Europeiska unionens
officiella tidning

SV
C-serien

C/2026/3795

16.7.2026

EUROPEISKA SYSTEMRISKNÄMNDENS VARNING

av den 25 juni 2026

om systemiska cyberrisker som utgår från de mest avancerade modellerna för artificiell intelligens

(ESRB/2026/3)

(C/2026/3795)

EUROPEISKA SYSTEMRISKNÄMNDENS STYRELSE HAR ANTAGIT DENNA VARNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av avtalet om Europeiska ekonomiska samarbetsområdet ([1]), särskilt bilaga IX,

med beaktande av Europaparlamentets och rådets förordning (EU) nr 1092/2010 av den 24 november 2010 om makrotillsyn av det finansiella systemet på EU-nivå och om inrättande av en europeisk systemrisknämnd ([2]), särskilt artikel 3.2 c samt artiklarna 16 och 18,

med beaktande av Europeiska systemrisknämndens beslut ESRB/2011/1 av den 20 januari 2011 om arbetsordningen för Europeiska systemrisknämnden ([3]), särskilt artiklarna 18 och 19, och

av följande skäl:

(1) Ledande leverantörer av artificiell intelligens (AI) har utvecklat avancerade AI-modeller (s.k. Frontier AI-modeller, FAIM), som har hög kapacitet på området cybersäkerhet och kan utföra helt automatiserade cyberattacker mot komplexa system, bl.a. genom att upptäcka sårbarheter och utveckla och missbruka sårbarhetsattacker, vilket har grundläggande konsekvenser för cyberhotbilden.

(2) FAIM är betydligt bättre än tidigare AI-modeller när det gäller att hitta sätt att utföra cyberattacker på, och överträffar tidigare modeller i fråga om kostnad, hastighet och precision, och kan nu utmana ledande mänskliga experter.

(3) FAIM har potentialen att hota de system som ligger till grund för den informations- och kommunikationsteknik (IKT) som den finansiella infrastrukturen är beroende av, vilket ökar sannolikheten för ännu mer allvarligliga cyberincidenter med systemeffekter.

(4) FAIM har visat sin förmåga att upptäcka sårbarheter och skapa sårbarhetsattacker, vilket exponerar stora operativsystem och programvara som används i nästan alla organisationers IKT-miljöer för risken för cyberattacker.

(5) Historiskt sett har upptäckten av sådana sårbarheter varit sällsynta och ofta gjorts av forskare inom området datasäkerhet, vilket har möjliggjort riktade insatser för att säkra system. I dessa fall får programvarutillverkare ofta en standardiserad tidsram – vanligtvis 90 dagar – för att åtgärda sårbarheten innan den offentliggörs. FAIM kommer dock sannolikt att öka antalet sårbarheter som upptäckts.

(6) Nuvarande uppdateringsmetoder i det finansiella systemet är främst reaktiva och bygger på regelbundna uppdateringar och ad hoc-åtgärder för att hantera sårbarheter som upptäckts. Denna strategi fungerar i en hotmiljö där man har tillräckligt med tid för att upptäckten av sårbarheter ska kunna hanteras. Med när antalet sårbarheter som upptäcks ökar, kan nuvarande praxis bli otillräcklig för att upprätthålla den operativa motståndskraften.

(7) Denna volymökning medför att de nuvarande uppdateringsprocesserna kan överbelastas, eftersom de prioriterar avhjälpande åtgärder utifrån en riskbedömning och kräver att man testar uppdateringar innan dessa genomförs för att säkerställa operativ stabilitet. Om alltför många kritiska sårbarheter upptäcks inom kort tid så att antalet nödvändiga uppdateringar ökar avsevärt, kan finansinstitut behöva välja mellan att antingen acceptera betydande cyberrisker eller sänka kraven på testning av uppdateringar av programvara vilket då kan medföra en ökad risk för operativa incidenter och driftsavbrott.

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

(8) Utformningen av sårbarhetsattacker i syfte att missbruka dessa skapades tidigare till stor del manuellt och tog dagar eller veckor för mänskliga experter, medan det nu kan göras av FAIM på några minuter eller timmar. Detta medför att defensiva tidsbuffertar krymper, som behövs för att upprätthålla kontinuiteten i kritiska och viktiga funktioner medan underhållsarbete utförs.

(9) När kritiska sårbarheter som sprids i syfte att missbruka dessa tas fram av AI, och de defensiva tidsbuffertarna krymper, ökar risken för enskilda kritiska eller viktiga funktioner och institutioner kraftigt. Om sådana risker uppstår samtidigt hos dessa funktioner och institut kan detta medföra en permanent ökning av systematiska cyberrisker för vilka det för närvarande inte finns något effektivt ramverk med motåtgärder. På grund av den starka sammanlänkningen av unionens finanssektor, samt även mellan den sektorn och andra sektorer och jurisdiktioner, utgör denna situation en systemrisk som kan skapa instabilitet i systemet.

(10) Dessutom utvecklas FAIM för närvarande bara av ett litet antal AI-leverantörer, varav flera har uttryckt oro över att kommande FAIM-modeller kan vara för kraftfulla för obegränsad allmän tillgång.

(11) AI används redan av kriminella aktörer för att öka cyberattackernas effekt. Det är sannolikt att sådana aktörer så småningom, antingen genom läckor, stöld, oberoende utveckling eller öppen åtkomst, kommer att få tillgång till AI-modeller med en kapacitet som är jämförbar med den som för närvarande används i kontrollerade defensiva miljöer.

(12) Även om FAIM avsevärt kan öka den offensiva kapaciteten och sannolikheten för sofistikerade cyberattacker, kommer de också att stärka den defensiva kapaciteten, särskilt när det gäller upptäckten av sårbarheter, korrelering av data och korrigerande åtgärder från enskilda institutioners sida. På kort till medellång sikt kommer dock den offensiva kapacitetens ökade hastighet, omfattning och kvalitet sannolikt att uppväga fördelarna.

(13) Den snabba utvecklingen av FAIM gör det nödvändigt att utan dröjsmål ta itu med de identifierade riskerna för den finansiella stabiliteten för att förhindra att de materialiseras eller åtminstone mildra deras potentiella effekter. För att säkerställa finansiell stabilitet på unionens finansmarknader bör alla medlemmar i Europeiska systemrisknämnden (ESRB) beakta vilka konsekvenser FAIM kan få för finansinstitutens operativa kapacitet och motståndskraft inom ramen för deras makrotillsynsåtgärder och mikrotillsynspolitiska åtgärder. Detta påverkar inte de penningpolitiska mandaten för centralbankerna i unionen. Som ett exempel, och bland andra myndigheters pågående initiativ, har ECB, i sin roll som banktillsynsmyndighet, uppmanat betydande institut att utan dröjsmål bedöma effekterna av den föränderliga hotbilden och att senast den 31 oktober 2026 ta fram en omfattande handlingsplan med konkreta åtgärder för att komma till rätta med dessa risker ([4]).

(14) I takt med att AI-tekniken blir alltmer spridd är det viktigt att se till att all kritisk infrastruktur, särskilt finansinstituten, är redo att hantera cyberattacker som styrs av FAIM och att i god tid vidta lämpliga förberedelser. Sådana defensiva insatser från enskilda enheter kan dock vara otillräckliga. Effektiva insatser och riskreducering kräver en samordnad respons som omfattar alla berörda parter, inbegripet AI-leverantörer, programvaruleverantörer, säkerhetsföretag, underhållare av öppen källkod, finansinstitut samt myndigheter på både nationell nivå och unionsnivå.

(15) När ovanstående frågor diskuteras är det viktigt att beakta unionens relevanta rättsliga och politiska ramar, särskilt Europaparlamentets och rådets förordning (EU) 2022/2554 ([5]), Europaparlamentets och rådets förordning (EU) 2024/1689 ([6]), Europaparlamentets och rådets förordning (EU) 2024/2847 ([7]) samt Europeiska systemrisknämndens rekommendation (ESRB/2021/17) ([8]).

([4]) Brevet till de betydande instituten finns på ECB:s webbplats www.bankingsupervision.europa.eu.

([5]) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) (EUT L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Europeiska systemrisknämndens rekommendation av den 2 december 2021 om ett europeisk ramverk för relevanta myndigheters samordning av åtgärder mot systemiska cyberincidenter (ESRB/2021/17) (EUT C 134, 25.3.2022, s. 1).

(16) Förordning (EU) 2022/2554 tillhandahåller en övergripande ram för finansiella institut för att identifiera, hantera, övervaka och minska IKT-risker, inbegripet risker som härrör från cyberattacker. Med tanke på finanssektorns sammanlänkning och dess beroende av IKT-system och tredjepartsleverantörer av tjänster kan en framgångsrik cyberattack som påverkar ett eller flera finansinstitut eller deras kritiska tjänsteleverantörer få betydande systemeffekter. De finansiella tillsynsmyndigheterna bör på lämpligt sätt prioritera tillsynsverksamhet på detta område, med beaktande av de potentiella effekterna som sådana cyberattacker kan få för det finansiella systemets stabilitet, integritet och tillförlitlighet samt den operativa och finansiella skadan samt skadan för konsumenterna som kan bli följden.

(17) Genom förordning (EU) 2024/1689 fastställs harmoniserade regler för utsläppande på marknaden, ibruktagande och användning av AI-system och AI-modeller för allmänna ändamål i unionen, inbegripet, under vissa omständigheter, system och modeller som tillhandahålls av AI-leverantörer som är etablerade i tredjeländer om de data som produceras av AI-systemet används i unionen, eller om en AI-modell integreras i ett system som släpps ut på unionsmarknaden. I denna förordning föreskrivs också särskilda regler, inbegripet ett striktare regelverk, för modeller som klassificeras som AI-modeller för allmänna ändamål med systemrisk.

(18) Genom förordning (EU) 2024/2847 införs obligatoriska cybersäkerhetskrav för tillverkare som omfattar planering, utformning, utveckling och underhåll av maskinvaru- och programvaruprodukter med digitala element som släpps ut på unionsmarknaden. Det uppställer också krav på att tillverkarna hanterar sårbarheter under sina produkters livscykel. När förordningen börjar tillämpas fullt ut i december 2027 måste finansiella enheter som släpper ut sådana produkter på unionsmarknaden också säkerställa att sådana produkter uppfyller dessa krav.

(19) I rekommendation ESRB/2021/17 rekommenderades att de europeiska tillsynsmyndigheterna, gemensamt genom den gemensamma kommittén och tillsammans med Europeiska centralbanken (ECB), ESRB och relevanta nationella myndigheter, bör förbereda en effektiv samordnad reaktion på unionsnivå i händelse av en gränsöverskridande större cyberincident eller därmed sammanhängande hot som kan ha systemiska konsekvenser för unionens finanssektor. Detta resulterade i inrättande av en europeisk ram för samordning av systemiska cyberincidenter (EU-SCICF), som utgör en värdefull och operativ plattform för informationsutbyte och samordning mellan finansmyndigheter.

(20) Mot denna bakgrund antar ESRB härmed en varning av allmän karaktär som är inriktad på de betydande risker för den finansiella stabiliteten som kan bli följden av utvecklingen av FAIM. Varningen beaktar det analytiska arbetet i ESRB:s not *Addressing Frontier AI Models with cyber capabilities from a financial stability perspective* ([9]), som offentliggjordes i juni 2026.

HÄRIGENOM KONSTATERAS FÖLJANDE.

AVSNITT 1

Varning

Ny hotbild

Den snabba utvecklingen av *avancerade AI-modeller (FAIM)* med cyberkapacitet medför väsentliga förändringar av hotbilden för unionens finansiella system. Aktuella studier tyder på att FAIM kan upptäcka sårbarheter, utforma sårbarhetsattacker och självständigt utföra fullskaliga cyberattacker med en hastighet, omfattning och precision som vida överstiger tidigare AI-modeller. Detta utgör ett paradigmskifte på området cybersäkerhet och skapar en ny realitet när det gäller AI-kapacitet.

ESRB anser att denna utveckling är en källa till systemrisk för det finansiella systemet, med potential att skapa betydande negativa effekter på cybersäkerheten genom att påskynda upptäckten av sårbarheter, reducera den tid som finns tillgänglig för insatser och effektivt försvar, öka cyberattackernas omfattning och sofistikering samt införa nya beroenden och koncentrationsrisker i det finansiella systemet. Samtidigt som ESRB är medveten om den förstärkta defensiva kapacitet som FAIM kommer att erbjuda finansinstituten, kommer denna kapacitet sannolikt att förverkligas gradvis under de kommande åren, vilket medför att finansinstituten under en övergångsperiod måste acceptera en förhöjd risk, hög osäkerhet och snabbt föränderligt teknik. Med tanke på det finansiella systemets starkt digitaliserade och sammanlänkade karaktär skulle sådana negativa effekter på cybersäkerheten snabbt kunna sprida sig och påverka kritiska och viktiga funktioner i finansinstitut, vilket i slutändan kan leda till systemstörningar och förlorat förtroende för det finansiella systemet.

([9]) Finns på ESRB:s webbplats www.esrb.europa.eu.

Ett framväxande FAIM ökar den inneboende IKT-risken, vilket medför försvagad operativ motståndskraft i hela finanssektorn, särskilt inom fyra områden: a) tid, inbegripet förmågan att snabbt uppdatera komplexa system utan att orsaka driftsavbrott, med beaktande av att defensiva tidsbuffertar kollapsar mellan upptäckt av sårbarhet och en sårbarhetsattack, b) försvararnas förmåga, inbegripet deras förmåga att genomföra automatiska och manuella säkerhetstester som stöds av FAIM, samt deras förmåga att skydda, upptäcka och reagera på hot som härrör från fientlig FAIM-användning, c) koncentration, inbegripet beroende av ett begränsat antal AI-leverantörer, som i sin tur är beroende av molnleverantörer, komponenter med öppen källkod och annan programvara som används i stor utsträckning, samt d) myndigheternas förmåga, inbegripet deras kalibrering av förväntningar, stresstester och beredskapsåtgärder i enlighet med utvecklingen av FAIM, så att operativa brister inte blir en källa till mer omfattande instabilitet.

Att fastställa och upprätthålla synligheten för införandet av AI hos alla finansinstitut – inbegripet att fullt ut förstå var och hur AI används – är dessutom en utmaning, eftersom AI används i kundgränssnitt, interna agenter, affärsprocesser och integrering med tredje parter.

Systemisk bedömning

Den utveckling som identifierats kan väsentligt ändra både cyberriskens omfattning och struktur, vilket ökar både de direkta och de indirekta riskerna för den finansiella stabiliteten. FAIM:s kapacitet kan sätta betydande press på befintliga resiliensramar, särskilt om incidenter är utbredda och inträffar samtidigt. Incidenter kan också spridas snabbt mellan finansinstitut och finansmarknader om kritiska tredjepartsleverantörer, gemensamma tekniska ekosystem eller allmänt använda komponenter med öppen källkod påverkas, vilket ökar risken för relaterade störningar med systemeffekter.

FAIM ändrar tre källor till asymmetri inom finanssektorn: den första mellan jurisdiktioner, den andra mellan försvarare och angripare och den tredje mellan finansinstitut med bättre resurser och sådana med mindre resurser.

För det första innebär den nuvarande geografiska koncentrationen av ledande AI-leverantörer utanför unionen att unionen utsätts för strategiskt beroende och geopolitiska risker. För att minska kunskaps- och teknikasymmetrin mellan jurisdiktioner är det nödvändigt att anta åtgärder för att underlätta adekvat och proportionell tillgång för unionen och dess medlemsstater till nyutvecklade FAIM. Sådana åtgärder bör vidtas i rätt tid, vara enhetliga och effektiva, både när det gäller policy och genomförande, och bör på lämpligt sätt beakta unionens olika finanssektorer och dra nytta av sakkunskapen hos respektive europeiska tillsynsmyndigheter. Detta kommer inte bara att minska asymmetrin mellan unionens och tredjeländers jurisdiktioner utan även mellan finansinstitut som är etablerade i olika medlemsstater, bevara konkurrens på lika villkor inom och utanför unionen samt minimera systemrisken. Arrangemang som underlättar tillgången till FAIM endast för vissa kategorier av institut eller i utvalda jurisdiktioner skulle bidra till en fragmentering av den inre marknaden för finansiering, och försämra dess likviditet och djup.

För det andra, vad gäller asymmetrin mellan angripare och försvarare, minskar FAIM kostnaden för angripare. Fientliga aktörer kommer sannolikt i allt högre grad att förlita sig på FAIM för att genomföra de mer tekniskt avancerade och arbetsintensiva delarna av offensiva insatser, vilket minskar kostnaderna. Försvararna begränsas däremot av operativa krav, beroenden och lagstadgade skyldigheter, vilket begränsar den effekt och omfattning i vilken de kan dra nytta av FAIM på kort till medellång sikt, vilket i slutändan kräver längre perioder för anpassning.

För det tredje finns det skillnader i de resurser och den utrustning för att hantera de utmaningar som FAIM innebär som olika finansinstitut har. Dessa skillnader kan uppstå på grund av fasta snarare än rörliga kostnader, resursbegränsningar och begränsad tillgång till specialister. Om det finns asymmetri i förmågan att hantera sådana utmaningar kan den svagaste länken i kedjan påverka systemets stabilitet.

Konsekvenser

Det är viktigt att se till att systemviktiga betalnings- och avvecklingssystem samt finansmarknadsinfrastrukturer förblir skyddad mot sårbarheter som uppstår till följd av användning och utveckling av FAIM. Offentliga och privata operatörer bör grundligt se över och uppdatera sina cybersäkerhetsarrangemang för att beakta sådana sårbarheter. Myndigheter med ansvar för tillsyn eller översyn bör vidta åtgärder för att se till att systemen är tillräckligt skyddade. Samarbete mellan myndigheter och privata finansinstitut bör eftersträvas närhelst det är nödvändigt för att öka säkerheten och motståndskraften i unionens finansiella system.

I sin rapport från 2020 om systemiska cyberrisker ([10]) identifierade ESRB cyberhotens hastighet, omfattning och illasinnade intentioner som möjliga källor till spridning av systemrisker. Myndigheterna bör vara medvetna om att FAIM utgör en ny spridningskälla som förstärker de tidigare identifierade källorna, och bör integrera denna insikt i sina policyåtgärder. Med tanke på alla risker för den finansiella stabiliteten som härrör från operativ exponering mot cyberrisker i finanssektorn, är det viktigt att säkerställa att de frågeställningar som identifieras i denna varning återspeglas i det tillsyns- och övervakningsarbete och de policydokument som de berörda myndigheterna antar, inom ramen för sina respektive mandat.

De berörda myndigheterna bör, inom ramen för sina respektive befogenheter och särskilt inom den ram som fastställs genom förordning (EU) 2022/2554, vara medvetna om tre tidigare nämnda källorna till asymmetri som FAIM medför inom finanssektorn. För att reducera dessa asymmetrier bör samarbetsarrangemang och sektoriell samordning övervägas tillsammans med befintliga ramar för tester ([11]). Finansmyndigheterna bör också säkerställa att privata finansinstituts styrelser är fast beslutna att reducera FAIM-drivna cyberrisker, att det finns tydliga ramar för styrning och ansvars och att snabba åtgärder planeras på lämpligt sätt, tillsammans med motsvarande interna investeringar.

Flera möjliga utvecklingar som nämns i denna varning – oavsett om det rör sig om systemeffekter, geopolitiska risker eller den förändrade balansen mellan angripare och försvarare – kan påverka det finansiella systemets funktion och förtroendet för det. För att kontinuerligt bedöma dessa kommer ESRB att överväga behovet av att spegla denna utveckling i riskbedömningar, ramar för tester, och tillsynsförväntningar, samt i en framtida scenarioutveckling. ESRB kommer också att övervaka användningen och utvecklingen av FAIM och deras inverkan på finanssektorn ur ett systemriskperspektiv. ESRB kommer dessutom att ompröva utvecklingen av varje kvartalsvis riskbedömning på styrelsenivå och vid behov överväga andra åtgärder.

AVSNITT 2

Definitioner

I denna varning gäller följande definitioner:

1. *AI-leverantör*: en leverantör enligt definitionen i artikel 3.3 i förordning (EU) 2024/1689.

2. *avancerade AI-modeller (FAIM)*: de mest avancerade AI-modellerna för allmänna ändamål som väsentligt kan påverka offensiva eller defensiva cyberoperationer.

3. *cyberattack*: en cyberattack enligt definitionen i artikel 1 i rådets förordning (EU) 2019/796 ([12]), även om den har sitt ursprung i unionen.

4. *sårbarhet*: en sårbarhet enligt definitionen i artikel 3.16 i förordning (EU) 2022/2554.

5. *sårbarhetsattack*: ett verktyg, en teknik eller en metod som används för att utnyttja en eller flera sårbarheter för att få obehörig åtkomst till system, ändra dem eller störa dem eller på annat sätt ge upphov till IKT-risker eller IKT-relaterade incidenter.

6. *missbruk:* förberedelse eller anpassning av sårbarhetsattacker som möjliggör ett systematiskt eller skalbart utnyttjande av sårbarheter.

7. *kritisk eller viktig funktion*: en kritisk eller viktig funktion enligt definitionen i artikel 3.22 i förordning (EU) 2022/2554.

8. *AI-modell för allmänna ändamål*: en AI-modell enligt definitionen i artikel 3.63 i förordning (EU) 2024/1689.

9. *AI-modeller för allmänna ändamål med systemrisk*: en AI-modell för allmänna ändamål som klassificerats som AI-modell för allmänna ändamål med systemrisk i enlighet med artikel 51.1 i förordning (EU) 2024/1689.

10. *IKT-relaterad incident*: en incident enligt definitionen i artikel 3.8 i förordning (EU) 2022/2554.

([10]) Se *Systemic cyber risk*, ESRB, februari 2020, finns på ESRB:s webbplats www.esrb.europa.eu.

([11]) T.ex. threat intelligence-based ethical red teaming (TIBER), threat-led penetration testing (TLPT), advanced red teaming (ART) and cyber resilience stress testing (CyRST).

([12]) Rådets förordning (EU) 2019/796 av den 17 maj 2019 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater (EUT L 129 I, 17.5.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11. *ICT-risk*: en risk enligt definitionen i artikel 3.5 i förordning (EU) 2022/2554.

12. *operativ motståndskraft*: en digital operativ motståndskraft enligt definitionen i artikel 3.1 i förordning (EU) 2022/2554.

Utfärdad i Frankfurt am Main den 25 juni 2026.

På ESRB-styrelsens vägnar

Francesco MAZZAFERRO

Chef för ESRB:s sekretariat