C/2026/3795

16.7.2026

AVERTISMENTUL COMITETULUI EUROPEAN PENTRU RISC SISTEMIC

din 25 iunie 2026

privind riscurile cibernetice sistemice generate de modelele de inteligență artificială de frontieră

(CERS/2026/3)

(C/2026/3795)

CONSILIUL GENERAL AL COMITETULUI EUROPEAN PENTRU RISC SISTEMIC,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Acordul privind Spațiul Economic European ([1]), în special anexa IX,

având în vedere Regulamentul (UE) nr. 1092/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 privind supravegherea macroprudențială la nivelul Uniunii Europene a sistemului financiar și de înființare a unui Comitet european pentru risc sistemic ([2]), în special articolul 3 alineatul (2) litera (c) și articolele 16 și 18,

având în vedere Decizia CERS/2011/1 a Comitetului european pentru risc sistemic din 20 ianuarie 2011 de adoptare a Regulamentului de procedură al Comitetului european pentru risc sistemic ([3]), în special articolele 18-19,

întrucât:

(1) Principalii furnizori de inteligență artificială (IA) au dezvoltat modele de IA de frontieră (Frontier AI Models) (FAIM), care sunt foarte capabile în domeniul securității cibernetice și pot să efectueze atacuri cibernetice complet automatizate asupra unor sisteme complexe, inclusiv prin descoperirea vulnerabilităților și dezvoltarea și utilizarea ca armă a instrumentelor software de exploatare a vulnerabilităților, modificând astfel în mod fundamental peisajul amenințărilor cibernetice.

(2) FAIM sunt semnificativ mai bune decât modelele de IA anterioare în ceea ce privește găsirea de modalități de efectuare a atacurilor cibernetice, depășind modelele anterioare din punctul de vedere al costurilor, al vitezei și al preciziei, rivalizând în prezent cu principalii experți umani.

(3) FAIM au capacitatea de a amenința sistemele care stau la baza mediilor de tehnologie a informației și comunicațiilor (TIC) pe care se bazează infrastructura financiară, sporind probabilitatea și gravitatea incidentelor cibernetice cu impact sistemic.

(4) FAIM au demonstrat capacitatea de a descoperi vulnerabilități și de a proiecta instrumente software noi de exploatare a vulnerabilităților, expunând astfel principalele sisteme software și de operare utilizate în aproape toate mediile TIC ale organizațiilor riscului de atacuri cibernetice.

(5) Din punct de vedere istoric, descoperirea unor astfel de vulnerabilități a fost rară și adesea realizată de cercetători în domeniul securității, permițând remedierea specifică. În aceste cazuri, furnizorilor de software li se acordă adesea un interval de timp standardizat – de obicei 90 de zile – pentru a corecta vulnerabilitatea înainte ca aceasta să fie divulgată public. Cu toate acestea, este probabil ca FAIM să mărească volumul vulnerabilităților descoperite.

(6) Practicile actuale de corecție din sistemul financiar sunt predominant reactive, bazându-se pe actualizări periodice și pe răspunsuri ad-hoc la vulnerabilitățile divulgate. Această abordare funcționează într-un mediu al amenințărilor în care timpul permite ca descoperirea vulnerabilităților să rămână gestionabilă. Cu toate acestea, odată cu creșterea volumului vulnerabilităților, practicile actuale pot deveni insuficiente pentru a menține reziliența operațională.

(7) Această creștere a volumului expune, de asemenea, procesele actuale de corecție la supraîncărcare, deoarece acestea acordă prioritate măsurilor de remediere în funcție de risc și necesită testarea corecțiilor software înainte de implementare pentru a asigura stabilitatea operațională. În cazul în care sunt descoperite prea multe vulnerabilități cu impact de importanță critică într-un interval scurt de timp, astfel încât numărul de corecții software de importanță critică necesare crește substanțial, instituțiile financiare ar putea fi nevoite să decidă între a se expune unor riscuri cibernetice semnificative sau a reduce cerințele de testare a corecțiilor și, prin urmare, a risca incidente operaționale și întreruperi.

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

(8) Instrumentele software de exploatare a vulnerabilităților folosite ca armă erau dezvoltate în trecut în mare măsură manual și experții umani aveau nevoie de zile sau săptămâni pentru asta, în timp ce, în prezent, acest lucru poate fi realizat de FAIM în câteva minute sau ore. Acest lucru constituie un colaps al amortizoarelor de timp defensive, care sunt necesare pentru a menține continuitatea funcțiilor critice și importante în timpul remedierii.

(9) Odată cu proliferarea instrumentelor software de exploatare a vulnerabilităților folosite ca armă care reprezintă vulnerabilități critice dezvoltate de IA și cu reducerea corespunzătoare a amortizoarelor de timp defensive, riscul pentru funcțiile și instituțiile individuale importante sau de importanță critică crește brusc. Dacă astfel de riscuri se materializează simultan la nivelul acelor funcții și instituții, acest lucru ar putea duce la o creștere permanentă a riscului cibernetic sistemic pentru care, în prezent, nu există un cadru de soluționare pe deplin eficace. Din cauza gradului ridicat de interconectare din cadrul sectorului financiar al Uniunii, precum și dintre acest sector și alte sectoare și jurisdicții, această situație prezintă un risc sistematic și are potențialul de a crea fragilități sistemice.

(10) În plus, FAIM sunt în prezent elaborate doar de către un număr mic de furnizori de IA, dintre care mai mulți și-au exprimat îngrijorarea cu privire la faptul că viitoarele FAIM ar putea fi prea puternice pentru accesul nerestricționat al publicului.

(11) IA este deja utilizată de actori răuvoitori pentru a intensifica atacurile cibernetice. Este probabil ca astfel de actori să obțină în cele din urmă, fie prin scurgeri, furt, dezvoltare independentă sau acces liber, modele de IA cu capacități comparabile cu cele utilizate în prezent în contexte defensive controlate.

(12) Deși FAIM pot spori în mod semnificativ capabilitățile ofensive și probabilitatea unor atacuri cibernetice sofisticate, acestea vor consolida și capabilitățile defensive, în special în ceea ce privește descoperirea vulnerabilităților, corelarea datelor și acțiunile de remediere întreprinse de instituțiile individuale. Cu toate acestea, pe termen scurt și mediu, este probabil ca creșterea vitezei, a amplorii și a preciziei capacităților ofensive să depășească beneficiile.

(13) Dezvoltarea rapidă a FAIM face necesară abordarea fără întârziere a riscurilor identificate la adresa stabilității financiare, astfel încât să se prevină materializarea acestora sau cel puțin să se atenueze impactul lor potențial. Pentru a asigura stabilitatea financiară pe piețele financiare ale Uniunii, toți membrii Comitetului european pentru risc sistemic (CERS) ar trebui să ia în considerare implicațiile FAIM asupra capacității operaționale și a rezilienței instituțiilor financiare în contextul măsurilor lor de politică macroprudențială și microprudențială. Aceasta nu aduce atingere mandatelor de politică monetară ale băncilor centrale din uniunea Europeană. De exemplu, printre alte inițiative actuale ale autorităților, BCE, în rolul său de supraveghetor bancar, a solicitat instituțiilor semnificative să evalueze fără întârziere impactul cadrului general de amenințări aflat în dezvoltare, și să dezvolte până la 31 octombrie 2026 un plan cuprinzător de acțiuni care să prezinte măsuri concrete menite să abordeze astfel de riscuri ([4]).

(14) Pe măsură ce tehnologia IA proliferează, este important să se asigure că toate infrastructurile de importanță critică și, în special, instituțiile financiare sunt pregătite să facă față atacurilor cibernetice alimentate de FAIM și să facă pregătiri adecvate și în timp util. Cu toate acestea, astfel de eforturi defensive ale entităților individuale ar fi insuficiente. Un răspuns eficace și atenuarea riscurilor necesită un răspuns coordonat care să implice toate părțile afectate, inclusiv furnizorii de IA, furnizorii de software, firmele de securitate, furnizorii de mentenanță cu sursă deschisă, instituțiile financiare și autoritățile, atât la nivel național, cât și la nivelul Uniunii.

(15) Atunci când se abordează aspectele de mai sus, este important să se aibă în vedere cadrele juridice și de politică relevante ale Uniunii, în special Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului ([5]), Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului ([6]), Regulamentul(UE) nr. 2024/2847 al Parlamentului European și al Consiliului ([7]) și Recomandarea Comitetului european pentru risc sistemic (CERS/2021/17) ([8]).

([4]) Scrisoarea adresată instituțiilor semnificative este disponibilă pe website-ulș de supraveghere bancară al BCE la adresa www.bankingsupervision.europa.eu.

([5]) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentelor (UE) nr. 168/2013 și (UE) 2019/1020, precum și a Directivei (UE) 2020/1828 (Regulamentul privind reziliența cibernetică) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Recomandarea Comitetului European Pentru risc Sistemic din 2 decembrie 2021 privind un cadru paneuropean de coordonare sistemică a incidentelor cibernetice pentru autoritățile relevante (CERS/2021/17) (JO C 134, 25.3.2022, p. 1).

(16) Regulamentul (UE) 2022/2554 oferă un cadru cuprinzător pentru ca instituțiile financiare să identifice, să gestioneze, să monitorizeze și să atenueze riscurile TIC, inclusiv riscurile generate de atacurile cibernetice. Având în vedere interconectarea sectorului financiar și dependența sa de sistemele TIC și de furnizorii terți de servicii, un atac cibernetic reușit care ar afecta una sau mai multe instituții financiare sau furnizorii lor de servicii critice ar putea avea implicații sistemice semnificative. Autoritățile de supraveghere financiară ar trebui să dea prioritatea adecvată activităților de supraveghere din acest domeniu, având în vedere impactul potențial al unor astfel de atacuri cibernetice asupra stabilității, integrității și credibilității sistemului financiar, precum și daunele operaționale, financiare și pierderile suferite de consumator care ar putea rezulta.

(17) Regulamentul (UE) 2024/1689 stabilește norme armonizate privind introducerea pe piață, punerea în serviciu și utilizarea sistemelor de IA și a modelelor de IA de uz general în Uniunea Europeană, inclusiv, în anumite circumstanțe, a sistemelor și modelelor furnizate de furnizori de IA stabiliți în țări terțe, atunci când producția generată de sistemul de IA este utilizată în Uniunea Europeană sau un model de IA este integrat într-un sistem introdus pe piața Uniunii Europene. Acest regulament prevede, de asemenea, norme specifice, inclusiv un regim de reglementare mai strict, pentru modelele clasificate ca modele de IA de uz general care prezintă risc sistemic.

(18) Regulamentul (UE) 2024/2847 introduce cerințe obligatorii de securitate cibernetică pentru producători, care acoperă planificarea, proiectarea, dezvoltarea și mentenanța produselor hardware și software cu elemente digitale plasate pe piața Uniunii Europene. Acesta prevede și ca producătorii să se ocupe de vulnerabilități pe durata de viață a produselor acestora. Odată ce va fi pe deplin aplicabil în decembrie 2027, entitățile financiare care plasează astfel de produse pe piața Uniunii Europene vor trebui, de asemenea, să se asigure că aceste produse respectă aceste cerințe.

(19) Recomandarea CERS/2021/17 a recomandat elaborarea, de către Autoritățile europene de supraveghere (AES) în comun prin Comitetul comun al autorităților europene de supraveghere și împreună cu Banca Centrală Europeană (BCE), Comitetul european pentru risc sistemic (CERS) și autoritățile naționale relevante, a unui răspuns eficient coordonat la nivelul Uniunii în cazul unui incident cibernetic transfrontalier major sau al unei amenințări aferente care ar putea avea un impact sistemic asupra sectorului financiar al Uniunii. Acest lucru a dus la înființarea Cadrului paneuropean de coordonare a incidentelor cibernetice sistemice (EU-SCICF), care oferă o platformă valoroasă și operațională pentru schimbul de informații și coordonare între autoritățile financiare.

(20) În acest context, Comitetul european pentru risc sistemic adoptă pe această cale un avertisment de natură generală care vizează riscurile semnificative pentru stabilitatea financiară, amplificate de evoluția FAIM. Avertismentul ia în considerare activitatea analitică din nota CERS: „Abordarea modelelor de IA de frontieră cu capabilități cibernetice din perspectiva stabilității financiare” publicată în iunie 2026 ([9]),

ADOPTĂ PREZENTUL AVERTISMENT:

SECȚIUNEA 1

Avertisment

Noul cadru de risc

Dezvoltarea rapidă a modelelor de IA de frontieră (FAIM) cu capabilitate cibernetică aduce schimbări semnificative în cadrul riscurilor pentru sistemul financiar al Uniunii. Datele actuale indică faptul că FAIM sunt capabile să descopere vulnerabilități, să genereze instrumente software funcționale de exploatare a vulnerabilităților și să execute autonom atacuri cibernetice de mare amploare la o viteză, scară și nivel de acuratețe care depășesc cu mult modelele de IA anterioare. Aceasta reprezintă o schimbare de paradigmă în domeniul securității cibernetice și un punct de inflexiune în ceea ce privește capacitatea IA.

CERS consideră aceste evoluții ca fiind o sursă de riscuri sistemice pentru sistemul financiar, cu potențialul de a genera efecte adverse semnificative asupra securității cibernetice prin descoperirea accelerată a vulnerabilităților, reducerea timpului disponibil pentru răspuns și apărare eficientă, creșterea amplitudinii și complexității atacurilor cibernetice și introducerea unor noi dependențe și riscuri de concentrare în cadrul sistemului financiar. Deși CERS recunoaște că FAIM consolidează capacitățile defensive ale instituțiilor financiare, aceste capacități sunt susceptibile să se materializeze treptat în următorii câțiva ani, necesitând ca instituțiile financiare să funcționeze pe durata unei perioade de tranziție caracterizate de risc ridicat, incertitudine accentuată și un cadru tehnologic în continuă evoluție. Având în vedere natura extrem de digitalizată și interconectată a sistemului financiar, astfel de efecte nefavorabile asupra securității cibernetice s-ar putea propaga rapid, afectând funcții critice și importante din cadrul instituțiilor financiare, conducând în cele din urmă la perturbare sistemică și pierderea încrederii în sistemul financiar.

([9]) Disponibilă pe website-ul CERS, la adresa www.esrb.europa.eu.

FAIM-urile emergente majorează riscul asociat TIC, ducând la slăbirea rezilienței operaționale în sectorul financiar, în special în patru domenii: (a) timpul, inclusiv capacitatea de a remedia rapid sisteme complexe fără a cauza nefuncționalități operaționale, ținând cont de reducerea radicală a amortizoarelor de timp defensive dintre descoperirea vulnerabilității și folosirea instrumentelor software de exploatare a vulnerabilităților ca armă; (b) capacitatea apărătorilor, inclusiv abilitatea acestora de a efectua testare de securitate automată și manuală asistată de FAIM, precum și capacitatea lor de a proteja, detecta și răspunde la amenințările provenite din utilizarea adversă a FAIM; (c) concentrarea, incluzând dependențele de un număr limitat de furnizori de IA, dependenți la rândul lor de furnizori de servicii cloud, componente open source și alte programe software utilizate pe scară largă; și (d) capacitatea autorităților, inclusiv calibrarea așteptărilor, testarea la stres și măsurile de pregătire în conformitate cu evoluția FAIM, astfel încât situațiile de dificultate operațională să nu devină o sursă de instabilitate mai largă.

Mai mult, stabilirea și menținerea vizibilității implementării IA în cadrul oricărei instituții financiare – inclusiv înțelegerea pe deplin a locului și modului în care este implementată IA – este o provocare, având în vedere că aceasta este utilizată în interfețele cu clienții, la agenți interni, în procesele de afaceri și în integrarea cu terți.

Evaluarea sistemică

Evoluțiile identificate pot modifica semnificativ atât amploarea, cât și structura riscului cibernetic, majorând atât riscurile directe, cât și pe cele indirecte pentru stabilitatea financiară. Capabilitățile FAIM pot supune cadrele existente de reziliență unei presiuni substanțiale, mai ales dacă incidentele sunt răspândite și au loc simultan. Incidentele se pot propaga rapid și în rândul instituțiilor financiare și al piețelor dacă sunt afectați furnizori terți de servicii de importantă critică, ecosisteme tehnologice comune sau componente open source utilizate pe scară largă, majorând riscul unor perturbări conexe cu implicații sistemice.

FAIM modifică trei surse de asimetrie în sectorul financiar: prima între jurisdicții, a doua între apărători și atacatori, iar a treia între instituțiile financiare mai bine finanțate și cele mai puțin bine echipate.

În primul rând, actuala concentrare geografică a principalilor furnizori de IA în afara Uniunii Europene lasă Uniunea Europeană expusă la riscuri geopolitice și de dependență strategică. Pentru a diminua asimetria de cunoștințe și tehnologică dintre jurisdicții, este necesară adoptarea unor măsuri care să faciliteze accesul adecvat și proporțional al Uniunii Europene și al statelor sale membre la FAIM-urile nou dezvoltate. Astfel de măsuri ar trebui să fie luate în timp util, coerente și eficiente, atât din punct de vedere al politicilor, cât și al punerii în aplicare, și să țină cont în mod adecvat de diferitele sectoare financiare ale Uniunii, beneficiind de expertiza Autorităților europene de supraveghere corespunzătoare. Aceasta va atenua nu doar o asimetrie între Uniune și jurisdicțiile din țări terțe, ci și între instituțiile financiare stabilite în diferite state membre, menținând condiții de concurență echitabile în interiorul și în afara Uniunii și minimizând riscul sistemic. Aranjamentele care facilitează accesul la FAIM doar pentru anumite categorii de instituții sau în jurisdicții selectate ar contribui la fragmentarea pieței unice financiare, reducând lichiditatea și profunzimea acesteia.

În al doilea rând, în ceea ce privește asimetria dintre atacatori și apărători, FAIM-urile reduc prețul de intrare pentru atacatori. Actorii amenințărilor vor tinde să se bazeze din ce în ce mai mult pe FAIM pentru a derula părțile mai avansate tehnic și care necesită mai multă muncă ale operațiunilor ofensive, reducând costurile. Apărătorii, prin contrast, sunt constrânși de cerințe operaționale, dependențe și obligații de reglementare, limitând efectul și amploarea la care pot beneficia de FAIM-uri pe termen scurt și mediu, necesitând în cele din urmă perioade mai lungi pentru a se ajusta.

În al treilea rând, există diferențe în modul în care instituțiile financiare sunt finanțate și echipate pentru a face față provocărilor generate de FAIM. Aceste diferențe pot fi generate de costuri care sunt fixe, mai degrabă decât graduale, de constrângeri de resurse și de accesul limitat la specialiști. Atunci când există o asimetrie în capacitatea de a face față unor astfel de provocări, cea mai slabă legătură a lanțului poate afecta stabilitatea sistemului.

Implicații

Este esențial să se asigure că sistemele de plată și decontare de importanță sistemică și infrastructurile pieței financiare rămân protejate împotriva vulnerabilităților care apar din utilizarea și evoluția FAIM. Operatorii publici și privați ar trebui să-și revizuiască atent și să-și actualizeze cadrele de securitate cibernetică pentru a lua în considerare astfel de vulnerabilități. Autoritățile responsabile cu supravegherea sau monitorizarea ar trebui să adopte măsuri pentru a se asigura că sistemele sunt protejate în mod adecvat. Cooperarea între autorități și instituțiile financiare private ar trebui urmărită ori de câte ori este necesar pentru a crește securitatea și reziliența sistemului financiar al Uniunii.

În raportul său din 2020 privind riscul cibernetic sistemic ([10]), Comitetul european pentru risc sistemic a identificat viteza, amploarea și intențiile negative ale amenințărilor cibernetice ca posibile surse de propagare a riscului sistemic. Autoritățile ar trebui să fie conștiente că, în timp ce FAIM-urile reprezintă o nouă sursă de propagare, acestea și amplifică sursele actuale care au fost identificate în trecut, și ar trebui să integreze această perspectivă în măsurile lor de politică. Având în vedere toate riscurile pentru stabilitatea financiară care decurg din expunerea operațională la riscul cibernetic în sectorul financiar, este important ca preocupările identificate în acest avertisment să fie reflectate în activitățile de supraveghere și monitorizare, precum și în orientările de politică adoptate de autoritățile relevante, în cadrul mandatelor lor respective.

Autoritățile relevante, în limitele competențelor lor și în cadrul stabilit de Regulamentul (UE) 2022/2554, ar trebui să cunoască cele 3 surse de asimetrie introduse de FAIM în sectorul financiar, care au fost menționate anterior. Pentru a reduce aceste asimetrii, ar trebui avute în vedere mecanisme de cooperare și coordonarea sectorială, împreună cu cadrele actuale de testare ([11]) Autoritățile financiare ar trebui să se asigure că organele de conducere ale instituțiilor financiare sunt complet angajate în atenuarea riscurilor cibernetice generate de FAIM, că există cadre de guvernanță și răspundere și că răspunsurile în timp util sunt planificate adecvat, împreună cu implicarea internă corespunzătoare.

Mai multe evoluții posibile avute în vedere în acest avertisment – fie impactul sistemic, riscul geopolitic sau schimbarea echilibrului dintre atacatori și apărători – au potențialul de a afecta funcționarea sistemului financiar și încrederea în acesta. Pentru a evalua continuu aceste aspecte, Comitetul european pentru risc sistemic va lua în considerare necesitatea reflectării acestor evoluții în evaluările riscurilor, cadrele de testare și așteptările în materie de supraveghere, precum și în dezvoltarea de scenarii în viitor. Comitetul european pentru risc sistemic va monitoriza, de asemenea, utilizarea și evoluția FAIM-urilor și impactul acestora asupra sectorului financiar din perspectiva riscului sistemic. În plus, Comitetul european pentru risc sistemic va reevalua evoluțiile în cadrul fiecărei evaluări trimestriale a riscurilor la nivelul Consiliului general și va lua în considerare alte acțiuni atunci când este necesar.

SECȚIUNEA 2

Definiții

În sensul prezentului avertisment, se aplică următoarele definiții:

1. „furnizor de IA” înseamnă un furnizor astfel cum este definit la articolul 3 punctul (3) din Regulamentul (UE) 2024/1689;

2. „Modele IA de frontieră” (FAIM) înseamnă modele avansate de IA de uz general capabile să afecteze semnificativ operațiuni cibernetice ofensive sau defensive;

3. „atac cibernetic” înseamnă un atac cibernetic astfel cum este definit la articolul 1 din Regulamentul (UE) 2019/796 al Consiliului ([12]), inclusiv atunci când își are originea înăuntrul Uniunii;

4. „vulnerabilitate” înseamnă o vulnerabilitate astfel cum este definită la articolul 3 punctul (16) din Regulamentul (UE) 2022/2554;

5. „instrumente software de exploatare a vulnerabilităților” înseamnă un instrument, o tehnică sau o metodă utilizată pentru a profita de una sau mai multe vulnerabilități pentru a dobândi acces neautorizat la sisteme, pentru a le modifica sau pentru a le crea întreruperi de funcționare, sau pentru a genera riscuri TIC sau incidente legate de TIC;

6. „folosirea ca armă” înseamnă pregătirea sau adaptarea instrumentelor software de exploatare a vulnerabilităților care să permită exploatarea sistematică sau graduală a vulnerabilităților;

7. „funcție importantă sau de importanță critică” înseamnă o funcție critică sau importantă astfel cum este definită la articolul 3 punctul (22) din Regulamentul (UE) 2022/2554;

8. „model de IA de uz general” înseamnă un furnizor astfel cum este definit la articolul 3 punctul (63) din Regulamentul (UE) 2024/1689;

9. „model de IA de uz general care prezintă risc sistemic” înseamnă un model de IA de uz general clasificat ca prezentând risc sistemic astfel cum este definit la articolul 51 punctul (1) din Regulamentul (UE) 2024/1689;

10. „Incident legat de TIC” înseamnă un incident astfel cum este definit la articolul 3 punctul (8) din Regulamentul (UE) 2022/2554;

([10]) A se vedea „Systemic cyber risk” (Riscul cibernetic sistemic), CERS, februarie 2020, disponibil pe website-ul CERS la adresawww.esrb.europa.eu.

([11]) De ex. cadrul pentru atacurile etice bazate pe informații operative privind amenințările (TIBER), teste de penetrare bazate pe amenințări (TLPT), atacurile etice avansate (ART) și testările la stres privind reziliența cibernetică (CyRST).

([12]) Regulamentul (UE) 2019/796 al Consiliului din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre (JO L 129 I, 17.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11. „risc TIC” înseamnă un risc astfel cum este definit la articolul 3 punctul (5) din Regulamentul (UE) 2022/2554;

12. „reziliență operațională” înseamnă reziliență operațională digitală astfel cum este definită la articolul 3 punctul (1) din Regulamentul (UE) 2022/2554;

Adoptat la Frankfurt pe Main, 25 iunie 2026.

Șeful secretariatului CERS,
în numele Consiliului general al CERS,
Francesco MAZZAFERRO