C/2026/3795

16.7.2026

OPOZORILO EVROPSKEGA ODBORA ZA SISTEMSKA TVEGANJA

z dne 25. junija 2026

o sistemskih kibernetskih tveganjih, ki izhajajo iz mejnih modelov umetne inteligence

(ESRB/2026/3)

(C/2026/3795)

SPLOŠNI ODBOR EVROPSKEGA ODBORA ZA SISTEMSKA TVEGANJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Sporazuma o evropskem gospodarskem prostoru ([1]), zlasti Priloge IX k Sporazumu,

ob upoštevanju Uredbe (EU) št. 1092/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o makrobonitetnem nadzoru nad finančnim sistemom Evropske unije in ustanovitvi Evropskega odbora za sistemska tveganja ([2]), in zlasti člena 3(2), točka (c), in členov 16 in 18 Uredbe,

ob upoštevanju Sklepa ESRB/2011/1 Evropskega odbora za sistemska tveganja z dne 20. januarja 2011 o sprejetju Poslovnika Evropskega odbora za sistemska tveganja ([3]), zlasti členov 18 in 19 Sklepa,

ob upoštevanju naslednjega:

(1) Vodilni ponudniki umetne inteligence (UI) so razvili mejne modele UI, ki so zelo zmogljivi na področju kibernetske varnosti in lahko izvajajo popolnoma avtomatizirane kibernetske napade na kompleksne sisteme, vključno z odkrivanjem ranljivosti ter razvojem in spreminjanjem izkoriščevalskih orodij v orodja za napad, s čimer temeljito spreminjajo naravo kibernetskih groženj.

(2) Mejni modeli UI so pri iskanju načinov za izvedbo kibernetskih napadov znatno boljši od prejšnjih modelov UI, saj jih prekašajo po stroških, hitrosti in natančnosti ter se zdaj lahko merijo z vodilnimi človeškimi strokovnjaki.

(3) Mejni modeli UI lahko ogrožajo sisteme, ki so podlaga za okolja informacijske in komunikacijske tehnologije (IKT), od katerih je odvisna finančna infrastruktura, s čimer povečujejo verjetnost in resnost kibernetskih incidentov s sistemskimi posledicami.

(4) Mejni modeli UI dokazujejo, da so zmožni odkrivati ranljivosti in razvijati nove, s čimer glavne operacijske sisteme in programsko opremo, ki se uporabljajo v IKT okoljih v skoraj vseh organizacijah, izpostavljajo tveganju kibernetskih napadov.

(5) V preteklosti so bile takšne ranljivosti le redko odkrite, največkrat so jih odkrili raziskovalci na področju varnosti, kar je omogočalo ciljno odpravljanje težav. V takšnih primerih se ponudnikom programske opreme pogosto določi standardni rok – običajno 90 dni – za odpravo ranljivosti, preden se ta javno razkrije. Vendar bodo mejni modeli UI verjetno povečali obseg odkritih ranljivosti.

(6) Sedanje prakse odpravljanja ranljivosti v finančnem sistemu so pretežno reaktivne in temeljijo na rednih posodobitvah in priložnostnih odzivih na razkrite ranljivosti. Ta pristop deluje v okolju groženj, kjer čas dopušča, da je odkrivanje ranljivosti obvladljivo. Vendar s povečevanjem obsega ranljivosti sedanje prakse lahko postanejo nezadostne pri ohranjanju operativne odpornosti.

(7) Zaradi takega povečevanja obsega so sedanji postopki odpravljanja ranljivosti tudi izpostavljeni preobremenitvi, saj se v teh postopkih prioriteta ukrepov za odpravo ranljivosti določi na podlagi tveganja in zahteva testiranje programskih popravkov pred njihovo uvedbo, da se zagotovi operativna stabilnost. Če se v kratkem časovnem obdobju odkrije preveč ranljivosti s kritičnimi posledicami, tako da se število potrebnih kritičnih programskih popravkov znatno poveča, se morajo finančne institucije morda odločiti, ali ostanejo izpostavljene znatnim kibernetskim tveganjem ali pa zmanjšajo zahteve glede testiranja popravkov in s tem tvegajo operativne incidente in izpade.

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

(8) Spreminjanje izkoriščevalskih orodij v orodja za napad se je v preteklosti večinoma izvajalo ročno in so strokovnjaki za to potrebovali dneve ali tedne, medtem ko lahko zdaj mejni modeli UI to izvedejo v nekaj minutah ali urah. To pomeni upad obrambnih časovnih rezerv, ki so potrebne za ohranjanje neprekinjenega delovanja kritičnih in pomembnih funkcij med odpravljanjem ranljivosti.

(9) Zaradi naraščajočega spreminjanja izkoriščevalskih orodij, ki se nanašajo na kritične ranljivosti, v orodja za napad, ki jih poganja UI, in s tem povezanega skrajšanja obrambnih časovnih rezerv se tveganje za posamezne kritične ali pomembne funkcije in institucije močno povečuje. Če se taka tveganja uresničijo hkrati v vseh teh funkcijah in institucijah, lahko pride do trajnega povečanja sistemskega kibernetskega tveganja, za katerega trenutno ni na voljo popolnoma učinkovit okvir za zmanjšanje tveganja. Zaradi močne medsebojne povezanosti znotraj finančnega sektorja Unije in povezanosti med tem sektorjem ter drugimi sektorji in jurisdikcijami ta položaj predstavlja sistemsko tveganje in lahko povzroči sistemske ranljivosti.

(10) Poleg tega mejne modele UI trenutno razvija le majhno število ponudnikov UI, od katerih so nekateri izrazili zaskrbljenost, da bi lahko bili prihodnji mejni modeli UI premočni za neomejen javni dostop.

(11) Zlonamerni akterji že zdaj uporabljajo UI za izboljšanje kibernetskih napadov. Verjetno je, da bodo ti akterji sčasoma prek uhajanja podatkov, kraje, lastnega razvoja ali odprtega dostopa pridobili modele UI, katerih zmogljivosti bodo primerljive s tistimi, ki se trenutno uporabljajo v nadzorovanih obrambnih okoljih.

(12) Čeprav lahko mejni modeli UI znatno povečajo napadalne zmogljivosti in verjetnost izvedbe zapletenih kibernetskih napadov, bodo hkrati okrepili tudi obrambne zmogljivosti, zlasti na področju odkrivanja ranljivosti, korelacije podatkov in izvajanja korektivnih ukrepov s strani posameznih institucij. Vendar bodo v kratkoročnem do srednjeročnem obdobju večja hitrost, obseg in natančnost napadalnih zmogljivosti verjetno prevladali nad koristmi.

(13) Hitri razvoj mejnih modelov UI zahteva, da se ugotovljena tveganja za finančno stabilnost nemudoma obravnavajo, da se prepreči njihova uresničitev ali vsaj ublaži njihov morebitni vpliv. Za zagotovitev finančne stabilnosti na finančnih trgih Unije bi morali vsi člani Evropskega odbora za sistemska tveganja (ESRB) v okviru makrobonitetnih in mikrobonitetnih ukrepov upoštevati posledice mejnih modelov UI za operativno sposobnost in odpornost finančnih institucij. To ne posega v pooblastila centralnih bank v Uniji na področju denarne politike. Poleg trenutnih pobud drugih organov je na primer ECB v vlogi bančnega nadzornika zahtevala, da pomembne institucije nemudoma ocenijo vpliv razvijajočih se groženj in do 31. oktobra 2026 oblikujejo celovit akcijski načrt, ki vsebuje konkretne ukrepe za obravnavo takih tveganj ([4]).

(14) Glede na vse večjo razširjenost tehnologije UI je pomembno zagotoviti, da je vsa kritična infrastruktura, zlasti pa finančne institucije, pripravljena na kibernetske napade, ki jih poganjajo mejni modeli UI, ter da se sprejmejo pravočasni in ustrezni ukrepi. Vendar takšna obrambna prizadevanja posameznih subjektov niso dovolj. Učinkovit odziv in zmanjšanje tveganja zahtevata usklajen odziv, v katerega so vključene vse vpletene strani, vključno s ponudniki UI, ponudniki programske opreme, varnostnimi podjetji, vzdrževalci odprtokodne programske opreme, finančnimi institucijami ter organi na nacionalni ravni in ravni Unije.

(15) Pri obravnavanju zgoraj navedenih vprašanj je pomembno upoštevati ustrezen pravni in politični okvir Unije, zlasti Uredbo (EU) 2022/2554 Evropskega parlamenta in Sveta ([5]), Uredbo (EU) 2024/1689 Evropskega parlamenta in Sveta ([6]), Uredbo (EU) 2024/2847 Evropskega parlamenta in Sveta ([7]) ter Priporočilo Evropskega odbora za sistemska tveganja (ESRB/2021/17) ([8]).

([4]) Dopis, naslovljen na pomembne institucije, je na voljo na spletnem mestu ECB o bančnem nadzoru na naslovu www.bankingsupervision.europa.eu.

([5]) Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (UL L 333, 27.12.2022, str. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi uredb (EU) št. 168/2013 in (EU) 2019/1020 ter Direktive (EU) 2020/1828 (Akt o kibernetski odpornosti) (UL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Priporočilo Evropskega odbora za sistemska tveganja z dne 2. decembra o vseevropskem okviru za usklajevanje v primeru sistemskih kibernetskih incidentov za ustrezne organe (ESRB/2021/17) (UL C 134, 25.3.2022, str. 1).

(16) Uredba (EU) 2022/2554 zagotavlja celovit okvir, da finančne institucije prepoznajo, upravljajo, spremljajo in zmanjšajo tveganja na področju IKT, vključno s tveganji, ki izhajajo iz kibernetskih napadov. Glede na medsebojno povezanost finančnega sektorja ter njegovo odvisnost od sistemov IKT in zunanjih ponudnikov storitev bi uspešen kibernetski napad, ki bi prizadel eno ali več finančnih institucij ali njihove ključne ponudnike storitev, lahko imel znatne sistemske posledice. Finančni nadzorni organi bi morali nadzorniškim dejavnostim na tem področju dati ustrezno prednost, ob upoštevanju morebitnega vpliva takšnih kibernetskih napadov na stabilnost, celovitost in verodostojnost finančnega sistema ter morebitno operativno, finančno in potrošniško škodo, ki bi lahko nastala.

(17) Uredba (EU) 2024/1689 določa usklajena pravila za dajanje na trg, dajanje v uporabo ter za uporabo sistemov UI in modelov UI za splošne namene v Uniji, vključno, v določenih okoliščinah, s sistemi in modeli, ki jih zagotavljajo ponudniki UI s sedežem v tretjih državah, kadar se izhodni podatki, ki jih ustvari sistem UI, uporabljajo v Uniji ali je model UI vgrajen v sistem, ki je dan na trg Unije. Ta uredba določa tudi posebna pravila, vključno s strožjo regulativno ureditvijo, za modele, ki so razvrščeni kot modeli UI za splošne namene s sistemskim tveganjem.

(18) Uredba (EU) 2024/2847 uvaja obvezne zahteve glede kibernetske varnosti za proizvajalce, ki zajemajo načrtovanje, zasnovo, razvoj in vzdrževanje strojne in programske opreme z digitalnimi elementi, ki se dajejo na trg Unije. Poleg tega zahteva, da proizvajalci med življenjskim ciklom izdelkov ustrezno obravnavajo ranljivosti. Ko bo uredba decembra 2027 začela uporabljati v celoti, bodo morali tudi finančni subjekti, ki dajejo takšne izdelke na trg Unije, zagotoviti, da ti izdelki izpolnjujejo navedene zahteve.

(19) Priporočilo ESRB/2021/17 priporoča, da evropski nadzorni organi prek skupnega odbora in v sodelovanju z Evropsko centralno banko (ECB), ESRB ter ustreznimi nacionalnimi organi oblikujejo učinkovit usklajen odziv na ravni Unije v primeru večjega čezmejnega kibernetskega incidenta ali s tem povezane grožnje, ki bi lahko imela sistemski učinek na finančni sektor Unije. To je privedlo do vzpostavitve vseevropskega okvira za usklajevanje v primeru sistemskih kibernetskih incidentov (EU-SCICF), ki zagotavlja dragoceno in operativno platformo za izmenjavo informacij in usklajevanje med finančnimi organi.

(20) Zato ESRB sprejema splošno opozorilo, ki obravnava pomembna tveganja za finančno stabilnost, ki jih še povečuje razvoj mejnih modelov UI. Opozorilo upošteva analitično delo iz poročila ESRB, ki obravnava mejne modele UI s kibernetskimi zmogljivostmi z vidika finančne stabilnosti in je bilo objavljeno junija 2026 ([9]) –

SPREJEL NASLEDNJE OPOZORILO:

ODDELEK 1

Opozorilo

Nova tveganja

Hiter razvoj mejnih modelov UI s kibernetskimi zmogljivostmi prinaša v finančni sistem Unije bistvene spremembe na področju tveganj. Trenutni podatki kažejo, da so mejni modeli UI zmožni odkrivati ranljivosti, ustvarjati delujoča izkoriščevalska orodja in samostojno izvajati obsežne kibernetske napade s hitrostjo, obsegom in natančnostjo, ki daleč presegajo prejšnje modele UI. To predstavlja konceptualni premik na področju kibernetske varnosti in prelomnico v zmogljivostih UI.

ESRB meni, da ti razvojni trendi predstavljajo vir sistemskih tveganj za finančni sistem, saj lahko povzročijo znatne negativne učinke na kibernetsko varnost zaradi pospešenega odkrivanja ranljivosti, skrajšanja časa, ki je na voljo za odziv in učinkovito obrambo, povečanja obsega in izpopolnjenosti kibernetskih napadov ter pojava novih odvisnosti in tveganj koncentracije znotraj finančnega sistema. Čeprav ESRB priznava, da bodo mejni modeli UI finančnim institucijam omogočili okrepljene obrambne zmogljivosti, se bodo te zmogljivosti verjetno uresničevale postopoma v naslednjih nekaj letih, kar pomeni, da bodo morale finančne institucije poslovati v prehodnem obdobju povečanih tveganj, velike negotovosti in hitro spreminjajočega se tehnološkega okolja. Glede na visoko digitalizirano in medsebojno povezano naravo finančnega sistema bi se takšni negativni učinki na kibernetsko varnost lahko hitro razširili ter vplivali na kritične in pomembne funkcije v finančnih institucijah, kar bi na koncu privedlo do sistemskih motenj in izgube zaupanja v finančni sistem.

([9]) Dostopno na spletišču ESRB na naslovu www.esrb.europa.eu.

Novi mejni modeli UI povečujejo tveganje, povezano z IKT, kar vodi v slabitev operativne odpornosti v celotnem finančnem sektorju, zlasti na štirih področjih: (a) čas, vključno z zmožnostjo hitrega opravljanja ranljivosti v zapletenih sistemih brez povzročanja operativnih motenj, ob upoštevanju upada obrambnih časovnih rezerv med odkritjem ranljivosti in spreminjanjem izkoriščevalskih orodij v orodja za napad; (b) sposobnost strokovnjakov za kibernetsko varnost, vključno s sposobnostjo izvajanja avtomatiziranih in ročnih varnostnih testiranj s pomočjo mejnih modelov UI ter sposobnostjo zaščite pred grožnjami, ki izhajajo iz škodljive uporabe mejnih modelov UI, ter njihovega odkrivanja in odzivanja nanje; (c) koncentracija, vključno z odvisnostjo od omejenega števila ponudnikov UI, ki so sami odvisni od ponudnikov storitev v oblaku, odprtokodnih komponent in druge široko uporabljene programske opreme; in (d) zmogljivost organov, vključno z usklajevanjem pričakovanj, stresnimi testi in ukrepi za pripravljenost v skladu z razvojem mejnih modelov UI, da operativne napake ne postanejo vir širše nestabilnosti.

Poleg tega sta vzpostavitev in ohranjanje preglednosti nad uvajanjem UI v kateri koli finančni instituciji – vključno s popolnim razumevanjem, kje in kako se UI uvaja – izziv, ob upoštevanju, da se ta tehnologija uporablja v vmesnikih za stranke, notranjih sistemih, poslovnih procesih ter pri integraciji s tretjimi stranmi.

Sistemska ocena

Ugotovljeni razvojni trendi lahko bistveno spremenijo obseg in strukturo kibernetskih tveganj, s čimer se povečajo neposredna in posredna tveganja za finančno stabilnost. Zmožnosti mejnih modelov UI lahko znatno obremenijo obstoječe okvire za odpornost, zlasti če so incidenti razširjeni in se pojavljajo sočasno. Incidenti se lahko hitro razširijo tudi na finančne institucije in trge, če so prizadeti ključni zunanji ponudniki, skupni tehnološki ekosistemi ali široko uporabljene odprtokodne komponente, kar poveča tveganje za povezane motnje s sistemskimi posledicami.

Mejni modeli UI spreminjajo tri vire nesorazmerja v finančnem sektorju: prvega med jurisdikcijami, drugega med strokovnjaki za kibernetsko varnost in napadalci ter tretjega med finančnimi institucijami z boljšimi viri in slabše opremljenimi finančnimi institucijami.

Prvič, trenutna geografska koncentracija vodilnih ponudnikov UI zunaj Unije izpostavlja Unijo strateški odvisnosti in geopolitičnemu tveganju. Da bi zmanjšali nesorazmerje na področju znanja in tehnologije med jurisdikcijami, je treba sprejeti ukrepe, ki bodo Uniji in državam članicam omogočili ustrezen in sorazmeren dostop do novo razvitih mejnih modelov UI. Takšni ukrepi morajo biti pravočasni, usklajeni in učinkoviti z vidika politike in izvajanja ter morajo ustrezno upoštevati različne finančne sektorje v Uniji, pri čemer morajo izkoristiti strokovno znanje ustreznih evropskih nadzornih organov. To bo zmanjšalo nesorazmerje ne le med Unijo in jurisdikcijami tretjih držav, temveč tudi med finančnimi institucijami s sedežem v različnih državah članicah, s čimer se bodo ohranili enaki pogoji znotraj Unije in zunaj nje ter zmanjšalo sistemsko tveganje. Ureditve, ki dostop do mejnih modelov UI omogočajo samo določenim kategorijam institucij ali v izbranih jurisdikcijah, bi prispevale k razdrobljenosti enotnega finančnega trga ter zmanjšale njegovo likvidnost in globino.

Drugič, v zvezi z nesorazmerjem med napadalci in strokovnjaki za kibernetsko varnost mejni modeli UI znižujejo ceno vstopa za napadalce. Akterji groženj se bodo verjetno pri izvajanju tehnično naprednih in delovno intenzivnih delov napadalnih operacij vse bolj zanašali na mejne modele UI, da bodo znižali stroške. Strokovnjake za kibernetsko varnost pa nasprotno omejujejo operativne zahteve, odvisnosti in regulativne obveznosti, kar omejuje učinek in obseg, v katerem lahko kratkoročno do srednjeročno izkoristijo prednosti mejnih modelov UI, zaradi česar bodo nazadnje potrebovali več časa za prilagoditev.

Tretjič, med finančnimi institucijami so razlike glede virov in opremljenosti za spopadanje z izzivi, ki jih predstavljajo mejni modeli UI. Te razlike lahko povzročajo fiksni in od obsega neodvisni stroški, omejeni viri in omejen dostop do strokovnjakov. Kadar obstaja nesorazmerje v zmožnostih spopadanja s takšnimi izzivi, lahko najšibkejši člen verige vpliva na stabilnost sistema.

Posledice

Bistveno je zagotoviti, da sistemsko pomembni plačilni sistemi in sistemi za poravnavo ter infrastrukture finančnega trga ostanejo zaščiteni pred ranljivostmi, ki izhajajo iz uporabe in razvoja mejnih modelov UI. Javni in zasebni izvajalci bi morali temeljito pregledati in posodobiti okvire za kibernetsko varnost, da se upoštevajo takšne ranljivosti. Organi, pristojni za nadzor ali pregled, bi morali sprejeti ukrepe za zagotovitev ustrezne zaščite sistemov. Treba je spodbujati sodelovanje med organi in zasebnimi finančnimi institucijami, kadar koli je to potrebno zaradi povečanja varnosti in odpornosti finančnega sistema Unije.

ESRB je v poročilu o sistemskih kibernetskih tveganjih ([10]) iz leta 2020 kot možne vire širjenja sistemskega tveganja opredelil hitrost, obseg in zlonamernost kibernetskih groženj. Organi bi se morali zavedati, da mejni modeli UI predstavljajo nov vir širjenja, hkrati pa krepijo obstoječe predhodno odkrite vire, in bi morali to spoznanje vključiti v ukrepe politike. Ob upoštevanju vseh tveganj za finančno stabilnost, ki izhajajo iz operativne izpostavljenosti kibernetskim tveganjem v finančnem sektorju, je pomembno zagotoviti, da se pomisleki, opredeljeni v tem opozorilu, odražajo v delu nadzora in pregleda ter v političnih stališčih, ki jih sprejmejo pristojni organi v okviru svojih pooblastil.

Pristojni organi bi morali v okviru svojih pristojnosti in zlasti v skladu z okvirom, vzpostavljenim z Uredbo (EU) 2022/2554, upoštevati tri predhodno navedene vire nesorazmerja, ki jih povzročajo mejni modeli UI v finančnem sektorju. Za zmanjšanje tega nesorazmerja bi bilo treba poleg obstoječih okvirov za testiranje ([11]) upoštevati tudi sporazume o sodelovanju in sektorsko usklajevanje. Finančni organi bi morali prav tako zagotoviti, da so upravni odbori zasebnih finančnih institucij v celoti zavezani k zmanjševanju kibernetskih tveganj, ki jih povzročajo mejni modeli UI, vzpostavitvi jasnih okvirov upravljanja in odgovornosti ter ustreznemu načrtovanju pravočasnih odzivov, skupaj z ustreznimi notranjimi naložbami.

Več možnih razvojnih trendov, obravnavanih v tem opozorilu – sistemski učinek, geopolitično tveganje ali spremenjeno ravnovesje med napadalci in strokovnjaki za kibernetsko varnost – lahko vpliva na delovanje finančnega sistema in zaupanje vanj. ESRB bo za nadaljnje ocenjevanje teh razvojnih trendov preučil potrebo po njihovem upoštevanju v ocenah tveganj, okvirih za testiranje in nadzorniških pričakovanjih ter pri pripravi prihodnjih scenarijev. ESRB bo prav tako spremljal uporabo in razvoj mejnih modelov UI ter njihov učinek na finančni sektor z vidika sistemskega tveganja. Poleg tega bo ESRB na ravni splošnega odbora ponovno ocenil razvojne trende v vsaki četrtletni oceni tveganj ter po potrebi preučil druge ukrepe.

ODDELEK 2

Opredelitev pojmov

V tem opozorilu se uporabljajo naslednje opredelitve pojmov:

(1) „ponudnik UI“ pomeni ponudnika, kakor je opredeljen v členu 3, točka (3), Uredbe (EU) 2024/1689;

(2) „mejni modeli UI“ pomenijo napredne modele UI za splošne namene, ki so zmožni bistveno vplivati na napadalne ali obrambne kibernetske operacije;

(3) „kibernetski napad“ pomeni kibernetski napad, kakor je opredeljen v členu 1 Uredbe Sveta (EU) 2019/796 ([12]), vključno kadar ima izvor v Uniji;

(4) „ranljivost“ pomeni ranljivost, kakor je opredeljena v členu 3, točka (16), Uredbe (EU) 2022/2554;

(5) „izkoriščevalsko orodje“ pomeni orodje, tehniko ali metodo, ki se uporablja za izkoriščanje ene ali več ranljivosti z namenom pridobitve nepooblaščenega dostopa do sistemov, njihovega spreminjanja ali motenja njihovega delovanja ali z namenom povzročanja tveganj na področju IKT ali incidentov, povezanih z IKT;

(6) „spreminjanje v orodje za napad“ pomeni pripravo ali prilagoditev izkoriščevalskih orodij, ki omogočajo sistematično ali skalabilno izkoriščanje ranljivosti;

(7) „kritična ali pomembna funkcija“ pomeni kritično ali pomembno funkcijo, kakor je opredeljena v členu 3, točka (22), Uredbe (EU) 2022/2554;

(8) „model UI za splošne namene“ pomeni model UI, kakor je opredeljen v členu 3, točka (63), Uredbe (EU) 2024/1689;

(9) „model UI za splošne namene s sistemskim tveganjem“ pomeni model UI za splošne namene, ki je razvrščen kot model UI za splošne namene s sistemskim tveganjem v skladu s členom 51(1) Uredbe (EU) 2024/1689;

(10) „incident, povezan z IKT“ pomeni incident, kakor je opredeljen v členu 3, točka (8), Uredbe (EU) 2022/2554;

([10]) Glej Systemic cyber risk, ESRB, februar 2020, na voljo na spletišču ESRB na naslovu www.esrb.europa.eu.

([11]) Npr. etično vdiranje v računalniške sisteme na podlagi obveščevalnih podatkov o grožnjah (TIBER), penetracijsko testiranje na podlagi analize groženj (TLPT), napredno vdiranje v računalniške sisteme (ART) in stresno testiranje kibernetske odpornosti (CyRST).

([12]) Uredba Sveta (EU) 2019/796 z dne 17. maja 2019 o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice (UL L 129 I, 17.5.2019, str. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

(11) „tveganje na področju IKT“ pomeni tveganje, kakor je opredeljeno v členu 3, točka (5), Uredbe (EU) 2022/2554;

(12) „operativna odpornost“ pomeni digitalno operativno odpornost, kakor je opredeljena v členu 3, točka (1), Uredbe (EU) 2022/2554.

V Frankfurtu na Majni, 25. junija 2026

Vodja sekretariata ESRB

v imenu splošnega odbora ESRB

Francesco MAZZAFERRO