C/2026/3795

16.7.2026.

UPOZORENJE EUROPSKOG ODBORA ZA SISTEMSKE RIZIKE

od 25. lipnja 2026.

o sistemskim kibernetičkim rizicima koji proizlaze iz naprednih modela umjetne inteligencije

(ESRB/2026/3)

(C/2026/3795)

OPĆI ODBOR EUROPSKOG ODBORA ZA SISTEMSKE RIZIKE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Sporazum o Europskom gospodarskom prostoru ([1]), a posebno njegov Prilog IX.,

uzimajući u obzir Uredbu (EU) br. 1092/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o makrobonitetnom nadzoru financijskog sustava Europske unije i osnivanju Europskog odbora za sistemske rizike ([2]), a osobito njezin članak 3. stavak 2. točku (c), te članke 16. i 18.,

uzimajući u obzir Odluku ESRB/2011/1 Europskog odbora za sistemske rizike od 20. siječnja 2011. o donošenju Poslovnika Europskog odbora za sistemske rizike ([3]), a posebno njezine članke 18. i 19.,

budući da:

(1) Vodeći dobavljači umjetne inteligencije (UI) razvili su napredne UI modele (engl. *Frontier AI Models*, FAIM), koji su vrlo sposobni u području kibersigurnosti i mogu provoditi potpuno automatizirane kibernapade na složene sustave, uključujući otkrivanjem ranjivosti te razvojem i osposobljavanjem eksploita za izvođenje napada, čime se iz temelja mijenja okruženje kiberprijetnji.

(2) FAIM-ovi su znatno bolji od ranijih modela umjetne inteligencije u pronalaženju načina za izvođenje kibernapada jer imaju bolje rezultate od ranijih modela u pogledu troškova, brzine i točnosti te su sada u konkurenciji s vodećim ljudskim stručnjacima.

(3) FAIM-ovi mogu ugroziti sustave na kojima se temelje okruženja informacijske i komunikacijske tehnologije (IKT) o kojima ovisi financijska infrastruktura, čime se povećavaju vjerojatnost i ozbiljnost kiberincidenata sa sistemskim učinkom.

(4) FAIM-ovi su pokazali sposobnost otkrivanja ranjivosti i stvaranja novih eksploita, čime su veliki operativni sustavi i softver koji se upotrebljavaju u gotovo svim IKT okruženjima organizacija izloženi riziku od kibernapada.

(5) U prošlosti su otkrića takvih ranjivosti bila rijetka i često su ih otkrivali istraživači u području sigurnosti, što je omogućilo ciljano uklanjanje ranjivosti. U tim slučajevima dobavljačima softvera često se daje standardizirani vremenski okvir – obično 90 dana – za uklanjanje ranjivosti prije njezina javnog otkrivanja. Međutim, FAIM-ovi će vjerojatno povećati broj utvrđenih ranjivosti.

(6) Trenutačne prakse zakrpa u financijskom sustavu uglavnom su reaktivne i oslanjaju se na periodična ažuriranja i *ad hoc* odgovore na otkrivene ranjivosti. Taj pristup funkcionira u okruženju prijetnji u kojem vrijeme omogućuje da se otkrića ranjivosti i dalje mogu kontrolirati. Međutim, s povećanjem broja ranjivosti postojeće prakse mogle bi postati nedovoljne za održavanje operativne otpornosti.

(7) To povećanje broja izlaže i trenutačne postupke zakrpa preopterećenju jer se njima prednost daje korektivnim mjerama na temelju rizika i zahtijeva testiranje softverskih zakrpa prije provedbe kako bi se osigurala operativna stabilnost. Ako se u kratkom roku otkrije previše ranjivosti s kritičnim učinkom kako bi se znatno povećao broj potrebnih kritičnih zakrpa softvera, financijske institucije možda će morati odlučiti hoće li ostati izložene znatnim kibernetičkim rizicima ili smanjiti zahtjeve za testiranje zakrpa, čime se riskiraju operativni incidenti i prekid rada.

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

(8) Osposobljavanje eksploita za izvođenje napada prethodno je u velikoj mjeri bilo ručna i za to su ljudskim stručnjacima bili potrebni dani ili tjedni, dok FAIM-ovi sada to mogu učiniti u roku od nekoliko minuta ili sati. To predstavlja slom zaštitnih vremenskih rezervi, koje su potrebne za održavanje kontinuiteta ključnih i važnih funkcija tijekom uklanjanja ranjivosti.

(9) Zbog sve većeg broja eksploita za izvođenje napada koji odgovaraju kritičnim ranjivostima koje UI koristi za izvođenje napada i s time povezanog smanjenja zaštitnih vremenskih rezervi, rizik za pojedinačne ključne ili važne funkcije i institucije naglo se povećava. Ako se takvi rizici istodobno realiziraju u tim funkcijama i institucijama, to bi moglo dovesti do trajnog povećanja sistemskog kibernetičkog rizika za koji trenutačno ne postoji potpuno učinkovit okvir za ublažavanje. Zbog snažne međusobne povezanosti unutar financijskog sektora Unije, kao i između tog sektora i drugih sektora i jurisdikcija, ova situacija predstavlja sustavan rizik i može stvoriti sistemske slabosti.

(10) Nadalje, FAIM-ove trenutačno razvija samo mali broj dobavljača UI-ja, od kojih je nekoliko izrazilo zabrinutost da bi budući FAIM-ovi mogli biti previše moćni za neograničen javni pristup.

(11) Zlonamjerni akteri već upotrebljavaju UI za jačanje kibernapada. Vjerojatno je da će takvi akteri u konačnici steći, bilo curenjem informacija, krađom, neovisnim razvojem ili otvorenim pristupom, UI modele sa sposobnostima usporedivima s onima koje se trenutačno upotrebljavaju u kontroliranim obrambenim okruženjima.

(12) Iako FAIM-ovi mogu znatno povećati napadačke sposobnosti i vjerojatnost sofisticiranih kibernapada, ojačat će i obrambene sposobnosti, posebno u pogledu otkrivanja ranjivosti, podatkovne korelacije i korektivnih mjera pojedinačnih institucija. Međutim, kratkoročno do srednjoročno povećanje brzine, razmjera i točnosti napadačkih sposobnosti vjerojatno će nadmašiti koristi.

(13) Zbog brzog razvoja FAIM-ova potrebno je bez odgode ukloniti utvrđene rizike za financijsku stabilnost kako bi se spriječila njihova realizacija ili barem ublažio njihov mogući učinak. Kako bi se osigurala financijska stabilnost financijskih tržišta Unije, svi članovi Europskog odbora za sistemske rizike (ESRB) trebali bi razmotriti implikacije FAIM-ova na operativnu sposobnost i otpornost financijskih institucija u kontekstu njihovih mjera makrobonitetne i mikrobonitetne politike. Ovo je bez utjecaja na ovlasti u području monetarne politike središnjih banaka u Uniji. Primjerice, među trenutačnim inicijativama drugih tijela, ESB je u svojoj ulozi nadzornog tijela za bankarstvo zatražio od značajnih institucija da bez odgađanja procijene učinak promjenjivog okruženja prijetnje te da do 31. listopada 2026. izrade sveobuhvatan akcijski plan u kojem će navesti konkretne mjere usmjerene na otklanjanje tih rizika ([4]).

(14) Budući da se tehnologija Ui-ja sve više širi, važno je osigurati da sva kritična infrastruktura, a posebno financijske institucije, budu spremne suočiti se s kibernapadima koje pokreću FAIM-ovi te provesti pravodobne i odgovarajuće pripreme. Međutim, takvi obrambeni napori pojedinačnih subjekata ne bi bili dovoljni. Za učinkovit odgovor i ublažavanje rizika potreban je koordinirani odgovor u kojem sudjeluju sve zahvaćene strane, uključujući dobavljače UI-ja, dobavljače softvera, zaštitarska društva, održavatelje otvorenog koda, financijske institucije i tijela na nacionalnoj razini i razini Unije.

(15) Pri rješavanju navedenih pitanja važno je podsjetiti na relevantne pravne okvire i okvire politike Unije, posebno na Uredbu (EU) 2022/2554 Europskog parlamenta i Vijeća ([5]), Uredbu (EU) 2024/1689 Europskog parlamenta i Vijeća ([6]), Uredbu (EU) 2024/2847 Europskog parlamenta i Vijeća ([7]) i Preporuku Europskog odbora za sistemske rizike (ESRB/2021/17) ([8]).

([4]) Dopis upućen značajnim institucijama dostupan je na mrežnim stranicama ESB-a o nadzoru banaka.

([5]) Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (SL L 333, 27.12.2022., str. 1., ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, 2024/1689, 12.7.2024., ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Uredba (EU) 2024/2847 Europskog parlamenta i Vijeća od 23. listopada 2024. o horizontalnim zahtjevima u pogledu kibernetičke sigurnosti za proizvode s digitalnim elementima i o izmjeni uredbi (EU) br. 168/2013 i (EU) 2019/1020 te Direktive (EU) 2020/1828 (Akt o kibernetičkoj otpornosti) (SL L, 2024/2847, 20.11.2024., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Preporuka Europskog odbora za sistemske rizike od 2. prosinca 2021. o paneuropskom okviru za sistemsku koordinaciju kiberincidenata za relevantna tijela (ESRB/2021/17) (SL C 134, 25.3.2022., str. 1.).

(16) Uredba (EU) 2022/2554 pruža sveobuhvatan okvir financijskim institucijama za utvrđivanje, upravljanje, praćenje i ublažavanje IKT rizika, uključujući rizike koji proizlaze iz kibernapada. S obzirom na međusobnu povezanost financijskog sektora i njegovo oslanjanje na IKT sustave i treće strane pružatelje usluga, uspješan kibernapad koji utječe na jednu ili više financijskih institucija ili njihove pružatelje ključnih usluga mogao bi imati znatne sistemske implikacije. Financijska nadzorna tijela trebala bi dati odgovarajuću prednost nadzornim aktivnostima u tom području, uzimajući u obzir mogući utjecaj takvih kibernapada na stabilnost, integritet i pouzdanost financijskog sustava, kao i operativnu i financijsku štetu te štetu za potrošače koja može nastati.

(17) Uredbom (EU) 2024/1689 utvrđuju se usklađena pravila za stavljanje na tržište, stavljanje u uporabu i korištenje UI sustava i UI modela opće namjene u Uniji, uključujući, u određenim okolnostima, sustave i modele koje isporučuju dobavljači UI-ja sustava s poslovnim nastanom u trećim zemljama ako se izlazni rezultati UI sustava upotrebljavaju u Uniji ili je UI model integriran u sustav stavljen na tržište Unije. Ovom se Uredbom utvrđuju i posebna pravila, uključujući stroži regulatorni režim, za modele klasificirane kao UI modeli opće namjene sa sistemskim rizikom.

(18) Uredbom (EU) 2024/2847 uvode se obvezni zahtjevi u pogledu kibernetičke sigurnosti za proizvođače koji obuhvaćaju planiranje, projektiranje, razvoj i održavanje hardverskih i softverskih proizvoda s digitalnim elementima koji se stavljaju na tržište Unije. Od proizvođača se zahtijeva i da se nose s ranjivostima tijekom životnog ciklusa svojih proizvoda. Nakon što se u potpunosti počnu primjenjivati u prosincu 2027., financijski subjekti koji takve proizvode stavljaju na tržište Unije morat će osigurati i usklađenost tih proizvoda s ovim zahtjevima.

(19) U Preporuci ESRB/2021/17 preporučuje se da europska nadzorna tijela, zajednički u okviru Zajedničkog odbora i zajedno s Europskom središnjom bankom (ESB), ESRB-om i odgovarajućim nacionalnim tijelima, razviju učinkovit odgovor koordiniran na razini Unije u slučaju velikog prekograničnog kiberincidenta ili povezane prijetnje koji bi mogli imati sistemski učinak na financijski sektor Unije. To je dovelo do uspostave paneuropskog okvira za sistemsku koordinaciju kiberincidenata (EU-SCICF), koji pruža vrijednu i operativnu platformu za razmjenu informacija i koordinaciju među financijskim tijelima.

(20) U tom kontekstu, ESRB ovime donosi opće upozorenje, kojim se upozorava na znatne rizike za financijsku stabilnost, a koji su dodatno pojačani razvojem FAIM-ova. U upozorenju se uzima u obzir analitički rad iz napomene ESRB-a *Addressing Frontier AI Models with cyber capabilities from a financial stability perspective* („Razmatranje naprednih UI modela s kibernetičkim sposobnostima iz perspektive financijske stabilnosti”), objavljene u lipnju 2026. ([9]),

DONIO JE OVO UPOZORENJE:

ODJELJAK 1.

Upozorenje

Novo okruženje rizika

Brzi razvoj naprednih UI modela (engl. *Frontier AI Models*, FAIM) s kiberkapacitetom donosi bitne promjene u rizičnom okruženju za financijski sustav Unije. Trenutačni dokazi upućuju na to da FAIM-ovi mogu otkrivati ranjivosti, stvarati funkcionalne eksploite i samostalno izvršavati kibernapade velikih razmjera brzinom, razmjerom i razinom točnosti koja znatno premašuje prethodne UI modele. To predstavlja promjenu paradigme u području kibersigurnosti i prekretnicu u pogledu sposobnosti UI-ja.

ESRB smatra da su ta kretanja izvor sistemskih rizika za financijski sustav, s mogućnošću stvaranja znatnih negativnih učinaka na kibersigurnost ubrzanim otkrivanjem ranjivosti, skraćivanjem vremena raspoloživog za odgovor i učinkovitu obranu, povećanim razmjerom i sofisticiranošću kibernapada te uvođenjem novih ovisnosti i koncentracijskih rizika unutar financijskog sustava. Iako ESRB uvažava pojačane obrambene sposobnosti koje će FAIM-ovi nuditi financijskim institucijama, te će se sposobnosti vjerojatno postupno realizirati tijekom sljedećih nekoliko godina, zbog čega će financijske institucije morati poslovati u prijelaznom razdoblju obilježenom povećanim rizikom, velikom nesigurnošću i tehnološkim okruženjem koje se brzo mijenja. S obzirom na izrazito digitaliziranu i međusobno povezanu prirodu financijskog sustava, takvi negativni učinci na kibersigurnost mogli bi se brzo proširiti te utjecati na ključne i važne funkcije u financijskim institucijama, što bi u konačnici dovelo do sistemskih poremećaja i gubitka povjerenja u financijski sustav.

([9]) Dostupno na mrežnim stranicama ESRB-a na www.esrb.europa.eu.

FAIM-ovi u nastajanju povećavaju inherentni IKT rizik, što dovodi do oslabljene operativne otpornosti u cijelom financijskom sektoru, posebno u četiri područja: (a) vrijeme, uključujući sposobnost brzih zakrpa složenih sustava bez uzrokovanja operativnog prekida, uzimajući u obzir slom zaštitnih vremenskih rezervi između otkrivanja ranjivosti i osposobljavanjem eksploita za izvođenje napada; (b) sposobnost stručnjaka za kibernetičku sigurnost, uključujući njihovu sposobnost provođenja automatiziranog i ručnog sigurnosnog testiranja uz pomoć FAIM-ova, kao i njihovu sposobnost da zaštite, otkriju i odgovore na prijetnje koje proizlaze iz zlonamjerne uporabe FAIM-ova; (c) koncentracija, uključujući ovisnost o ograničenom broju dobavljača UI-ja, koji su pak ovisni o pružateljima usluga u oblaku, komponentama otvorenog koda i drugom široko korištenom softveru; te (d) sposobnost nadležnih tijela, uključujući njihovu kalibraciju očekivanja, testiranja otpornosti na stres i mjera pripravnosti u skladu s razvojem FAIM-ova, kako operativni prekidi ne bi postali izvor šire nestabilnosti.

Nadalje, uspostava i održavanje vidljivosti uvođenja UI-ja u bilo kojoj financijskoj instituciji – uključujući potpuno razumijevanje gdje i kako se UI uvodi – izazovno je s obzirom na to da se upotrebljava u sučeljima za korisnike, internim agentima, poslovnim procesima i integraciji s trećim stranama.

Sustavna procjena

Utvrđena kretanja mogu bitno promijeniti razmjer i strukturu kiberrizika, čime se povećavaju i izravni i neizravni rizici za financijsku stabilnost. Sposobnosti FAIM-a mogu izložiti postojeće okvire za otpornost znatnom pritisku, posebno ako su incidenti raširenii i događaju se istodobno. Incidenti se mogu brzo širiti i među financijskim institucijama i tržištima ako to utječe na ključne treće strane pružatelje usluga, zajedničke tehnološke ekosustave ili široko korištene komponente otvorenog koda, čime se povećava rizik od povezanih poremećaja sa sistemskim implikacijama.

FAIM-ovi mijenjaju tri izvora asimetrije u financijskom sektoru: prvi između jurisdikcija, drugi između stručnjaka za kibernetičku sigurnost i napadača, a treći između financijskih institucija s boljim resursima i slabije opremljenih financijskih institucija.

Prvo, zbog trenutačne geografske koncentracije vodećih dobavljača UI-ja izvan Unije, Unija je izložena strateškoj ovisnosti i geopolitičkom riziku. Kako bi se ublažila asimetrija u znanju i tehnologiji među jurisdikcijama, potrebno je donijeti mjere za olakšavanje odgovarajućeg i proporcionalnog pristupa Unije i njezinih država članica novorazvijenim FAIM-ovima. Takve bi mjere trebale biti pravodobne, usklađene i učinkovite, kako u smislu politike tako i u smislu provedbe, te bi se njima trebali na odgovarajući način uzeti u obzir različiti financijski sektori Unije, koristeći se stručnim znanjem odgovarajućih europskih nadzornih tijela. Time će se smanjiti ne samo asimetrija između jurisdikcija Unije i trećih zemalja nego i među financijskim institucijama s poslovnim nastanom u različitim državama članicama, uz očuvanje jednakih uvjeta unutar i izvan Unije te svođenje sistemskog rizika na najmanju moguću. Aranžmani kojima se olakšava pristup FAIM-ovima samo za određene kategorije institucija ili u odabranim jurisdikcijama pridonijeli bi rascjepkanosti jedinstvenog tržišta u području financija, čime bi se smanjila njegova likvidnost i dubina.

Drugo, kad je riječ o asimetriji između napadača i stručnjaka za kibernetičku sigurnost, FAIM-ovi smanjuju cijenu prihvata napadača. Akteri prijetnji vjerojatno će se sve više oslanjati na FAIM-ove za provedbu tehnički naprednijih i radno intenzivnijih dijelova obrambenih operacija, uz smanjenje troškova. S druge strane, stručnjaci za kibernetičku sigurnost ograničeni su operativnim zahtjevima, ovisnostima i regulatornim obvezama, čime se ograničavaju učinak i razmjeri do kojih mogu imati koristi od FAIM-ova u kratkoročnom do srednjoročnom razdoblju, zbog čega su u konačnici potrebna dulja razdoblja za prilagodbu.

Treće, postoje razlike u načinu na koji financijske institucije raspolažu resursima i na koji su pripremljene za suočavanje s izazovima koje predstavljaju FAIM-ovi. Te razlike mogu nastati zbog troškova koji su fiksni, a ne skalirani, ograničenja resursa i ograničenog pristupa stručnjacima. Kada postoji asimetrija u sposobnosti suočavanja s takvim izazovima, najslabija karika u lancu može utjecati na stabilnost sustava.

Implikacije

Ključno je osigurati da sistemski važni platni sustavi i sustavi namire te infrastrukture financijskog tržišta ostanu zaštićeni od ranjivosti koje proizlaze iz upotrebe i razvoja FAIM-a. Javni i privatni subjekti trebali bi temeljito preispitati i ažurirati svoje okvire za kibersigurnost kako bi se uzele u obzir takve ranjivosti. Tijela zadužena za nadzor trebala bi donijeti mjere kako bi se osigurala odgovarajuća zaštita sustava. Suradnja između tijela i privatnih financijskih institucija trebala bi se provoditi kad god je to potrebno kako bi se povećala sigurnost i otpornost financijskog sustava Unije.

ESRB je u svojem izvješću o sistemskom kiberriziku ([10]) iz 2020. utvrdio brzinu, razmjer i zlonamjernu prirodu kiberprijetnji kao moguće izvore širenja sistemskog rizika. Nadležna tijela trebala bi biti svjesna da iako FAIM-ovi predstavljaju novi izvor širenja, također pojačavaju postojeće prethodno utvrđene izvore, te bi to saznanje trebala uključiti u svoje mjere politike. S obzirom na sve rizike za financijsku stabilnost koji proizlaze iz operativne izloženosti kiberriziku u financijskom sektoru, važno je osigurati da se zabrinutosti utvrđene u ovom Upozorenju odražavaju u radu na nadzoru te stajalištima o politikama koje su donijela odgovarajuća tijela u okviru svojih ovlasti.

Relevantna tijela, u okviru svojih nadležnosti, a posebno na temelju okvira uspostavljenog Uredbom (EU) 2022/2554, trebala bi biti upoznata s trima prethodno navedenim izvorima asimetrije koje su FAIM-ovi uveli u financijski sektor. Kako bi se smanjile te asimetrije, trebalo bi razmotriti dogovore o suradnji i sektorsku koordinaciju, uz postojeće okvire za testiranje ([11]). Financijska tijela trebala bi također osigurati da su odbori privatnih financijskih institucija u potpunosti predani ublažavanju kiberrizika uzrokovanih FAIM-om, da postoje jasni okviri za upravljanje i odgovornost te da se na odgovarajući način planiraju pravovremeni odgovori, zajedno s odgovarajućim unutarnjim ulaganjima.

Nekoliko mogućih događaja razmatranih u ovom Upozorenju – bilo da je riječ o sistemskom učinku, geopolitičkom riziku ili promjeni ravnoteže između napadača i stručnjaka za kibernetičku sigurnost – moglo bi utjecati na funkcioniranje financijskog sustava i povjerenje u njega. Kako bi ih kontinuirano ocjenjivao, ESRB će razmotriti potrebu za odražavanjem takvih kretanja u procjenama rizika, okvirima za testiranje i nadzornim očekivanjima, kao i u razvoju budućih scenarija. ESRB će također pratiti upotrebu i razvoj FAIM-ova i njihov učinak na financijski sektor iz perspektive sistemskog rizika. Nadalje, ESRB će ponovno procijeniti kretanja u svakoj tromjesečnoj procjeni rizika na razini općeg odbora i prema potrebi razmotriti druge mjere.

ODJELJAK 2.

Definicije

Za potrebe ove Preporuke primjenjuju se sljedeće definicije:

1. „dobavljač UI-ja” znači dobavljač kako je definiran u članku 3. točki 3. Uredbe (EU) 2024/1689;

2. „napredni UI modeli” ili „FAIM” (*Frontier AI Models*, FAIM) znači napredni UI modeli opće namjene koji mogu bitno utjecati na napadačke ili obrambene kibernetičke operacije;

3. „kibernapad” znači kibernapad kako je definiran u članku 1. Uredbe Vijeća (EU) 2019/796 ([12]), uključujući i ako potječe iz Unije;

4. „ranjivost” znači ranjivost kako je definirana u članku 3. točki 16. Uredbe (EU) 2022/2554;

5. „eksploit” (*exploit*) znači alat, tehnika ili metoda koja se upotrebljava za iskorištavanje jedne ili više ranjivosti kako bi se dobio neovlašten pristup sustavima, kako bi ih se izmijenilo ili poremetilo ili kako bi na drugi način došlo do IKT rizika ili IKT incidenata;

6. „osposobljavanje za izvođenje napada” (*weaponisation*) znači priprema ili prilagodba eksploita kojima se omogućuje sustavno ili prilagodljivo iskorištavanje ranjivosti;

7. „ključna ili važna funkcija” znači ključna ili važna funkcija kako je definirana u članku 3. točki 22. Uredbe (EU) 2022/2554;

8. „UI model opće namjene” znači UI model kako je definiran u članku 3. točki 63. Uredbe (EU) 2024/1689;

9. „UI model opće namjene sa sistemskim rizikom” znači UI model opće namjene klasificiran kao model koji predstavlja sistemski rizik u skladu s člankom 51. stavkom 1. Uredbe (EU) 2024/1689;

10. „IKT incident” znači incident kako je definiran u članku 3. točki 8. Uredbe (EU) 2022/2554;

([10]) Vidjeti *Systemic cyber risk* (Sistemski kiberrizik), ESRB, veljača 2020., dostupno na mrežnim stranicama ESRB-a na www.esrb.europa.eu.
([11]) Npr. etičko hakiranje koje se zasniva na obavještajnim podacima o prijetnjama (TIBER), penetracijsko testiranje vođeno prijetnjama (TLPT), napredno hakiranje (ART) i testiranje kibernetičke otpornosti (CyRST).
([12]) Uredba Vijeća (EU) 2019/796 od 17. svibnja 2019. o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama (SL L 129 I, 17.5.2019., str. 1., ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11. „IKT rizik” znači rizik kako je definiran u članku 3. točki 5. Uredbe (EU) 2022/2554;

12. „digitalna operativna otpornost” znači digitalna operativna otpornost kako je definirana u članku 3. točki 1. Uredbe (EU) 2022/2554.

Sastavljeno u Frankfurtu na Majni, 25. lipnja 2026.

Voditelj Tajništva ESRB-a,
u ime Općeg odbora ESRB-a,
Francesco MAZZAFERRO