Publicatieblad
van de Europese Unie

NL
C-serie

C/2026/3795

16.7.2026

WAARSCHUWING VAN HET EUROPEES COMITÉ VOOR SYSTEEMRISICO'S

van 25 juni 2026

betreffende systemische cyberrisico's die voortvloeien uit grensverleggende artificiële intelligentiemodellen

(ESRB/2026/3)

(C/2026/3795)

DE ALGEMENE RAAD VAN HET EUROPEES COMITÉ VOOR SYSTEEMRISICO'S,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien de Overeenkomst betreffende de Europese Economische Ruimte ([1]), en met name bijlage IX,

Gezien Verordening (EU) nr. 1092/2010 van het Europees Parlement en de Raad van 24 november 2010 betreffende macroprudentieel toezicht van de Europese Unie op het financiële stelsel en tot oprichting van een Europees Comité voor systeemrisico's ([2]), en met name artikel 3, lid 2, punt c), en de artikelen 16 en 18,

Gezien Besluit ESRB/2011/1 van het Europees Comité voor systeemrisico's van 20 januari 2011 houdende goedkeuring van het reglement van orde van het Europees Comité voor systeemrisico's ([3]), en met name de artikelen 18 en 19,

Overwegende hetgeen volgt:

(1) Toonaangevende aanbieders van artificiële intelligentie (AI) hebben grensverleggende AI-modellen (*Frontier AI Models* — FAIM's) ontwikkeld, die zeer geschikt zijn op het gebied van cyberbeveiliging en volledig geautomatiseerde cyberaanvallen kunnen uitvoeren op complexe systemen, onder meer door het opsporen van kwetsbaarheden en de ontwikkeling en inzet van exploits als wapen, waardoor het cyberdreigingslandschap fundamenteel wordt veranderd.

(2) FAIM's zijn aanzienlijk beter dan eerdere AI-modellen in het vinden van manieren om cyberaanvallen uit te voeren wat betreft kosten, snelheid en nauwkeurigheid, waardoor zij nu kunnen concurreren met vooraanstaande menselijke deskundigen.

(3) FAIM's kunnen een bedreiging vormen voor de systemen die ten grondslag liggen aan de omgevingen voor informatie- en communicatietechnologie (ICT) waarvan de financiële infrastructuur afhankelijk is, waardoor de waarschijnlijkheid en ernst van cyberincidenten met systemische gevolgen toenemen.

(4) FAIM's hebben aangetoond dat zij in staat zijn kwetsbaarheden te ontdekken en nieuwe exploits te vervaardigen, waardoor grote besturingssystemen en software die in bijna alle ICT-omgevingen van organisaties worden gebruikt, worden blootgesteld aan het risico van cyberaanvallen.

(5) In het verleden was de ontdekking van dergelijke kwetsbaarheden zeldzaam en deze werd vaak gedaan door veiligheidsonderzoekers, waardoor gericht herstel mogelijk was. In die gevallen krijgen softwareaanbieders vaak een gestandaardiseerde termijn — gewoonlijk 90 dagen — om de kwetsbaarheid te verhelpen voordat deze openbaar wordt gemaakt. Het is echter waarschijnlijk dat FAIM's het aantal vastgestelde kwetsbaarheden zullen doen toenemen.

(6) De huidige patchingpraktijken in het financiële stelsel zijn overwegend reactief en berusten op periodieke updates en ad-hocreacties op bekendgemaakte kwetsbaarheden. Deze aanpak werkt in een dreigingsomgeving waarin de beschikbare tijd het toelaat om het aantal ontdekte kwetsbaarheden op een beheersbaar niveau te houden. Door de toename van het aantal kwetsbaarheden kunnen de huidige praktijken echter ontoereikend worden om de operationele weerbaarheid te behouden.

(7) Deze toename van het aantal stelt de huidige patchingprocessen ook bloot aan overbelasting, aangezien zij prioriteit geven aan herstelmaatregelen op basis van risico's en vereisen dat softwarepatches vóór de implementatie worden getest om de operationele stabiliteit te waarborgen. Indien binnen een kort tijdsbestek te veel kwetsbaarheden met kritieke gevolgen worden ontdekt, waardoor het vereiste aantal kritieke softwarepatches aanzienlijk wordt verhoogd, worden financiële instellingen mogelijk genoodzaakt te beslissen of zij zichzelf aan aanzienlijke cyberrisico's blootstellen of de vereisten voor patchtests verminderen waarbij zij operationele incidenten en storingen riskeren.

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

(8) Het vervaardigen van als wapen gebruikte exploits gebeurde voorheen grotendeels handmatig en nam dagen of weken van menselijke deskundigen in beslag, terwijl dit nu binnen enkele minuten of uren door FAIM's kan worden gedaan. Dit leidt tot het wegvallen van defensieve tijdbuffers, die nodig zijn om de continuïteit van kritieke en belangrijke functies tijdens de remediëring te handhaven.

(9) Met de toename van als wapen ingezette exploits die verband houden met kritieke kwetsbaarheden die worden aangedreven door AI en de overeenkomstige vermindering van defensieve tijdbuffers neemt het risico voor individuele kritieke of belangrijke functies en instellingen sterk toe. Als dergelijke risico's zich gelijktijdig voordoen in die functies en instellingen, kan dit leiden tot een permanente toename van het systemische cyberrisico waarvoor momenteel geen volledig doeltreffend mitigatiekader beschikbaar is. Door de sterke verwevenheid binnen de financiële sector van de Unie, alsook tussen die sector en andere sectoren en rechtsgebieden, vormt deze situatie een systematisch risico en kan zij systemische kwetsbaarheden creëren.

(10) Bovendien worden FAIM's momenteel ontwikkeld door slechts een klein aantal AI-aanbieders, van wie er verscheidene hun bezorgdheid hebben geuit over het feit dat toekomstige FAIM's mogelijk te krachtig zijn voor onbeperkte publieke toegang.

(11) AI wordt al door kwaadwillende actoren gebruikt om cyberaanvallen te versterken. Het is waarschijnlijk dat dergelijke actoren uiteindelijk AI-modellen zullen verkrijgen, hetzij door lekken, diefstal, onafhankelijke ontwikkeling of open toegang, met capaciteiten die vergelijkbaar zijn met die welke momenteel in gecontroleerde defensieve omgevingen worden ingezet.

(12) Hoewel FAIM's de offensieve capaciteiten en de waarschijnlijkheid van geavanceerde cyberaanvallen aanzienlijk kunnen vergroten, zullen zij ook de defensieve capaciteiten versterken, met name wat betreft het opsporen van kwetsbaarheden, gegevenscorrelatie en herstelmaatregelen door individuele instellingen. Op de korte tot middellange termijn zullen echter de toename van de snelheid, de omvang en de nauwkeurigheid van de offensieve capaciteiten waarschijnlijk opwegen tegen de voordelen.

(13) De snelle ontwikkeling van FAIM's maakt het noodzakelijk de vastgestelde risico's voor de financiële stabiliteit onverwijld aan te pakken om te voorkomen dat deze zich voordoen of ten minste om de potentiële gevolgen ervan te beperken. Om de financiële stabiliteit op de financiële markten van de Unie te waarborgen, moeten alle leden van het Europees Comité voor systeemrisico's (ESRB) in het kader van hun macroprudentiële en microprudentiële beleidsmaatregelen rekening houden met de gevolgen van FAIM's voor de operationele capaciteit en weerbaarheid van financiële instellingen. Dit doet geen afbreuk aan de monetaire beleidsmandaten van de centrale banken in de Unie. Zo heeft bijvoorbeeld de ECB, in het kader van de huidige initiatieven van diverse autoriteiten en in haar hoedanigheid van bankentoezichthouder, de belangrijke instellingen verzocht om onverwijld de gevolgen van het veranderende dreigingslandschap te beoordelen en uiterlijk op 31 oktober 2026 een uitgebreid actieplan op te stellen met concrete maatregelen om dergelijke risico's aan te pakken ([4]).

(14) Naarmate AI-technologie zich uitbreidt, is het belangrijk ervoor te zorgen dat alle kritieke infrastructuur en met name financiële instellingen voorbereid zijn op cyberaanvallen die door FAIM's worden aangedreven, en tijdig passende voorbereidingen treffen. Dergelijke defensieve inspanningen van afzonderlijke entiteiten zouden echter ontoereikend zijn. Een doeltreffende respons en risicobeperking vereisen een gecoördineerd antwoord waarbij alle partijen die dit aangaat worden betrokken, met inbegrip van AI-aanbieders, softwareaanbieders, beveiligingsbedrijven, opensource-beheerders, financiële instellingen en autoriteiten op zowel nationaal niveau als het niveau van de Unie.

(15) Bij het aanpakken van de bovenstaande kwesties is het belangrijk om rekening te houden met de relevante rechts- en beleidskaders van de Unie, met name Verordening (EU) 2022/2554 van het Europees Parlement en de Raad ([5]), Verordening (EU) 2024/1689 van het Europees Parlement en de Raad ([6]), Verordening (EU) nr. 2024/2847 van het Europees Parlement en de Raad ([7]) en de aanbeveling van het Europees Comité voor systeemrisico's (ESRB/2021/17) ([8]).

([4]) De brief aan de belangrijke instellingen is beschikbaar op de ECB-website voor bankentoezicht onder: www.bankingsupervision.europa.eu.

([5]) Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (PB L 333 van 27.12.2022, blz. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144 en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie) (PB L, 2024/1689 van 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid) (PB L, 2024/2847 van 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Aanbeveling van het Europees Comité voor systeemrisico's van 2 december 2021 betreffende een pan-Europees coördinatiekader voor systemische cyberincidenten voor relevante autoriteiten (ESRB/2021/17) (PB C 134 van 25.3.2022, blz. 1).

(16) Verordening (EU) 2022/2554 biedt financiële instellingen een alomvattend kader voor het identificeren, beheren, monitoren en beperken van ICT-risico's, met inbegrip van risico's die voortvloeien uit cyberaanvallen. Gezien de verwevenheid van de financiële sector en zijn afhankelijkheid van ICT-systemen en derde dienstverleners, kan een succesvolle cyberaanval die een of meer financiële instellingen of hun aanbieders van kritieke diensten treft, aanzienlijke systemische gevolgen hebben. De financiële toezichthoudende autoriteiten moeten gepaste prioriteit geven aan toezichtactiviteiten op dit gebied, rekening houdend met de mogelijke gevolgen van dergelijke cyberaanvallen voor de stabiliteit, integriteit en betrouwbaarheid van het financiële stelsel, alsook met de operationele, financiële en consumentenschade die daaruit kan voortvloeien.

(17) Verordening (EU) 2024/1689 stelt geharmoniseerde regels vast voor het in de handel brengen, in gebruik stellen en gebruik van AI-systemen en AI-modellen voor algemene doeleinden in de Unie, met inbegrip van, in bepaalde omstandigheden, systemen en modellen die worden geleverd door in derde landen gevestigde AI-aanbieders wanneer de door het AI-systeem geproduceerde output in de Unie wordt gebruikt of een AI-model wordt geïntegreerd in een systeem dat in de Unie in de handel wordt gebracht. Deze verordening voorziet ook in specifieke regels, waaronder een strenger regelgevingskader, voor modellen die zijn geclassificeerd als AI-modellen voor algemene doeleinden met een systeemrisico.

(18) Bij Verordening (EU) 2024/2847 worden verplichte cyberbeveiligingseisen voor fabrikanten ingevoerd die betrekking hebben op de planning, het ontwerp, de ontwikkeling en het onderhoud van hardware- en softwareproducten met digitale elementen die op de markt in de Unie worden gebracht. Ook moeten fabrikanten kwetsbaarheden aanpakken tijdens de levenscyclus van hun producten. Zodra zij in december 2027 volledig van toepassing zijn, zullen financiële instellingen die dergelijke producten in de Unie in de handel brengen, er ook voor moeten zorgen dat die producten aan deze eisen voldoen.

(19) In Aanbeveling ESRB/2021/17 werd aanbevolen dat de Europese toezichthoudende autoriteiten (ETA's), gezamenlijk via het Gemengd Comité en samen met de Europese Centrale Bank (ECB), het ESRB en de betrokken nationale autoriteiten, een doeltreffende gecoördineerde respons op Unieniveau ontwikkelen in geval van een ernstig grensoverschrijdend cyberincident of een daarmee verband houdende dreiging die systemische gevolgen kan hebben voor de financiële sector van de Unie. Dit heeft geleid tot de oprichting van het pan-Europese coördinatiekader voor systemische cyberincidenten (pan-European systemic cyber incident coordination framework — EU-SCICF), dat een waardevol en operationeel platform biedt voor informatie-uitwisseling en coördinatie tussen financiële autoriteiten.

(20) Tegen deze achtergrond stelt het ESRB hierbij een algemene waarschuwing vast om de aanzienlijke risico's voor de financiële stabiliteit aan te pakken die door de ontwikkeling van FAIM's worden versterkt. In de waarschuwing wordt rekening gehouden met de analytische werkzaamheden in de in juni 2026 gepubliceerde ESRB-nota "Addressing Frontier AI Models with cyber capabilities from a financial stability perspective" ([9]),

HEEFT DE VOLGENDE WAARSCHUWING VASTGESTELD:

AFDELING 1

Waarschuwing

Nieuw risicolandschap

De snelle ontwikkeling van grensverleggende AI-modellen (*Frontier AI Models* — FAIM) met cybercapaciteit brengt materiële veranderingen met zich mee in het risicolandschap voor het financiële stelsel van de Unie. Uit de huidige gegevens blijkt dat FAIM's in staat zijn kwetsbaarheden te ontdekken, werkende exploits te genereren en op autonome wijze grootschalige cyberaanvallen uit te voeren met een snelheid, schaal en nauwkeurigheid die die van eerdere AI-modellen in grote mate overtreffen. Dit vormt een paradigmaverschuiving op het gebied van cyberbeveiliging en een keerpunt voor wat betreft de AI-capaciteit.

Het ESRB beschouwt deze ontwikkelingen als een bron van systeemrisico's voor het financiële stelsel, die aanzienlijke negatieve gevolgen kunnen hebben voor de cyberbeveiliging door de versnelde ontdekking van kwetsbaarheden, de verkorting van de tijd die beschikbaar is voor respons en doeltreffende verdediging, de toegenomen schaal en complexiteit van cyberaanvallen en de invoering van nieuwe afhankelijkheden en concentratierisico's binnen het financiële stelsel. Hoewel het ESRB erkent dat FAIM's financiële instellingen versterkte defensievermogens zullen bieden, zullen deze vermogens de komende jaren waarschijnlijk geleidelijk tot stand komen, waardoor financiële instellingen in een overgangsperiode moeten opereren die wordt gekenmerkt door een hoog risico, grote onzekerheid en een snel evoluerend technologisch landschap. Gezien de sterk gedigitaliseerde en onderling verweven aard van het financiële stelsel zouden dergelijke negatieve gevolgen voor de cyberbeveiliging zich snel kunnen verspreiden, met gevolgen voor kritieke en belangrijke functies in alle financiële instellingen, wat uiteindelijk zou leiden tot systemische verstoring en verlies van vertrouwen in het financiële stelsel.

([9]) Beschikbaar op de ESRB-website onder: www.esrb.europa.eu.

De opkomende FAIM's verhogen het inherente ICT-risico, wat leidt tot een verzwakte operationele weerbaarheid in de gehele financiële sector, met name op vier gebieden: a) tijd, met inbegrip van het vermogen om op snelle wijze gecompliceerde systemen te herstellen zonder operationele storing te veroorzaken, rekening houdend met het wegvallen van defensieve tijdbuffers tussen ontdekking van kwetsbaarheden en het inzetten als wapen van exploits; b) het vermogen van verdedigingsexperts, met inbegrip van hun vermogen om geautomatiseerde en handmatige veiligheidstesten uit te voeren die worden ondersteund met FAIM, als ook hun vermogen om te beschermen tegen dreigingen afkomstig van het vijandig gebruik van FAIM, deze op te sporen en erop te reageren, c) concentratie, met inbegrip van afhankelijkheden van een beperkt aantal AI-aanbieders, die op hun beurt afhangen van cloudproviders, open-sourcecomponenten en andere veelgebruikte software; en d) de capaciteit van de autoriteiten, met inbegrip van het afstemmen van verwachtingen, stresstests en voorbereidingsmaatregelen met de ontwikkeling van FAIM's, zodat operationele storingen geen bron worden van een bredere instabiliteit.

Bovendien is het vaststellen en in stand houden van de zichtbaarheid van de inzet van AI binnen elke financiële instelling — met inbegrip van een volledig inzicht in waar en hoe AI wordt ingezet — een uitdaging, rekening houdend met het feit dat AI wordt gebruikt in cliëntinterfaces, interne agenten, bedrijfsprocessen en integratie met derden.

Systeembeoordeling

De vastgestelde ontwikkelingen kunnen zowel de omvang als de structuur van het cyberrisico wezenlijk veranderen, waardoor zowel de directe als de indirecte risico's voor de financiële stabiliteit toenemen. De FAIM-capaciteiten kunnen bestaande weerbaarheidskaders onder aanzienlijke druk zetten, met name wanneer incidenten wijdverbreid zijn en zich gelijktijdig voordoen. Incidenten kunnen zich ook snel verspreiden over financiële instellingen en markten als kritieke derde aanbieders, gedeelde technologische ecosystemen of op grote schaal gebruikte open-sourcecomponenten worden getroffen, waardoor het risico op daarmee samenhangende verstoringen met systemische gevolgen toeneemt.

FAIM's veranderen drie bronnen van asymmetrie in de financiële sector: de eerste tussen rechtsgebieden, de tweede tussen verdedigers en aanvallers, en de derde tussen beter toegeruste en minder goed uitgeruste financiële instellingen.

Ten eerste wordt de Unie door de huidige geografische concentratie van toonaangevende AI-aanbieders buiten de Unie blootgesteld aan strategische afhankelijkheid en geopolitieke risico's. Om de kennis- en technologische asymmetrie tussen rechtsgebieden te beperken, moeten maatregelen worden vastgesteld om adequate en evenredige toegang voor de Unie en haar lidstaten tot nieuw ontwikkelde FAIM's te vergemakkelijken. Dergelijke maatregelen moeten tijdig, coherent en efficiënt zijn, zowel wat het beleid als de uitvoering betreft, en moeten op gepaste wijze rekening houden met de verschillende financiële sectoren van de Unie, waarbij gebruik wordt gemaakt van de deskundigheid van de overeenkomstige ETA's. Dit zal niet alleen de asymmetrie tussen de rechtsgebieden van de Unie en die van derde landen verminderen, maar ook tussen financiële instellingen die in verschillende lidstaten zijn gevestigd, waardoor een gelijk speelveld binnen en buiten de Unie in stand wordt gehouden en het systeemrisico tot een minimum wordt beperkt. Regelingen die de toegang tot FAIM's alleen voor bepaalde categorieën instellingen of in geselecteerde rechtsgebieden vergemakkelijken, zouden bijdragen aan de versnippering van de eengemaakte markt voor financiering, waardoor de liquiditeit en diepte ervan zouden afnemen.

Ten tweede, wat de asymmetrie tussen aanvallers en verdedigers betreft, verlagen FAIM's de toegangsprijs voor aanvallers. Dreigingsactoren zullen waarschijnlijk steeds meer een beroep doen op FAIM's om de technisch meer geavanceerde en arbeidsintensieve onderdelen van offensieve operaties uit te voeren, waardoor de kosten dalen. Verdedigers worden daarentegen beperkt door operationele vereisten, afhankelijkheden en wettelijke verplichtingen, waardoor het effect en de omvang waarin ze van de FAIM's kunnen profiteren op de korte tot middellange termijn worden beperkt, waardoor uiteindelijk langere perioden nodig zijn om zich aan te passen.

Ten derde zijn er verschillen in de wijze waarop financiële instellingen worden toegerust en uitgerust om het hoofd te bieden aan de uitdagingen die FAIM's met zich meebrengen. Deze verschillen kunnen het gevolg zijn van vaste in plaats van geschaalde kosten, beperkte middelen en beperkte toegang tot specialisten. Wanneer er sprake is van asymmetrie in het vermogen om dergelijke uitdagingen het hoofd te bieden, kan de zwakste schakel van de keten van invloed zijn op de stabiliteit van het systeem.

Implicaties

Het is van essentieel belang ervoor te zorgen dat systeemrelevante betalings- en afwikkelingssystemen en financiële marktinfrastructuren beschermd blijven tegen kwetsbaarheden die voortvloeien uit het gebruik en de ontwikkeling van FAIM's Publieke en particuliere exploitanten moeten hun cyberbeveiligingskaders grondig evalueren en actualiseren om rekening te houden met dergelijke kwetsbaarheden. De met toezicht of oversight belaste autoriteiten moeten maatregelen nemen om ervoor te zorgen dat de systemen adequaat worden beschermd. Samenwerking tussen autoriteiten en particuliere financiële instellingen moet worden nagestreefd wanneer dat nodig is om de veiligheid en weerbaarheid van het financiële stelsel van de Unie te vergroten.

In het verslag van 2020 over systemische cyberrisico's ([10]) heeft het ESRB snelheid, schaal en kwaadaardige intentie van cyberdreigingen aangemerkt als mogelijke bronnen van verspreiding van systeemrisico's. De autoriteiten moeten zich ervan bewust zijn dat hoewel FAIM's een nieuwe bron van verspreiding vormen, zij ook de eerder geïdentificeerde bronnen versterken, en dientengevolge dit inzicht in hun beleidsmaatregelen moeten integreren. Gezien alle risico's voor de financiële stabiliteit die voortvloeien uit operationele blootstelling aan cyberrisico's in de financiële sector, is het belangrijk ervoor te zorgen dat de in deze waarschuwing vastgestelde punten van zorg tot uiting komen in de toezicht- en begeleidingswerkzaamheden en beleidsstandpunten van de betrokken autoriteiten, binnen het kader van hun respectieve mandaten.

De betrokken autoriteiten moeten, binnen hun respectieve bevoegdheden en met name binnen het bij Verordening (EU) 2022/2554 vastgestelde kader, op de hoogte zijn van drie eerdergenoemde bronnen van asymmetrie die door FAIM's in de financiële sector zijn ingevoerd. Om deze asymmetrieën te verminderen, moeten naast de bestaande testkaders ook samenwerkingsregelingen en sectorale coördinatie worden overwogen ([11]). Financiële autoriteiten moeten er ook voor zorgen dat de raden van bestuur van particuliere financiële instellingen zich ten volle inzetten om FAIM-gedreven cyberrisico's te beperken, ervoor zorgen dat er duidelijke governance- en verantwoordingskaders zijn en dat tijdige reacties adequaat worden gepland, samen met overeenkomstige interne investeringen.

Verschillende mogelijke ontwikkelingen die in deze waarschuwing aan bod komen — of het nu gaat om de systemische impact, het geopolitieke risico of het gewijzigde evenwicht tussen aanvallers en verdedigers — kunnen gevolgen hebben voor de werking van het financiële stelsel en het vertrouwen daarin. Om deze voortdurend te beoordelen, zal het ESRB nagaan of dergelijke ontwikkelingen moeten worden weerspiegeld in risicobeoordelingen, testkaders en toezichtverwachtingen, alsook in de ontwikkeling van toekomstige scenario's. Het ESRB zal ook toezicht houden op het gebruik en de ontwikkeling van FAIM's en de gevolgen ervan voor de financiële sector vanuit het oogpunt van systeemrisico's. Bovendien zal het ESRB de ontwikkelingen in elke driemaandelijkse risicobeoordeling op het niveau van de algemene raad opnieuw beoordelen en zo nodig andere maatregelen overwegen.

AFDELING 2

Definities

Voor de toepassing van deze waarschuwing gelden de volgende definities:

1. "AI-aanbieder": een aanbieder als gedefinieerd in artikel 3, punt 3, van Verordening (EU) 2024/1689;

2. "Grensverleggende AI-modellen (*Frontier AI Models* — FAIM's)": geavanceerde AI-modellen voor algemene doeleinden die een wezenlijke invloed kunnen hebben op offensieve of defensieve cyberoperaties;

3. "cyberaanval": een cyberaanval als gedefinieerd in artikel 1 van Verordening (EU) 2019/796 van de Raad ([12]), ook wanneer deze van binnen de Unie afkomstig is;

4. "kwetsbaarheid": een kwetsbaarheid als gedefinieerd in artikel 3, punt 16), van Verordening (EU) 2022/2554;

5. "exploit": een instrument, techniek of methode die wordt toegepast om van een of meer kwetsbaarheden gebruik te maken om ongeoorloofde toegang tot systemen te verkrijgen, deze te wijzigen of te verstoren, of anderszins aanleiding te geven tot ICT-risico of ICT-gerelateerde incidenten;

6. "inzet als wapen": het voorbereiden of aanpassen van exploits die de systematische of schaalbare exploitatie van kwetsbaarheden mogelijk maken;

7. "kritieke of belangrijke functie": een kritieke of belangrijke functie als gedefinieerd in artikel 3, punt 22), van Verordening (EU) 2022/2554;

8. "AI-model voor algemene doeleinden": een AI-model zoals gedefinieerd in artikel 3, punt 63, van Verordening (EU) 2024/1689;

9. "AI-model voor algemene doeleinden met een systeemrisico": een AI-model voor algemene doeleinden dat is geclassificeerd als een AI-model dat een systeemrisico inhoudt overeenkomstig artikel 51, lid 1, van Verordening (EU) 2024/1689;

10. "ICT-gerelateerd incident": een incident zoals gedefinieerd in artikel 3, punt 8, van Verordening (EU) 2022/2554;

([10]) Zie Systemic cyber risk, ESRB, februari 2020, beschikbaar op de ESRB website onder: www.esrb.europa.eu.

([11]) Bv. op dreigingsintelligentie gebaseerde ethische red-teaming (TIBER), dreigingsgestuurde penetratietests (TLPT), geavanceerde red-teaming (ART) en cyberweerbaarheidsstresstests (CyRST).

([12]) Verordening (EU) 2019/796 van de Raad van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen (PB L 129 I van 17.5.2019, blz. 1, ELI:http://data.europa.eu/eli/reg/2019/796/oj).

11. “ICT-risico”: een risico als gedefinieerd in artikel 3, punt 5), van Verordening (EU) 2022/2554;

12. ““operationele weerbaarheid”: digitale operationele weerbaarheid als gedefinieerd in artikel 3, punt 1), van Verordening (EU) 2022/2554;

Gedaan te Frankfurt am Main, 25 juni 2026.

Hoofd van het ESRB-secretariaat,
namens de algemene raad van het ESRB,
Francesco MAZZAFERRO