C/2026/3795

16.7.2026

WARNUNG DES EUROPÄISCHEN AUSSCHUSSES FÜR SYSTEMRISIKEN
vom 25. Juni 2026
zu von hochmodernen Modellen künstlicher Intelligenz ausgehenden systemischen Cyberrisiken
(ESRB/2026/3)

(C/2026/3795)

DER VERWALTUNGSRAT DES EUROPÄISCHEN AUSSCHUSSES FÜR SYSTEMRISIKEN —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum ([1]), insbesondere auf Anhang IX,

gestützt auf die Verordnung (EU) Nr. 1092/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 über die Finanzaufsicht der Europäischen Union auf Makroebene und zur Errichtung eines Europäischen Ausschusses für Systemrisiken ([2]), insbesondere auf Artikel 3 Absatz 2 Buchstabe c sowie die Artikel 16 und 18,

gestützt auf den Beschluss ESRB/2011/1 des Europäischen Ausschusses für Systemrisiken vom 20. Januar 2011 zur Verabschiedung der Geschäftsordnung des Europäischen Ausschusses für Systemrisiken ([3]), insbesondere auf die Artikel 18 und 19,

in Erwägung nachstehender Gründe:

(1) Führende Anbieter im Bereich künstliche Intelligenz (KI) haben hochmoderne KI-Modelle („Frontier-KI-Modelle“ oder „Frontier-Modelle“ genannt) entwickelt, die auf dem Gebiet der Cybersicherheit überaus leistungsfähig und in der Lage sind, vollständig automatisierte Cyberangriffe auf komplexe Systeme durchzuführen — unter anderem durch die Entdeckung von Schwachstellen und die Entwicklung von Exploits und deren Einsatz als Waffe (weaponisation) –, wodurch sich die Cyberbedrohungslandschaft grundlegend verändert

(2) Frontier-Modelle sind bei der Suche nach Möglichkeiten zur Durchführung von Cyberangriffen deutlich besser als frühere KI-Modelle. Sie sind diesen in Bezug auf Kosten, Geschwindigkeit und Genauigkeit überlegen und können nunmehr mit führenden menschlichen Experten mithalten

(3) Frontier-Modelle sind in der Lage, die den Informations- und Kommunikationstechnologie-(IKT)-Umgebungen zugrundeliegenden Systeme, auf denen sich die Finanzinfrastruktur stützt, zu bedrohen, wodurch Wahrscheinlichkeit und Schwere von Cybervorfällen mit systemischen Auswirkungen zunehmen

(4) Frontier-Modelle haben gezeigt, dass sie in der Lage sind, Schwachstellen zu entdecken und neuartige Exploits zu entwickeln, wodurch wichtige Betriebssysteme und Software, die in den IKT-Umgebungen fast aller Organisationen zum Einsatz kommen, dem Risiko von Cyberangriffen ausgesetzt sind

(5) In der Vergangenheit wurden solche Schwachstellen nur selten entdeckt. Oftmals waren Sicherheitsexperten involviert, was gezielte Abhilfemaßnahmen ermöglichte. In diesen Fällen wird Softwareanbietern häufig ein standardisierter Zeitrahmen — in der Regel 90 Tage — eingeräumt, um die Schwachstelle vor ihrer öffentlichen Bekanntmachung zu schließen. Durch die Verbreitung von Frontier-Modellen dürfte sich jedoch die Anzahl der entdeckten Schwachstellen erhöhen

(6) Die derzeitigen Patching-Verfahren im Finanzsystem sind überwiegend reaktiv und beruhen auf regelmäßigen Aktualisierungen und Ad-hoc-Reaktionen auf offengelegte Schwachstellen. Dieser Ansatz funktioniert in einem Bedrohungsumfeld, in dem ausreichend Zeit für die Entdeckung von Schwachstellen bleibt. Angesichts der zunehmenden Anzahl der Schwachstellen reichen die derzeitigen Verfahren jedoch unter Umständen nicht mehr aus, um die operationale Resilienz aufrechtzuerhalten

(7) Infolge der zunehmenden Anzahl der Schwachstellen stoßen zudem die derzeitigen Patching-Verfahren an ihre Grenzen, da in deren Rahmen Abhilfemaßnahmen anhand des Risikos priorisiert werden und Software-Patches vor ihrer Implementierung getestet werden müssen, um die Betriebsstabilität zu gewährleisten. Werden innerhalb kurzer Zeit zu viele Schwachstellen mit kritischen Auswirkungen entdeckt, sodass die Anzahl der erforderlichen kritischen Software-Patches erheblich zunimmt, müssen die Finanzinstitute womöglich entscheiden, ob sie erhebliche Cyberrisiken in Kauf nehmen oder ob sie die Anforderungen an das Testen von Patches verringern und dadurch operative Vorfälle und Ausfälle riskieren

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

(8) Die Entwicklung von Exploits, die als Waffe eingesetzt werden („weaponised exploits"), wurde früher weitgehend manuell von menschlichen Experten durchgeführt und nahm Tage oder Wochen in Anspruch, während sie nun von Frontier-Modellen innerhalb weniger Minuten oder Stunden erstellt werden können. Dies führt zu einem Wegfall defensiver Zeitpuffer, die erforderlich sind, um die Kontinuität kritischer und wichtiger Funktionen während der Abhilfemaßnahmen aufrechtzuerhalten

(9) Mit der zunehmenden Nutzung von Exploits als Waffe zur Ausnutzung kritischer Schwachstellen durch den Einsatz von KI und der damit einhergehenden Verringerung defensiver Zeitpuffer steigt das Risiko für einzelne kritische oder wichtige Funktionen und Institute stark an. Treten solche Risiken bei diesen Funktionen und Instituten gleichzeitig ein, könnte dies zu einer dauerhaften Zunahme systemischer Cyberrisiken führen, für die derzeit kein vollständig wirksamer Rahmen zur Risikominderung zur Verfügung steht. Aufgrund der engen Verflechtungen innerhalb des Finanzsektors der Union sowie zwischen diesem Sektor und anderen Sektoren und Ländern stellt diese Situation ein systematisches Risiko dar und birgt das Potenzial, systemische Angriffsflächen zu schaffen

(10) Darüber hinaus werden Frontier-Modelle gegenwärtig nur von einer kleinen Zahl von KI-Anbietern entwickelt, von denen mehrere Bedenken geäußert haben, dass künftige Frontier-Modelle für einen uneingeschränkten Zugang der Öffentlichkeit zu leistungsfähig sein könnten

(11) KI wird bereits von böswilligen Akteuren eingesetzt, um Cyberangriffe zu verstärken. Es ist wahrscheinlich, dass diese Akteure irgendwann –, sei es durch Datenlecks, Diebstahl, unabhängige Entwicklung oder offenen Zugang — KI-Modelle erlangen werden, deren Fähigkeiten mit denen vergleichbar sind, die gegenwärtig in kontrollierten Abwehrumgebungen eingesetzt werden

(12) Zwar können Frontier-Modelle die offensiven Fähigkeiten und die Wahrscheinlichkeit komplexer Cyberangriffe erheblich erhöhen, doch werden sie auch die defensiven Fähigkeiten stärken, insbesondere in Bezug auf die Entdeckung von Schwachstellen, die Datenkorrelation und die Abhilfemaßnahmen einzelner Institute. Kurz- bis mittelfristig dürfte jedoch die Steigerung der Geschwindigkeit, des Umfangs und der Genauigkeit der offensiven Fähigkeiten die Vorteile überwiegen

(13) Aufgrund der rasanten Entwicklung von Frontier-Modellen ist es erforderlich, die für die Finanzstabilität ermittelten Risiken unverzüglich anzugehen, um deren Eintreten zu verhindern oder zumindest ihre potenziellen Auswirkungen abzufedern. Um die Finanzstabilität auf den Finanzmärkten der Union zu gewährleisten, sollten alle Mitglieder des Europäischen Ausschusses für Systemrisiken (ESRB) im Rahmen ihrer makroprudenziellen und mikroprudenziellen Maßnahmen die Auswirkungen von Frontier-Modellen auf die operativen Fähigkeiten und die operationale Resilienz von Finanzinstituten berücksichtigen. Dies gilt unbeschadet des geldpolitischen Mandats der Zentralbanken der Union. Im Rahmen der derzeitigen Initiativen der Behörden hat die EZB beispielsweise in ihrer Rolle als Bankenaufsicht die bedeutenden Institute aufgefordert, die Auswirkungen der sich entwickelnden Bedrohungslage unverzüglich zu bewerten und bis zum 31. Oktober 2026 einen umfassenden Maßnahmenplan zu entwickeln, der konkrete Maßnahmen zur Bewältigung dieser Risiken darlegt ([4])

(14) Im Lichte der zunehmenden Verbreitung von KI-Technologien ist es wichtig sicherzustellen, dass alle kritischen Infrastrukturen und insbesondere Finanzinstitute darauf vorbereitet sind, Frontier-Modell-gestützten Cyberangriffen zu begegnen und rechtzeitig angemessene Vorbereitungen zu treffen. Solche defensiven Maßnahmen einzelner Unternehmen wären jedoch unzureichend. Eine wirksame Reaktion und Risikominderung erfordert eine koordinierte Antwort aller betroffenen Parteien, einschließlich KI-Anbietern, Softwareanbietern, Sicherheitsfirmen, Open-Source-Maintainern, Finanzinstituten und Behörden sowohl auf nationaler als auch auf Unionsebene

(15) Bei der Behandlung der oben genannten Fragen ist es wichtig, auf die einschlägigen rechtlichen und politischen Rahmenbedingungen der Union hinzuweisen, insbesondere auf die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates ([5]), die Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates ([6]), die Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates ([7]) sowie die Empfehlung des Europäischen Ausschusses für Systemrisiken (ESRB/2021/17) ([8])

([4]) Das Schreiben an die bedeutenden Institute ist auf der Website der EZB zur Bankenaufsicht unter www.bankingsupervision.europa.eu abrufbar.

([5]) Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) (ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Empfehlung des Europäischen Ausschusses für Systemrisiken vom 2. Dezember 2021 zu einem europaweiten Koordinierungsrahmen für betreffende Behörden in Bezug auf systemische Cybervorfälle (ESRB/2021/17) (ABl. C 134 vom 25.3.2022, S. 1).

(16) Die Verordnung (EU) 2022/2554 bietet einen umfassenden Rahmen für Finanzinstitute, um IKT-Risiken, einschließlich jener, die von Cyberangriffen herrühren, zu ermitteln, zu managen, zu überwachen und zu mindern. Angesichts der Verflechtung des Finanzsektors und seiner Abhängigkeit von IKT-Systemen und -Drittdienstleistern könnte ein erfolgreicher Cyberangriff, der ein oder mehrere Finanzinstitute oder deren kritische Dienstleister betrifft, erhebliche systemische Auswirkungen haben. Die Finanzaufsichtsbehörden sollten den Aufsichtstätigkeiten in diesem Bereich angemessene Priorität einräumen und dabei den potenziellen Auswirkungen solcher Cyberangriffe auf die Stabilität, Integrität und Vertrauenswürdigkeit des Finanzsystems sowie dem daraus möglicherweise resultierenden operativen, finanziellen und verbraucherbezogenen Schaden Rechnung tragen

(17) In der Verordnung (EU) 2024/1689 werden harmonisierte Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck in der Union festgelegt, darunter unter bestimmten Bedingungen auch von Systemen und Modellen, die von in Drittländern niedergelassenen KI-Anbietern bereitgestellt werden, wenn die vom KI-System generierten Ergebnisse in der Union verwendet werden oder wenn ein KI-Modell in ein System integriert ist, das auf dem Unionsmarkt in Verkehr gebracht wird. Diese Verordnung sieht ferner spezifische Vorschriften vor, unter anderem einen strengeren Rechtsrahmen für Modelle, die als KI-Modelle mit allgemeinem Verwendungszweck eingestuft sind und systemische Risiken bergen

(18) In der Verordnung (EU) 2024/2847 werden verpflichtende Cybersicherheitsanforderungen für Hersteller eingeführt, welche die Planung, den Entwurf, die Entwicklung und die Wartung von Hardware- und Softwareprodukten mit digitalen Elementen betreffen, die auf dem Unionsmarkt in Verkehr gebracht werden. Nach Maßgabe der Verordnung sind Hersteller zudem verpflichtet, Schwachstellen während des Lebenszyklus ihrer Produkte zu beheben. Sobald sie im Dezember 2027 in vollem Umfang anwendbar ist, müssen auch Finanzunternehmen, die solche Produkte auf dem Unionsmarkt in Verkehr bringen, sicherstellen, dass sie diese Anforderungen erfüllen

(19) In der Empfehlung ESRB/2021/17 wurde empfohlen, dass die Europäischen Aufsichtsbehörden (European Supervisory Authorities — ESAs) gemeinsam im Rahmen des Gemeinsamen Ausschusses und zusammen mit der Europäischen Zentralbank (EZB), dem ESRB und den jeweiligen nationalen Behörden eine wirksame koordinierte Reaktion auf Unionsebene entwickeln, für den Fall, dass es zu einem schwerwiegenden grenzüberschreitenden Cybervorfall oder zu einer vergleichbaren Bedrohung kommt, die systemische Auswirkungen auf den Finanzsektor der Union mit sich bringen könnte. Dies führte zur Einrichtung des europaweiten Koordinierungsrahmens für systemische Cybervorfälle (EU-SCICF), der eine wertvolle operative Plattform für den Informationsaustausch und die Koordinierung zwischen den Finanzbehörden bietet

(20) Vor diesem Hintergrund gibt der ESRB hiermit eine allgemeine Warnung aus, welche die erheblichen Risiken für die Finanzstabilität zum Gegenstand hat, die durch die Entwicklung von Frontier-Modellen verstärkt werden. Die Warnung berücksichtigt die analytischen Arbeiten in der im Juni 2026 veröffentlichten ESRB-Mitteilung „Addressing Frontier AI Models with cyber capabilities from a financial stability perspective“ (Umgang mit Frontier-KI-Modellen mit Cyberfähigkeiten aus Sicht der Finanzstabilität) ([9]).

HAT FOLGENDE WARNUNG AUSGEGEBEN:

ABSCHNITT 1

Warnung

Neue Risikolandschaft

Die rasante Entwicklung hochmoderner KI-Modelle (Frontier-Modelle) mit Cyberfähigkeiten bringt wesentliche Veränderungen der Risikolandschaft für das Finanzsystem der Union mit sich. Aktuelle Erkenntnisse deuten darauf hin, dass Frontier-Modelle in der Lage sind, Schwachstellen zu entdecken, funktionsfähige Exploits zu generieren und eigenständig groß angelegte Cyberangriffe mit einer Geschwindigkeit, einem Umfang und einer Genauigkeit durchzuführen, die bisherige KI-Modelle bei weitem übertreffen. Dies stellt einen Paradigmenwechsel auf dem Gebiet der Cybersicherheit und einen Wendepunkt hinsichtlich der KI-Fähigkeiten dar.

Der ESRB ist der Auffassung, dass diese Entwicklungen eine Quelle systemischer Risiken für das Finanzsystem darstellen, die das Potenzial bergen, erhebliche negative Auswirkungen auf die Cybersicherheit zu haben — durch die beschleunigte Entdeckung von Schwachstellen, die Verkürzung der für Reaktionen und wirksame Abwehrmaßnahmen zur Verfügung stehenden Zeit, das zunehmende Ausmaß und die größere Raffinesse von Cyberangriffen sowie die Entstehung neuer Abhängigkeiten und Konzentrationsrisiken innerhalb des Finanzsystems. Zwar erkennt der ESRB an, dass Frontier-Modelle den Finanzinstituten verbesserte defensive Fähigkeiten eröffnen, doch werden diese Fähigkeiten wahrscheinlich erst in den nächsten Jahren schrittweise zum Tragen kommen, sodass die Finanzinstitute einen Übergangszeitraum überstehen müssen, der durch erhöhte Risiken, hohe Unsicherheit und eine sich rasant wandelnde technologische Landschaft gekennzeichnet ist. Angesichts der starken Digitalisierung und Verflechtung des Finanzsystems könnten sich solche negativen Auswirkungen auf die Cybersicherheit rasch ausbreiten und kritische und wichtige Funktionen in Finanzinstituten beeinträchtigen, was letztlich zu systemischen Störungen und einem Verlust des Vertrauens in das Finanzsystem führen würde.

([9]) Abrufbar auf der Website des ESRB unter www.esrb.europa.eu.

Die neuen Frontier-Modelle erhöhen das inhärente IKT-Risiko und bewirken eine Schwächung der operationalen Resilienz im gesamten Finanzsektor, insbesondere in den folgenden vier Bereichen: a) Zeit, einschließlich der Fähigkeit, komplexe Systeme zügig zu patchen, ohne operative Ausfälle zu verursachen, unter Berücksichtigung des Wegfalls defensiver Zeitpuffer zwischen der Entdeckung von Schwachstellen und dem Einsatz von Exploits als Waffe (weaponisation); b) die Fähigkeit der Verteidiger, einschließlich ihrer Fähigkeit, Frontier-Modell-gestützte automatisierte und manuelle Sicherheitstests durchzuführen, sowie ihrer Fähigkeit, Schutz vor dem feindlichen Einsatz von Frontier-Modellen zu bieten und Bedrohungen durch den feindlichen Einsatz von Frontier-Modellen zu erkennen und darauf zu reagieren; c) Konzentration, einschließlich der Abhängigkeiten von einer begrenzten Zahl von KI-Anbietern, die ihrerseits von Cloud-Anbietern, Open-Source-Komponenten und anderer weitverbreiteter Software abhängig sind; und d) die Fähigkeit der Behörden, einschließlich der Kalibrierung ihrer Erwartungen sowie der Durchführung von Stresstests und Vorsorgemaßnahmen im Einklang mit der Entwicklung von Frontier-Modellen, damit operative Ausfälle nicht zu einer Quelle weitergehender Instabilität werden.

Darüber hinaus ist es schwierig, innerhalb von Finanzinstituten den Einsatz von KI sichtbar zu machen und aufrechtzuerhalten — einschließlich eines umfassenden Verständnisses dessen, wo und wie KI eingesetzt wird –, wenn man bedenkt, dass KI in Kundenschnittstellen, internen Agenten, Geschäftsprozessen und bei der Integration mit Dritten zum Einsatz kommt.

Systemische Bewertung

Die festgestellten Entwicklungen können sowohl das Ausmaß als auch die Struktur von Cyberrisiken wesentlich verändern und sowohl direkte als auch indirekte Risiken für die Finanzstabilität verstärken. Die Frontier-Modell-Fähigkeiten können erheblichen Druck auf die bestehenden Resilienzrahmen ausüben, insbesondere wenn Vorfälle weit verbreitet sind und simultan auftreten. Vorfälle können sich zudem rasch bei Finanzinstituten und auf Finanzmärkten ausbreiten, wenn kritische Drittanbieter, gemeinsame technologische Ökosysteme oder weit verbreitete Open-Source-Komponenten betroffen sind, wodurch sich das Risiko diesbezüglicher Störungen mit systemischen Auswirkungen erhöht.

Durch Frontier-Modelle werden drei Quellen der Asymmetrie im Finanzsektor beeinflusst: erstens zwischen Ländern, zweitens zwischen Verteidigern und Angreifern und drittens zwischen besser und weniger gut ausgestatteten Finanzinstituten.

Erstens ist die Union aufgrund der derzeitigen geografischen Konzentration führender KI-Anbieter außerhalb der Union strategischen Abhängigkeiten und geopolitischen Risiken ausgesetzt. Um die Asymmetrie in den Bereichen Wissen und Technologie zwischen den Ländern zu verringern, müssen Maßnahmen ergriffen werden, um der Union und ihren Mitgliedstaaten einen angemessenen und verhältnismäßigen Zugang zu neu entwickelten Frontier-Modellen zu ermöglichen. Diese Maßnahmen sollten sowohl in Bezug auf die politischen Vorgaben als auch auf die Umsetzung zeitnah, kohärent und effizient sein und den verschiedenen Finanzsektoren der Union angemessen Rechnung tragen, wobei die Fachkenntnisse der entsprechenden ESAs genutzt werden sollten. Dies wird nicht nur die Asymmetrie zwischen der Union und Drittländern, sondern auch zwischen Finanzinstituten mit Sitz in verschiedenen Mitgliedstaaten verringern, wodurch gleiche Wettbewerbsbedingungen innerhalb und außerhalb der Union gewahrt und systemische Risiken minimiert werden. Regelungen, die den Zugang zu Frontier-Modellen nur für bestimmte Kategorien von Instituten oder in ausgewählten Ländern ermöglichen, würden zur Fragmentierung des Finanzbinnenmarkts beitragen und dessen Liquidität und Tiefe verringern.

Was zweitens die Asymmetrie zwischen Angreifern und Verteidigern betrifft, so werden die Einstiegshürden für Angreifer durch Frontier-Modelle gesenkt. Bedrohungsakteure werden sich wahrscheinlich zunehmend auf Frontier-Modelle stützen, um die technisch fortschrittlicheren und arbeitsintensiveren Teile offensiver Operationen durchzuführen und so die Kosten zu senken. Verteidiger hingegen werden durch operative Anforderungen, Abhängigkeiten und regulatorische Verpflichtungen eingeschränkt, was die Wirkung und den Umfang, in dem sie kurz- bis mittelfristig von Frontier-Modellen profitieren können, begrenzt und letztlich längere Anpassungszeiträume erfordert.

Drittens gibt es Unterschiede hinsichtlich der Finanzinstituten zur Verfügung stehenden Ressourcen und Ausstattung, um den durch Frontier-Modellen verursachten Herausforderungen zu begegnen. Diese Unterschiede können auf Kosten zurückzuführen sein, die eher fix als skaliert sind, auf begrenzte Ressourcen und auf einen eingeschränkten Zugang zu Spezialisten. Wenn die Fähigkeit zur Bewältigung solcher Herausforderungen asymmetrisch ist, kann das schwächste Glied der Kette die Stabilität des Systems beeinträchtigen.

Auswirkungen

Es muss unbedingt sichergestellt werden, dass systemrelevante Zahlungsverkehrs- und Abwicklungssysteme und Finanzmarktinfrastrukturen weiterhin vor Schwachstellen geschützt bleiben, die sich aus der Nutzung und Entwicklung von Frontier-Modellen ergeben. Öffentliche und private Betreiber sollten ihre Cybersicherheitsrahmen gründlich überprüfen und aktualisieren, um solchen Schwachstellen Rechnung zu tragen. Die für die Aufsicht oder Überwachung zuständigen Behörden sollten Maßnahmen ergreifen, die sicherstellen, dass die Systeme angemessen geschützt sind. Die Zusammenarbeit zwischen Behörden und privaten Finanzinstituten sollte fortgesetzt werden, wann immer dies erforderlich ist, um die Sicherheit und Resilienz des Finanzsystems der Union zu stärken.

In seinem Bericht zu „Systemic cyber risk“ aus dem Jahr 2020 ([10]) nannte der ESRB Geschwindigkeit, Ausmaß und böswillige Absicht von Cyberbedrohungen als mögliche Quellen der Ausbreitung systemischer Risiken. Die Behörden sollten sich darüber bewusst sein, dass Frontier-Modelle zwar eine neue Quelle für die Ausbreitung darstellen, sie jedoch auch die zuvor ermittelten Quellen verstärken, und sie sollten diese Erkenntnis in ihre politischen Maßnahmen einbeziehen. Unter Berücksichtigung aller Risiken für die Finanzstabilität, die sich aus der operativen Exposition gegenüber Cyberrisiken im Finanzsektor ergeben, ist es wichtig sicherzustellen, dass den in dieser Warnung aufgeführten Bedenken in der Aufsichts- und Überwachungstätigkeit und den politischen Positionen der betreffenden Behörden im Rahmen ihrer jeweiligen Mandate Rechnung getragen wird.

Die betreffenden Behörden sollten sich im Rahmen ihrer jeweiligen Zuständigkeiten und insbesondere innerhalb des durch die Verordnung (EU) 2022/2554 geschaffenen Rahmens der drei zuvor genannten Quellen der Asymmetrie bewusst sein, die von den Frontier-Modellen im Finanzsektor verursacht werden. Um diese Asymmetrien zu verringern, sollten neben den bestehenden Testrahmen Kooperationsvereinbarungen und eine sektorbezogene Koordinierung in Betracht gezogen werden ([11]). Die Finanzbehörden sollten darüber hinaus sicherstellen, dass sich die Leitungsorgane privater Finanzinstitute uneingeschränkt für die Minderung der von Frontier-Modellen ausgehenden Cyberrisiken einsetzen, dass klare Governance- und Rechenschaftsrahmen vorhanden sind und dass zeitnahe Reaktionen angemessen geplant sowie entsprechende interne Investitionen getätigt werden.

Mehrere mögliche Entwicklungen, die in dieser Warnung berücksichtigt werden — seien es die systemischen Auswirkungen, das geopolitische Risiko oder das verschobene Gleichgewicht zwischen Angreifern und Verteidigern — sind geeignet, das Funktionieren des Finanzsystems zu beeinträchtigen und sich auf das Vertrauen in das Finanzsystem auszuwirken. Um diese Entwicklungen kontinuierlich zu bewerten, wird der ESRB prüfen, ob sie bei Risikobewertungen, Testrahmen und aufsichtlichen Erwartungen sowie bei der Entwicklung künftiger Szenarien berücksichtigt werden müssen. Der ESRB wird ferner die Nutzung und Entwicklung von Frontier-Modellen und ihre Auswirkungen auf den Finanzsektor unter dem Gesichtspunkt systemischer Risiken überwachen. Darüber hinaus wird der ESRB die Entwicklungen bei jeder vierteljährlichen Risikobewertung auf Ebene des Verwaltungsrats neu bewerten und erforderlichenfalls weitere Maßnahmen in Erwägung ziehen.

ABSCHNITT 2

Begriffsbestimmungen

Für die Zwecke dieser Warnung gelten die folgenden Begriffsbestimmungen:

1. „KI-Anbieter“ ein Anbieter im Sinne von Artikel 3 Nummer 3 der Verordnung (EU) 2024/1689;
2. „hochmoderne KI-Modelle (Frontier-Modelle)“ fortgeschrittene KI-Modelle mit allgemeinem Verwendungszweck, die in der Lage sind, offensive oder defensive Cyberoperationen wesentlich zu beeinflussen;
3. „Cyberangriff“ ein Cyberangriff im Sinne von Artikel 1 der Verordnung (EU) 2019/796 des Rates ([12]), auch wenn dieser seinen Ausgang innerhalb der Union hat;
4. „Schwachstelle“ eine Schwachstelle im Sinne von Artikel 3 Nummer 16 der Verordnung (EU) 2022/2554;
5. „Exploit“ ein Tool, ein Verfahren oder eine Methode, das bzw. die verwendet wird, um eine oder mehrere Schwachstellen auszunutzen, um sich unbefugten Zugriff zu Systemen zu verschaffen, diese zu verändern oder Systemstörungen herbeizuführen oder auf andere Weise IKT-Risiken oder IKT-bezogene Vorfälle zu verursachen;
6. „Einsatz als Waffe“ (weaponisation) die Erstellung oder Anpassung von Exploits zur systematischen oder skalierbaren Ausnutzung von Schwachstellen;
7. „kritische oder wichtige Funktion“ eine kritische oder wichtige Funktion im Sinne von Artikel 3 Nummer 22 der Verordnung (EU) 2022/2554;
8. „KI-Modell mit allgemeinem Verwendungszweck“ ein KI-Modell im Sinne von Artikel 3 Nummer 63 der Verordnung (EU) 2024/1689;
9. „KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko“ ein KI-Modell mit allgemeinem Verwendungszweck, das gemäß Artikel 51 Absatz 1 der Verordnung (EU) 2024/1689 als KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko eingestuft ist;
10. „IKT-bezogener Vorfall“ ein Vorfall im Sinne von Artikel 3 Nummer 8 der Verordnung (EU) 2022/2554;

([10]) Siehe Systemic cyber risk, ESRB, Februar 2020, abrufbar auf der Website des ESRB unter www.esrb.europa.eu.

([11]) Z. B. ethisches Hacking auf Basis von Threat Intelligence (TIBER), bedrohungsorientierte Penetrationstests (TLPT), fortgeschrittenes Hacking (ART) und Stresstests zur Cyberresilienz (CyRST)

([12]) Verordnung (EU) 2019/796 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (ABl. L 129 I vom 17.5.2019, S. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11. „IKT-Risiko“ ein Risiko im Sinne von Artikel 3 Nummer 5 der Verordnung (EU) 2022/2554;

12. „operationale Resilienz“ digitale operationale Resilienz im Sinne von Artikel 3 Nummer 1 der Verordnung (EU) 2022/2554.

Geschehen zu Frankfurt am Main am 25. Juni 2026.

Der Leiter des ESRB-Sekretariats,
im Auftrag des Verwaltungsrats des ESRB,
Francesco MAZZAFERRO