyydessä.

EJRK katsoo, että tämä kehityskulku on rahoitusjärjestelmään kohdistuvien systeemisten riskien lähde, jolla on potentiaalia aiheuttaa merkittävää haittaa kyberturvallisuudelle, sillä haavoittuvuudet havaitaan entistä nopeammin, reagointiin ja tehokkaisiin torjuntatoimiin käytettävissä oleva aika on lyhentynyt ja kyberhyökkäykset ovat aiempaa laajempia ja kehittyneempiä, minkä lisäksi rahoitusjärjestelmään on syntynyt uusia kytköksiä ja keskittymäriskejä. EJRK tiedostaa, että etulinjan tekoälymallit tulevat vahvistamaan rahoituslaitosten torjuntavalmiuksia, mutta on todennäköistä, että nämä valmiudet konkretisoituvat asteittain muutaman vuoden kuluessa; näin ollen rahoituslaitosten on siirtymäaikana pystyttävä toimimaan kohonneen riskin ja suuren epävarmuuden olosuhteissa, joissa myös teknologinen toimintaympäristö muuttuu nopeasti. Kun otetaan huomioon, että rahoitusjärjestelmä on pitkälle digitalisoitu ja kytköksissä moniin muihin järjestelmiin, tällaiset kyberturvallisuuteen kohdistuvat haitalliset vaikutukset voivat levitä nopeasti ja vaikuttaa kriittisiin ja tärkeisiin toimintoihin kaikkien rahoituslaitosten laajuudelta, mikä johtaa lopulta järjestelmähäiriöihin ja heikentää luottamusta rahoitusjärjestelmään.

([9]) Luettavissa EJRK:n verkkosivuilla osoitteessa www.esrb.europa.eu.

Kehittymässä olevat etulinjan tekoälymallit suurentavat sisäistä tieto- ja viestintätekniikkaan liittyvää luontaista riskiä, ja sen vuoksi rahoitusalan operatiivinen häiriönsietokyky heikkenee erityisesti neljällä seuraavalla osa-alueella: a) aika, mukaan luettuna kyky korjata monimutkaisia järjestelmiä nopeasti aiheuttamatta toimintahäiriöitä ja ottaen huomioon, että haavoittuvuuden havaitsemisen ja hyväksikäyttömenetelmien välineellistämisen väliset suoja-aikapuskurit lyhenevät; b) torjuntatoimista vastaavien työntekijöiden valmiudet sekä heidän kykynsä toteuttaa automaattista ja manuaalista tietoturvatestausta etulinjan tekoälymallien avustamina ja suojata järjestelmiä etulinjan tekoälymallien vilpillisestä käytöstä johtuvilta uhkilta, havaita niitä ja reagoida niihin; c) keskittymät, myös riippuvuus vain muutamasta tekoälyjärjestelmien tarjoajasta, jotka puolestaan ovat riippuvaisia pilvipalvelujen tarjoajista, avoimeen lähdekoodiin perustuvista komponenteista ja muista laajalti käytössä olevista ohjelmistoista, ja d) viranomaisten valmiudet sekä niiden odotukset, stressitestaus ja varautumistoimet, joita kaikkia on tarkistettava etulinjan tekoälymallien kehityksen myötä, jotta toimintahäiriöt eivät muutu laajemman epävakauden lähteeksi.

Myös ajan tasalla pysytteleminen tekoälymallien käytöstä rahoituslaitoksissa on haasteellista, aivan kuten perusteellisen ymmärryksen ylläpitäminen siitä, missä ja miten tekoälyä käytetään, kun otetaan huomioon, että sitä käytetään sisäisten tekoälyagenttien lisäksi myös asiakasrajapinnoissa, liiketoimintaprosesseissa sekä integroinnissa kolmansien osapuolten järjestelmiin.

Systeeminen arviointi

Havaittu kehitys voi muuttaa sekä kyberriskin laajuutta että sen rakennetta perin pohjin, jolloin rahoitusvakauteen kohdistuvat suorat ja epäsuorat riskit kasvavat. Etulinjan tekoälymallien valmiudet voivat aiheuttaa nykyisille häiriönsieto-mekanismeille valtavaa painetta etenkin, jos häiriöt ovat laajoja ja ilmaantuvat samanaikaisesti. Häiriöt voivat myös levitä nopeasti muihin rahoituslaitoksiin ja rahoitusmarkkinoille, jos kriittisiä palveluja tarjoavat kolmannet osapuolet, jaetut teknologiset ekosysteemit tai laajalti käytössä olevat avoimen lähdekoodin komponentit joutuvat häiriön kohteiksi, sillä tällöin sellaisten häiriöiden riski kasvaa, joilla on systeemisiä vaikutuksia.

Etulinjan tekoälymallit muuttavat rahoitussektorin kolmea epätasapainon lähdettä, joista ensimmäinen on eri maiden välinen, toinen torjuntatoimista vastaavien ja hyökkääjien välinen ja kolmas rahoituslaitosten välinen, kun otetaan huomioon, että toiset laitokset ovat paremmin varautuneita ja varustautuneita häiriöihin kuin toiset.

Ensinnäkin se, että johtavien tekoälyjärjestelmien tarjoajien maantieteellinen keskittymä sijaitsee tällä hetkellä unionin ulkopuolella, altistaa unionin strategiselle riippuvuudelle ja geopoliittiselle riskille. Jotta voidaan vähentää eri maiden välistä tiedollista ja teknologista epätasapainoa, on toteutettava toimenpiteitä, joilla mahdollistetaan se, että unioni ja sen jäsenvaltiot voivat hyödyntää uusimpia etulinjan tekoälymalleja asianmukaisesti ja oikeasuhteisesti. Tällaisten toimenpiteiden on oltava oikea-aikaisia, johdonmukaisia ja tehokkaita sekä toimintapolitiikan että toteutuksen osalta, ja niissä on otettava asianmukaisesti huomioon unionin rahoitussektorin eri osa-alueet Euroopan valvontaviranomaisten asiantuntemusta hyödyntäen. Näin voidaan vähentää sekä unionin ja kolmansien maiden välistä että eri jäsenvaltioihin sijoittautuneiden rahoituslaitosten välistä epätasapainoa ja siten mahdollistaa tasapuoliset toimintaedellytykset unionissa ja sen ulkopuolella ja minimoida systeeminen riski. Sellaiset järjestelyt, joilla etulinjan tekoälymallien käyttö on mahdollista vain tietyntyyppisille laitoksille tai vain tietyissä maissa, lisäisivät sisämarkkinoiden pirstoutumista rahoitussektorin osalta ja vähentäisivät niiden likviditeettiä ja syvyyttä.

Toiseksi hyökkääjien ja torjuntatoimista vastaavien tahojen välisen epätasapainon osalta on otettava huomioon, että etulinjan tekoälymallit madaltavat hyökkääjien kynnystä toteuttaa hyökkäys. Hyökkäysoperaatioiden teknisesti kehittyneempien ja työvoimavaltaisten osuuksien toteuttamisessa uhkatoimijat nimittäin todennäköisesti tukeutuvat entistä enemmän etulinjan tekoälymalleihin, sillä se pienentää kustannuksia. Sitä vastoin torjuntatoimista vastaavien tahojen mahdollisuuksia rajoittavat toiminnalliset vaatimukset, riippuvuudet ja sääntelyyn perustuvat velvollisuudet, joiden vuoksi se, miten tehokkaasti ja laajasti ne voivat hyödyntää etulinjan tekoälymalleja lyhyellä ja keskipitkällä aikavälillä, on rajallista, ja sen takia muuttuvaan ympäristöön mukautuminen vie enemmän aikaa.

Kolmanneksi siinä, millaiset resurssit ja valmiudet rahoituslaitoksilla on reagoida etulinjan tekoälymalleista johtuviin haasteisiin, on eroja. Tällaisia eroja voivat aiheuttaa kiinteät kustannukset, koska ne pysyvät aina samansuuruisina eivätkä skaalaudu, resurssirajoitteet sekä se, että käytettävissä on liian vähän asiantuntijoita. Kun valmiudet reagoida haasteisiin ovat epätasapainossa, ketjun heikoin lenkki saattaa vaikuttaa järjestelmän vakauteen.

Päätelmät

On tärkeää varmistaa, että systeemisesti merkittävät maksu- ja selvitysjärjestelmät sekä rahoitusmarkkinainfrastruktuurit on suojattu etulinjan tekoälymallien käytöstä ja kehittämisestä aiheutuvilta haavoittuvuuksilta. Julkisten ja yksityisten toimijoiden on arvioitava ja päivitettävä kyberturvallisuuskehyksensä perusteellisesti, jotta kyseiset haavoittuvuudet voidaan ottaa huomioon. Valvontaviranomaisten on toteutettava toimenpiteitä sen varmistamiseksi, että järjestelmät on suojattu asianmukaisesti. Viranomaisten ja yksityisten rahoituslaitosten on tarvittaessa tehtävä yhteistyötä unionin rahoitusjärjestelmän turvallisuuden ja häiriönsietokyvyn vahvistamiseksi.

Systeemisiä kyberriskejä koskevassa vuoden 2020 raportissaan ([10]) EJRK määritti kyberuhkien nopeuden, laajuuden ja pahantahtoiset aikomukset mahdollisiksi lähteiksi systeemisen riskin leviämiselle. Viranomaisten on oltava tietoisia siitä, että etulinjan tekoälymallit ovat uusi häiriöiden leviämisen lähde, minkä lisäksi ne myös vahvistavat olemassa olevia aiemmin tunnistettuja lähteitä, ja siksi viranomaisten on sisällytettävä tämä näkökulma toimintapolitiikkaansa. Kun otetaan huomioon kaikki rahoitusvakauteen liittyvät riskit, jotka johtuvat rahoitussektorin altistumisesta kyberriskeille toiminnassaan, on tärkeää varmistaa, että tässä varoituksessa määritetyt huolenaiheet huomioidaan asiaankuuluvien viranomaisten valvontatyössä ja toimintapolitiikassa, jota ne toteuttavat tehtäviensä puitteissa.

Asiaankuuluvien viranomaisten, jotka toimivat niille annettujen toimivaltuuksien ja etenkin asetuksella (EU) 2022/2554 perustetun kehyksen puitteissa, on oltava tietoisia kolmesta edellä mainitusta epätasapainon lähteestä, jotka johtuvat etulinjan tekoälymallien käyttöönotosta rahoitussektorilla. Epätasapainon vähentämiseksi on aihetta harkita yhteistyöjärjestelyjä ja alakohtaista koordinointia nykyisten testauskehysten ([11]) ohella. Lisäksi rahoitusvalvontaviranomaisten on varmistettava, että yksityisten rahoituslaitosten hallintoelimet ovat täysin sitoutuneet lieventämään etulinjan tekoälymalleista johtuvia kyberriskejä, että käytössä on selkeät hallinto- ja vastuuvelvollisuusrakenteet ja että oikea-aikaiset vastatoimet ja niihin liittyvät sisäiset investoinnit suunnitellaan asianmukaisesti.

Monet tässä varoituksessa käsitellyt kehityskulut – järjestelmätason vaikutus, geopoliittinen riski tai muuttunut tasapaino hyökkääjien ja torjuntatoimista vastaavien tahojen välillä – voivat vaikuttaa sekä rahoitusjärjestelmän toimintaan että sen luotettavuuteen. Jotta näitä seikkoja voidaan arvioida jatkuvasti, EJRK selvittää, miten nämä kehityskulut pitää ottaa huomioon riskinarvioinneissa, testauskehyksissä ja valvontaan liittyvissä odotuksissa sekä tulevaisuuden skenaarioiden laatimisessa. EJRK seuraa myös etulinjan tekoälymallien käyttöä ja kehitystä sekä niiden vaikutusta rahoitussektoriin systeemisen riskin näkökulmasta. Lisäksi EJRK arvioi kehitystä uudelleen jokaisessa neljännesvuosittaisessa riskinarvioinnissa hallintoneuvoston tasolla ja harkitsee tarvittaessa muita toimia.

2 JAKSO

Määritelmät

Tässä varoituksessa sovelletaan seuraavia määritelmiä:

1) ’tekoälyjärjestelmän tarjoajalla’ tarkoitetaan asetuksen (EU) 2024/1689 3 artiklan 3 kohdassa määriteltyä tarjoajaa;

2) ’etulinjan tekoälymalleilla’ tarkoitetaan kehittyneitä yleiskäyttöisiä tekoälymalleja, jotka pystyvät vaikuttamaan kyberhyökkäyksiin tai niiden torjuntaan merkittävästi;

3) ’kyberhyökkäyksellä’ tarkoitetaan neuvoston asetuksen (EU) 2019/796 ([12]) 1 artiklassa määriteltyä kyberhyökkäystä, myös sellaista, joka on peräisin unionin rajojen sisäpuolelta;

4) ’haavoittuvuudella’ tarkoitetaan asetuksen (EU) 2022/2554 3 artiklan 16 kohdassa määriteltyä haavoittuvuutta;

5) ’hyväksikäyttömenetelmällä’ tarkoitetaan työkalua, tekniikkaa tai menetelmää, jolla hyödynnetään yhtä tai useampaa haavoittuvuutta luvattoman pääsyn saamiseksi järjestelmiin, jotta niitä voidaan muuttaa tai niiden toimintaa häiritä taikka aiheuttaa muutoin TVT-riskejä tai TVT:hen liittyviä poikkeamia;

6) ’välineellistämisellä’ tarkoitetaan sellaisten hyväksikäyttömenetelmien kehittämistä tai mukauttamista, joilla haavoittuvuuksia voidaan hyödyntää järjestelmällisesti tai skaalautuvasti;

7) ’kriittisellä tai tärkeällä toiminnolla’ tarkoitetaan asetuksen (EU) 2022/2554 3 artiklan 22 kohdassa määriteltyä kriittistä tai tärkeää toimintoa;

8) ’yleiskäyttöisellä tekoälymallilla’ tarkoitetaan asetuksen (EU) 2024/1689 3 artiklan 63 kohdassa määriteltyä tekoälymallia;

9) ’yleiskäyttöisellä tekoälymallilla, johon liittyy systeeminen riski’ tarkoitetaan yleiskäyttöistä tekoälymallia, joka on luokiteltu asetuksen (EU) 2024/1689 51 artiklan 1 kohdan mukaisesti tekoälymalliksi, johon liittyy systeeminen riski;

10) ’TVT:hen liittyvällä poikkeamalla’ tarkoitetaan asetuksen (EU) 2022/2554 3 artiklan 8 kohdassa määriteltyä poikkeamaa;

([10]) Ks. systeemisiä kyberriskejä koskeva julkaisu ”Systemic cyber risk”, EJRK, helmikuu 2020, luettavissa EJRK:n verkkosivustolla www.esrb.europa.eu.

([11]) Esimerkiksi uhkatiedustelutietoihin perustuva hyökkäystestaus (TIBER), uhkaperusteinen tunkeutumistestaus (TLPT), kehittynyt hyökkäystestaus (ART) ja kyberhäiriöiden sietokykyä koskeva stressitesti (CyRST).

([12]) Neuvoston asetus (EU) 2019/796, annettu 17 päivänä toukokuuta 2019, unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä (EUVL L 129 I, 17.5.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11) ’TVT-riskillä’ tarkoitetaan asetuksen (EU) 2022/2554 3 artiklan 5 kohdassa määriteltyä riskiä;

12) ’digitaalisella häiriönsietokyvyllä’ tarkoitetaan asetuksen (EU) 2022/2554 3 artiklan 1 kohdassa määriteltyä digitaalista häiriönsietokykyä.

Tehty Frankfurt am Mainissa 25 päivänä kesäkuuta 2026.

EJRK:n sihteeristön päällikkö,

EJRK:n hallintoneuvoston puolesta

Francesco MAZZAFERRO