C/2026/3795

16.7.2026

DET EUROPÆISKE UDVALG FOR SYSTEMISKE RISICIS ADVARSEL

af 25. juni 2026

om systemiske cyberrisici fra banebrydende modeller for kunstig intelligens

(ESRB/2026/3)

(C/2026/3795)

DET ALMINDELIGE RÅD FOR DET EUROPÆISKE UDVALG FOR SYSTEMISKE RISICI HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til aftalen om Det Europæiske Økonomiske Samarbejdsområde ([1]), særlig bilag IX,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 1092/2010 af 24. november 2010 om makrotilsyn på EU-plan med det finansielle system og om oprettelse af et europæisk udvalg for systemiske risici ([2]), særlig artikel 3, stk. 2, litra c), og artikel 16 og 18,

under henvisning til Det Europæiske Udvalg for Systemiske Risicis afgørelse ESRB/2011/1 af 20. januar 2011 om vedtagelse af forretningsordenen for Det Europæiske Udvalg for Systemiske Risici ([3]), særlig artikel 18 og 19, og

ud fra følgende betragtninger:

(1) Førende udbydere af kunstig intelligens (AI) har udviklet banebrydende AI-modeller (Frontier AI Models, FAIM'er), som er yderst kompetente på cybersikkerhedsområdet og kan udføre fuldautomatiske cyberangreb på komplekse systemer, herunder gennem opdagelse af sårbarheder og udvikling og anvendelse af exploits som våben, hvilket grundlæggende ændrer cybertrusselsbilledet

(2) FAIM'er er betydeligt bedre end tidligere AI-modeller hvad angår at finde måder at udføre cyberangreb på, idet de klarer sig bedre end tidligere modeller med hensyn til omkostninger, hastighed og nøjagtighed, og de konkurrerer nu med førende menneskelige eksperter

(3) FAIM'er har kapacitet til at true de systemer, der understøtter de informations- og kommunikationsteknologiske (IKT) miljøer, som den finansielle infrastruktur er afhængig af, hvilket øger sandsynligheden for og alvoren af cyberhændelser med systemiske virkninger

(4) FAIM'er har vist, at de er i stand til at opdage sårbarheder og udnytte nye muligheder og dermed udsætte store operativsystemer og software, der anvendes i næsten alle organisationers IKT-miljøer, for risikoen for cyberangreb

(5) Historisk set har opdagelsen af sådanne sårbarheder været sjælden og ofte foretaget af sikkerhedsforskere, hvilket har givet mulighed for målrettet afhjælpning. I disse tilfælde får softwareudbydere ofte en standardiseret tidsramme — normalt 90 dage — til at afhjælpe sårbarheden, inden den offentliggøres. FAIM'er vil dog sandsynligvis øge omfanget af konstaterede sårbarheder

(6) Den nuværende lapningspraksis i det finansielle system er overvejende reaktiv og bygger på periodiske opdateringer og ad hoc-reaktioner på afslørede sårbarheder. Denne tilgang fungerer i et trusselsmiljø, hvor der er tid til, at opdagelsen af sårbarheder fortsat kan håndteres. Med en stigning i sårbarhedernes omfang kan den nuværende praksis imidlertid blive utilstrækkelig til at opretholde den operationelle modstandsdygtighed

(7) Denne stigning i mængden udsætter også de nuværende lapningsprocesser for overbelastning, da de prioriterer afhjælpende foranstaltninger baseret på risiko og kræver test af softwarelapninger inden gennemførelsen for at sikre operationel stabilitet. Hvis der opdages for mange sårbarheder med kritiske virkninger inden for en kort tidsramme, således at antallet af nødvendige kritiske softwarelapninger øges betydeligt, kan de finansielle institutioner være nødt til at vælge mellem at udsætte sig selv for væsentlige cyberrisici eller reducere kravene om at teste lapninger og dermed risikere operationelle hændelser og afbrydelser

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

(8) Fremstillingen af exploits til anvendelse som våben foregik tidligere i vid udstrækning manuelt og tog menneskelige ekspertdage eller -uger, mens det nu kan gøres af FAIM'er på få minutter eller timer. Dette udgør et sammenbrud af defensive tidsbuffere, som er nødvendige for at opretholde videreførelsen af kritiske og vigtige funktioner under afhjælpningen

(9) Med udbredelsen af kunstig intelligens som våben mod kritiske sårbarheder og den tilsvarende reduktion af defensive tidsbuffere øges risikoen for individuelle kritiske eller vigtige funktioner og institutioner kraftigt. Hvis sådanne risici opstår samtidig på tværs af disse funktioner og institutter, kan dette føre til en permanent stigning i systemiske cyberrisici, for hvilke der på nuværende tidspunkt ikke findes nogen fuldt ud effektiv afbødningsramme. På grund af den stærke indbyrdes forbundethed inden for Unionens finansielle sektor samt mellem denne sektor og andre sektorer og jurisdiktioner udgør denne situation en systematisk risiko og kan potentielt skabe systemiske svagheder

(10) Desuden er FAIM'er i øjeblikket kun ved at blive udviklet af et lille antal AI-udbydere, hvoraf flere har udtrykt bekymring for, at kommende FAIM'er kan være for kraftige til at give ubegrænset offentlig adgang

(11) Kunstig intelligens anvendes allerede af ondsindede aktører til at øge antallet af cyberangreb. Det er sandsynligt, at sådanne aktører i sidste ende vil opnå AI-modeller med kapaciteter, der kan sammenlignes med dem, der i øjeblikket anvendes i kontrollerede defensive miljøer, enten gennem lækager, tyveri, uafhængig udvikling eller åben adgang

(12) Selv om FAIM'er i væsentlig grad kan øge offensive kapaciteter og sandsynligheden for sofistikerede cyberangreb, vil de også styrke defensive kapaciteter, navnlig med hensyn til opdagelse af sårbarheder, datakorrelation og individuelle institutioners afhjælpende foranstaltninger. På kort til mellemlang sigt vil forøgelsen af offensive kapaciteters hastighed, omfang og nøjagtighed dog sandsynligvis opveje fordelene

(13) Den hurtige udvikling af FAIM'er gør det nødvendigt straks at imødegå de identificerede risici for den finansielle stabilitet for at forhindre, at de opstår, eller i det mindste for at afbøde deres potentielle virkninger. For at sikre finansiel stabilitet på Unionens finansielle markeder bør alle medlemmer af Det Europæiske Udvalg for Systemiske Risici (ESRB) overveje konsekvenserne af FAIM'er for finansielle institutioners operationelle kapacitet og modstandsdygtighed i forbindelse med deres makroprudentielle og mikroprudentielle politiske tiltag. Dette berører ikke de pengepolitiske mandater for centralbankerne i Unionens. Som et eksempel, og blandt andre myndigheders nuværende initiativer, har ECB i sin rolle som banktilsynsmyndighed anmodet de signifikante institutter om straks at vurdere virkningen af det skiftende trusselsbillede og senest 31. oktober 2026 udarbejde en omfattende handlingsplan med konkrete foranstaltninger til håndtering af sådanne risici ([4])

(14) Efterhånden som AI-teknologien udbredes, er det vigtigt at sikre, at al kritisk infrastruktur og navnlig finansielle institutioner er parate til at imødegå cyberangreb, der drives af FAIM'er, og foretage rettidige og passende forberedelser. En sådan defensiv indsats fra de enkelte enheders side vil imidlertid være utilstrækkelig. En effektiv indsats og risikoreduktion kræver en koordineret reaktion, der involverer alle berørte parter, herunder AI-udbydere, softwareudbydere, sikkerhedsfirmaer, open source-vedligeholdelsesvirksomheder, finansielle institutioner og myndigheder på både nationalt plan og EU-plan

(15) Når ovennævnte spørgsmål behandles, er det vigtigt at minde om Unionens relevante retlige og politiske rammer, navnlig Europa-Parlamentets og Rådets forordning (EU) 2022/2554 ([5]), Europa-Parlamentets og Rådets forordning (EU) 2024/1689 ([6]), Europa-Parlamentets og Rådets forordning (EU) 2024/2847 ([7]) og Det Europæiske Udvalg for Systemiske Risicis henstilling (ESRB/2021/17) ([8])

([4]) Brevet til signifikante institutter er tilgængeligt på ECB's websted for banktilsyn www.bankingsupervision.europa.eu.

([5]) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 af 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens og om ændring af forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 samt direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (Ai-forordningen) (EUT L, 2024/1689 af 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed) (EUT L, 2024/2847 af 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Det Europæiske Udvalg for Systemiske Risicis henstilling af 2. december 2021 om en paneuropæisk ramme for relevante myndigheders koordinering i tilfælde af systemiske cyberhændelser (ESRB/2021/17) (EUT C 134 af 25.3.2022, s. 1).

(16) Forordning (EU) 2022/2554 udgør en omfattende ramme for finansielle institutioner med henblik på at identificere, styre, overvåge og afbøde IKT-risici, herunder risici som følge af cyberangreb. I betragtning af den finansielle sektors indbyrdes forbundethed og dens afhængighed af IKT-systemer og tredjepartsudbydere af tjenester kan et vellykket cyberangreb, der påvirker en eller flere finansielle institutioner eller deres udbydere af kritiske tjenester, have betydelige systemiske konsekvenser. De finansielle tilsynsmyndigheder bør give passende prioritet til tilsynsaktiviteter på dette område under hensyntagen til sådanne cyberangrebs potentielle indvirkning på det finansielle systems stabilitet, integritet og troværdighed samt til den operationelle, finansielle og forbrugermæssige skade, der kan opstå som følge heraf

(17) Ved forordning (EU) 2024/1689 fastsættes der harmoniserede regler for omsætning, ibrugtagning og anvendelse af AI-systemer og AI-modeller til almen brug i Unionen, herunder under visse omstændigheder systemer og modeller, der leveres af AI-udbydere etableret i tredjelande, hvis det output, der produceres af AI-systemet, anvendes i Unionen, eller hvis en AI-model integreres i et system, der bringes i omsætning på EU-markedet. Denne forordning fastsætter også specifikke regler, herunder en strengere reguleringsordning, for modeller, der er klassificeret som AI-modeller til almen brug med systemisk risiko

(18) Ved forordning (EU) 2024/2847 indføres obligatoriske cybersikkerhedskrav for fabrikanter, som omfatter planlægning, design, udvikling og vedligeholdelse af hardware- og softwareprodukter med digitale elementer, der bringes i omsætning på EU-markedet. Det kræver også, at fabrikanterne håndterer sårbarheder i løbet af deres produkters livscyklus. Når den er fuldt ud gældende i december 2027, vil finansielle enheder, der bringer sådanne produkter i omsætning på EU-markedet, også skulle sikre, at produkterne opfylder disse krav

(19) I henstilling ESRB/2021/17 henstilles det, at de europæiske tilsynsmyndigheder (ESA'er) i fællesskab gennem Det Fælles Udvalg og sammen med Den Europæiske Centralbank (ECB), ESRB og de relevante nationale myndigheder udvikler en effektiv koordineret reaktion på EU-plan i tilfælde af en større grænseoverskridende cyberhændelse eller relateret trussel, der kan have en systemisk indvirkning på Unionens finansielle sektor. Dette resulterede i oprettelsen af den paneuropæiske ramme for koordinering af systemiske cyberhændelser (EU- SCICF), som udgør en værdifuld og operationel platform for udveksling af oplysninger og koordinering mellem finansielle myndigheder

(20) På denne baggrund vedtager ESRB hermed en generel advarsel om de betydelige risici for den finansielle stabilitet, der forstærkes af udviklingen af FAIM'er. Advarslen tager hensyn til det analytiske arbejde i ESRB's notat »Addressing Frontier AI Models with cyber capabilities from a financial stability perspective« ([9]), der blev offentliggjort i juni 2026 —

VEDTAGET DENNE ADVARSEL:

AFDELING 1

Advarsel

Nyt risikolandskab

Den hurtige udvikling af banebrydende AI-modeller (FAIM'er) med cyberkapacitet medfører væsentlige ændringer i risikolandskabet for Unionens finansielle system. Den nuværende dokumentation viser, at FAIM'er er i stand til at opdage sårbarheder, generere exploits og selvstændigt udføre cyberangreb i fuld skala med en hastighed, et omfang og en nøjagtighed, der langt overstiger tidligere AI-modeller. Dette udgør et paradigmeskift på cybersikkerhedsområdet og et springbræt hvad angår AI-kapacitet.

ESRB anser denne udvikling for at være en kilde til systemiske risici for det finansielle system med potentiale til at skabe betydelige negative virkninger for cybersikkerheden gennem fremskyndet opdagelse af sårbarheder, reduktion af den tid, der er til rådighed til reaktion og effektivt forsvar, øget omfang og kompleksitet af cyberangreb og indførelse af nye afhængigheds- og koncentrationsrisici i det finansielle system. Selv om ESRB anerkender, at FAIM'er vil tilbyde finansielle institutioner styrkede forsvarskapaciteter, vil disse kapaciteter sandsynligvis gradvist blive til virkelighed i løbet af de kommende år, hvilket kræver, at finansielle institutioner opererer i en overgangsperiode, der er kendetegnet ved høj risiko, stor usikkerhed og et teknologisk landskab i hastig udvikling. I betragtning af det finansielle systems stærkt digitaliserede og indbyrdes forbundne karakter kan sådanne negative virkninger for cybersikkerheden hurtigt spredes og påvirke kritiske og vigtige funktioner på tværs af finansielle institutioner, hvilket i sidste ende fører til systemiske forstyrrelser og tab af tillid til det finansielle system.

([9]) Findes på ESRB's websted www.esrb.europa.eu.

De nye FAIM'er øger den iboende IKT-risiko, hvilket fører til svækket operationel modstandsdygtighed i hele den finansielle sektor, navnlig på fire områder: a) tid, herunder evnen til hurtigt at fange komplekse systemer uden at forårsage operationelle fejl, under hensyntagen til sammenbruddet af defensive tidsbuffere mellem opdagelse af sårbarheder og anvendelse af exploits som våben b) forkæmperes kapacitet, herunder deres evne til at foretage automatiseret og manuel sikkerhedstestning støttet af FAIM samt deres evne til at beskytte, opdage og reagere på trusler, der stammer fra FAIM-anvendelse, c) koncentration, herunder afhængighed af et begrænset antal AI-udbydere, der igen er afhængige af cloududbydere, open source-komponenter og anden bredt anvendt software og d) myndighedernes kapacitet, herunder deres kalibrering af forventninger, stresstest og beredskabsforanstaltninger i overensstemmelse med udviklingen af FAIM'er, således at operationelle svigt ikke bliver en kilde til større ustabilitet.

Desuden er det en udfordring at etablere og opretholde synligheden af udbredelsen af kunstig intelligens i enhver finansiel institution — herunder fuldt ud at forstå, hvor og hvordan kunstig intelligens anvendes — under hensyntagen til, at den anvendes i kundegrænseflader, interne agenter, forretningsprocesser og integration med tredjeparter.

Systemisk vurdering

Den konstaterede udvikling kan i væsentlig grad ændre både omfanget og strukturen af cyberrisici og øge både direkte og indirekte risici for den finansielle stabilitet. FAIM-kapaciteterne kan sætte de eksisterende rammer for modstandsdygtighed under betydeligt pres, navnlig hvis hændelser er udbredte og forekommer samtidig. Hændelser kan også hurtigt sprede sig på tværs af finansielle institutioner og markeder, hvis kritiske tredjepartsudbydere, fælles teknologiske økosystemer eller almindeligt anvendte open source-komponenter påvirkes, hvilket øger risikoen for relaterede forstyrrelser med systemiske konsekvenser.

FAIM'er ændrer tre kilder til asymmetri i den finansielle sektor: den første mellem jurisdiktioner, den anden mellem forsvarere og angribere og den tredje mellem finansielle institutioner med bedre ressourcer og mindre veludstyrede finansielle institutioner.

For det første betyder den nuværende geografiske koncentration af førende AI-udbydere uden for Unionen, at Unionen er udsat for strategisk afhængighed og geopolitiske risici. For at mindske den videnbaserede og teknologiske asymmetri mellem jurisdiktioner er der behov for at vedtage foranstaltninger til at lette en passende og forholdsmæssig adgang for Unionen og dens medlemsstater til nyligt udviklede FAIM'er. Sådanne foranstaltninger bør være rettidige, sammenhængende og effektive, både med hensyn til politik og gennemførelse, og bør i tilstrækkelig grad tage hensyn til de forskellige finansielle sektorer i Unionen og drage fordel af de tilsvarende ESA'ers ekspertise. Dette vil ikke blot afhjælpe en asymmetri mellem Unionens og tredjelandes jurisdiktioner, men også mellem finansielle institutioner, der er etableret i forskellige medlemsstater, bevare lige vilkår i og uden for Unionen og minimere systemiske risici. Ordninger, der kun letter adgangen til FAIM'er for visse kategorier af institutter eller i udvalgte jurisdiktioner, vil bidrage til fragmenteringen af det indre marked for finansiering og mindske dets likviditet og dybde.

Hvad for det andet angår asymmetrien mellem angribere og forsvarere sænker FAIM adgangsprisen for angribere. Trusselsaktører vil sandsynligvis i stigende grad være afhængige af FAIM'er til at gennemføre de mere teknisk avancerede og arbejdskraftintensive dele af offensive operationer, hvilket reducerer omkostningerne. Forsvarere er derimod begrænset af operationelle krav, afhængighedsforhold og lovgivningsmæssige forpligtelser, hvilket begrænser den virkning og det omfang, som de kan drage fordel af FAIM'er til på kort til mellemlang sigt, hvilket i sidste ende kræver længere tilpasningsperioder.

For det tredje er der forskelle med hensyn til, hvordan de finansielle institutioner har ressourcer og udstyr til at håndtere udfordringerne i forbindelse med FAIM'er. Disse forskelle kan skyldes omkostninger, der er faste snarere end skalerede, ressourcemæssige begrænsninger og begrænset adgang til specialister. Hvis der er asymmetri i evnen til at håndtere sådanne udfordringer, kan det svageste led i kæden påvirke systemets stabilitet.

Implikationer

Det er vigtigt at sikre, at systemisk vigtige betalings- og afviklingssystemer og finansielle markedsinfrastrukturer fortsat er beskyttet mod sårbarheder, der opstår som følge af brug og udvikling af FAIM. Offentlige og private operatører bør grundigt gennemgå og opdatere deres cybersikkerhedsrammer for at tage hensyn til sådanne sårbarheder. Myndigheder med ansvar for tilsyn eller overvågning bør vedtage foranstaltninger for at sikre, at systemerne er tilstrækkeligt beskyttet. Samarbejdet mellem myndigheder og private finansielle institutioner bør fortsættes, når det er nødvendigt for at øge sikkerheden og modstandsdygtigheden i Unionens finansielle system.

I sin rapport fra 2020 om systemiske cyberrisici ([10]) identificerede ESRB hastighed, omfang og cybertruslers ondsindede hensigter som mulige kilder til udbredelse af systemiske risici. Myndighederne bør være opmærksomme på, at selv om FAIM'er udgør en ny kilde til udbredelse, forstærker de også eksisterende tidligere identificerede kilder, og bør integrere denne indsigt i deres politiske tiltag. I betragtning af alle de risici for den finansielle stabilitet, der følger af operationel eksponering for cyberrisici i den finansielle sektor, er det vigtigt at sikre, at de betænkeligheder, der er identificeret i denne advarsel, afspejles i det tilsyns- og tilsynsarbejde og de politiske holdninger, som de relevante myndigheder har vedtaget inden for deres respektive mandater.

De relevante myndigheder bør inden for deres respektive beføjelser og specifikt inden for den ramme, der er fastsat ved forordning (EU) 2022/2554, være opmærksomme på tre tidligere nævnte kilder til asymmetri, som FAIM'er har indført i den finansielle sektor. For at mindske disse asymmetrier bør samarbejdsordninger og sektorkoordinering overvejes sideløbende med eksisterende testrammer ([11]). De finansielle myndigheder bør også sikre, at de private finansielle institutioners bestyrelser er fast besluttet på at afbøde FAIM-drevne cyberrisici, at der er indført klare forvaltnings- og ansvarlighedsrammer, og at der planlægges rettidige reaktioner på passende vis sammen med tilsvarende interne investeringer.

Flere mulige udviklinger, der overvejes i denne advarsel — uanset om den systemiske indvirkning, den geopolitiske risiko eller den ændrede balance mellem angribere og forsvarere– har potentiale til at påvirke det finansielle systems funktion og tilliden hertil. For løbende at vurdere disse vil ESRB overveje behovet for at afspejle denne udvikling i risikovurderinger, testrammer og tilsynsmæssige forventninger samt i den fremtidige udvikling af scenarier. ESRB vil også overvåge anvendelsen og udviklingen af FAIM'er og deres indvirkning på den finansielle sektor ud fra et systemisk risikoperspektiv. Desuden vil ESRB revurdere udviklingen i hver kvartalsvis risikovurdering i Det Almindelige Råd og overveje andre foranstaltninger, når det er nødvendigt.

AFDELING 2

Definitioner

I denne advarsel gælder følgende definitioner:

1) »AI-udbyder«: en udbyder som defineret i artikel 3, nr. 3), i forordning (EU) 2024/1689

2) »banebrydende AI-modeller« (Frontier AI Models, FAIM'er): avancerede AI-modeller til almen brug, der i væsentlig grad kan påvirke offensive eller defensive cyberoperationer

3) »cyberangreb«: cyberangreb som defineret i artikel 1 i Rådets forordning (EU) 2019/796 ([12]), herunder når de har oprindelse i Unionen

4) »sårbarhed«: en sårbarhed som defineret i artikel 3, nr. 16), i forordning (EU) 2022/2554

5) »exploit«: et værktøj, en teknik eller en metode, der anvendes til at udnytte en eller flere sårbarheder til at opnå uautoriseret adgang til systemer, ændre dem eller afbryde dem eller på anden måde give anledning til IKT-risiko eller IKT-relaterede hændelser

6) »anvendelse som våben«: forberedelse eller tilpasning af exploits, der muliggør systematisk eller skalerbar udnyttelse af sårbarheder

7) »kritisk eller vigtig funktion«: en kritisk eller vigtig funktion som defineret i artikel 3, nr. 22), i forordning (EU) 2022/2554

8) »AI-model til almen brug«: en AI-model som defineret i artikel 3, nr. 63), i forordning (EU) 2024/1689

9) »AI-model til almen brug med systemisk risiko«: en AI-model til almen brug, der er klassificeret som en model, der udgør en systemisk risiko i overensstemmelse med artikel 51, stk. 1, i forordning (EU) 2024/1689

10) »IKT-relateret hændelse«: en hændelse som defineret i artikel 3, nr. 8), i forordning (EU) 2022/2554

([10]) Jf. »Systemic cyber risk«, ESRB, februar 2020, som findes på ESRB's websted www.esrb.europa.eu.

([11]) 10 F.eks. etiske red teams baseret på trusselsefterretninger (TIBER), trusselsbaserede penetrationstest (TLPT), avanceret red teaming (ART) og stresstest af cyberrobusthed (CyRST).

([12]) Rådets forordning (EU) 2019/796 af 17. maj 2019 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater (EUT L 129 I af 17.5.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11) »IKT-risiko«: en risiko som defineret i artikel 3, nr. 5), i forordning (EU) 2022/2554

12) »operationel modstandsdygtighed«: en digital operationel modstandsdygtighed som defineret i artikel 3, nr. 1), i forordning (EU) 2022/2554.

Udfærdiget i Frankfurt am Main, den 25. juni 2026.

På vegne af ESRB's Almindelige Råd

Francesco MAZZAFERRO

Leder af ESRB's sekretariat