C/2026/3795

16.7.2026

OSTRZEŻENIE EUROPEJSKIEJ RADY DS. RYZYKA SYSTEMOWEGO

z dnia 25 czerwca 2026 r.

w sprawie systemowego ryzyka cybernetycznego wynikającego z pionierskich modeli sztucznej inteligencji

(ERRS/2026/3)

(C/2026/3795)

RADA GENERALNA EUROPEJSKIEJ RADY DS. RYZYKA SYSTEMOWEGO,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając Porozumienie o Europejskim Obszarze Gospodarczym ([1]), w szczególności załącznik IX,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1092/2010 z dnia 24 listopada 2010 r. w sprawie unijnego nadzoru makroostrożnościowego nad systemem finansowym i ustanowienia Europejskiej Rady ds. Ryzyka Systemowego ([2]), w szczególności art. 3 ust. 2 lit. c) oraz art. 16 i 18,

uwzględniając decyzję Europejskiej Rady ds. Ryzyka Systemowego ERRS/2011/1 z dnia 20 stycznia 2011 r. ustanawiającą regulamin Europejskiej Rady ds. Ryzyka Systemowego ([3]), w szczególności art. 18 i 19,

a także mając na uwadze, co następuje:

(1) Wiodący dostawcy sztucznej inteligencji (*artificial intelligence* – AI) opracowali pionierskie modele AI (*Frontier AI Models* – FAIM), które są wysoce kompetentne w dziedzinie cyberbezpieczeństwa i zdolne do przeprowadzania w pełni zautomatyzowanych cyberataków na złożone systemy, w tym poprzez wykrywanie podatności oraz opracowywanie eksploitów i ich wykorzystywanie jako narzędzia ataku, co zasadniczo zmienia krajobraz cyberzagrożeń.

(2) Modele FAIM znacznie przewyższają wcześniejsze modele AI pod względem wyszukiwania sposobów przeprowadzania cyberataków, osiągając lepsze wyniki niż poprzednie modele pod względem kosztów, szybkości i dokładności, konkurując obecnie z czołowymi ekspertami w tej dziedzinie.

(3) Modele FAIM mogą stanowić zagrożenie dla systemów wspierających środowiska technologii informacyjno-komunikacyjnych (ICT), na których opiera się infrastruktura finansowa, zwiększając prawdopodobieństwo i dotkliwość cyberincydentów o skutkach systemowych.

(4) Modele FAIM wykazują zdolność do wykrywania podatności i tworzenia nowatorskich eksploitów, narażając tym samym główne systemy operacyjne i oprogramowanie wykorzystywane w środowiskach ICT niemal wszystkich organizacji na ryzyko cyberataków.

(5) Dotychczas podatności takie wykrywane były rzadko, często przez badaczy zajmujących się bezpieczeństwem, co pozwalało na zastosowanie ukierunkowanych środków naprawczych. W takich przypadkach dostawcom oprogramowania często zapewnia się ustalony termin – zazwyczaj 90 dni – na usunięcie podatności przed jej publicznym ujawnieniem. Modele FAIM prawdopodobnie zwiększą jednak liczbę wykrywanych podatności.

(6) Obecne praktyki w zakresie usuwania podatności w systemie finansowym mają głównie charakter reaktywny i opierają się na okresowych aktualizacjach i doraźnych reakcjach na ujawnione podatności. Takie podejście sprawdza się w środowisku zagrożeń, w którym podatności wykrywane są w tempie umożliwiającym skuteczne zarządzanie nimi. Wraz ze wzrostem liczby podatności obecne praktyki mogą jednak okazać się niewystarczające do utrzymania odporności operacyjnej.

(7) Ten wzrost liczby podatności naraża również obecne procesy ich usuwania na przeciążenie, ponieważ procesy te nadają priorytet środkom naprawczym opartym na ryzyku i wymagają testowania poprawek oprogramowania przed ich wdrożeniem w celu zapewnienia stabilności operacyjnej. W przypadku wykrycia w krótkim czasie zbyt wielu podatności o znaczeniu krytycznym prowadzącego do znacznego zwiększenia liczby wymaganych krytycznych poprawek oprogramowania instytucje finansowe mogą być zmuszone do wyboru między pozostaniem w stanie podwyższonego ryzyka cybernetycznego a ograniczeniem wymogów dotyczących testów poprawek, narażając się tym samym na ryzyko wystąpienia incydentów operacyjnych i wyłączeń.

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

(8) W przeszłości wykorzystywanie eksploitów jako narzędzia ataku odbywało się w dużej mierze ręcznie i zajmowało specjalistom wiele dni lub tygodni, natomiast obecnie modele FAIM mogą tego dokonać w ciągu kilku minut lub godzin. Powoduje to załamanie się obronnych buforów czasowych, które są niezbędne do utrzymania ciągłości krytycznych i istotnych funkcji podczas działań naprawczych.

(9) Wraz z szybkim wzrostem eksploitów wykorzystywanych jako narzędzia ataku w odniesieniu do krytycznych podatności przy użyciu AI i odpowiadającym mu ograniczeniem obronnych buforów czasowych ryzyko dla poszczególnych krytycznych lub istotnych funkcji i instytucji gwałtownie rośnie. Jeżeli takie ryzyko urzeczywistni się jednocześnie w odniesieniu do tych funkcji i instytucji, może to doprowadzić do trwałego wzrostu systemowego ryzyka cybernetycznego, w odniesieniu do którego w pełni skuteczne mechanizmy kontroli nie są obecnie dostępne. Ze względu na silne wewnętrzne powiązania w unijnym sektorze finansowym, a także między tym sektorem a innymi sektorami i jurysdykcjami, sytuacja ta stwarza ryzyko systemowe i może powodować niestabilność systemową.

(10) Ponadto modele FAIM są obecnie opracowywane jedynie przez niewielką liczbę dostawców AI, z których kilku wyraziło obawy, że przyszłe modele FAIM mogą być zbyt potężne, by udostępniać je publicznie bez żadnych ograniczeń.

(11) AI jest już wykorzystywana przez podmioty działające w złym zamiarze do wzmocnienia cyberataków. Prawdopodobne jest, że takie podmioty ostatecznie uzyskają – czy to w wyniku wycieków, kradzieży, niezależnego opracowania, czy otwartego dostępu – modele AI o zdolnościach porównywalnych z tymi, które są obecnie wdrażane w kontrolowanych warunkach obronnych.

(12) Chociaż modele FAIM mogą znacznie zwiększyć zdolności ofensywne i prawdopodobieństwo wyrafinowanych cyberataków, wzmocnią one również zdolności obronne, w szczególności w odniesieniu do wykrywania podatności, korelacji danych i działań naprawczych podejmowanych przez poszczególne instytucje. W perspektywie krótko- i średnioterminowej wzrost szybkości, skali i dokładności zdolności ofensywnych prawdopodobnie przeważy jednak nad korzyściami.

(13) Szybki rozwój modeli FAIM sprawia, że konieczne jest niezwłoczne przeciwdziałanie zidentyfikowanym zagrożeniom dla stabilności finansowej, aby zapobiec ich urzeczywistnieniu się lub przynajmniej złagodzić ich potencjalne skutki. Aby zapewnić stabilność finansową na unijnych rynkach finansowych, wszyscy członkowie Europejskiej Rady ds. Ryzyka Systemowego (ERRS) powinni uwzględnić wpływ modeli FAIM na zdolność operacyjną i odporność instytucji finansowych w kontekście swoich działań w ramach polityki makroostrożnościowej i mikroostrożnościowej. Pozostaje to bez uszczerbku dla mandatów banków centralnych Unii w zakresie polityki pieniężnej. Na przykład, obok innych obecnych inicjatyw organów, EBC jako organ nadzoru bankowego, zwrócił się do instytucji istotnych o niezwłoczną ocenę wpływu zmieniającego się krajobrazu zagrożeń oraz o opracowanie do 31 października 2026 r. kompleksowego planu działania określającego konkretne środki mające na celu przeciwdziałania takim zagrożeniom ([4]).

(14) W miarę rozpowszechniania się technologii AI ważne jest zapewnienie, aby cała infrastruktura krytyczna, ze szczególnym uwzględnieniem instytucji finansowych, była przygotowana na cyberataki z wykorzystaniem modeli FAIM oraz aby we właściwym czasie podjęto odpowiednie działania zapobiegawcze. Takie wysiłki obronne podejmowane przez pojedyncze podmioty byłyby jednak niewystarczające. Skuteczne reagowanie i ograniczanie ryzyka wymaga skoordynowanej odpowiedzi obejmującej wszystkie zainteresowane strony, w tym dostawców AI, dostawców oprogramowania, firmy zajmujące się bezpieczeństwem, podmioty odpowiedzialne za utrzymanie otwartego oprogramowania, instytucje finansowe i organy, zarówno na szczeblu krajowym, jak i unijnym.

(15) Odnosząc się do powyższych kwestii, należy przywołać odpowiednie unijne ramy prawne i polityczne, w szczególności rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 ([5]), rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 ([6]), rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 ([7]) oraz zalecenie Europejskiej Rady ds. Ryzyka Systemowego (ERRS/2021/17) ([8]).

([4]) Pismo skierowane do istotnych instytucji jest dostępne na stronie internetowej na stronie internetowej EBC poświęconej nadzorowi bankowemu.

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.U. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2487 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) (Dz.U. L, 2024/2487, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Zalecenie Europejskiej Rady ds. Ryzyka Systemowego z dnia 2 grudnia 2021 r. w sprawie ogólnoeuropejskich ram koordynacji dla odpowiednich organów w odniesieniu do cyberincydentów o charakterze systemowym (ERRS/2021/17) (Dz.U. C 134 z 25.3.2022, s. 1).

(16) Rozporządzenie (UE) 2022/2554 ustanawia dla instytucji finansowych kompleksowe ramy identyfikacji ryzyka związanego z ICT, w tym ryzyka wynikającego z cyberataków, zarządzania tym ryzykiem, jego monitorowania i ograniczania. Biorąc pod uwagę wzajemne powiązania w ramach sektora finansowego i jego zależność od systemów ICT i zewnętrznych dostawców usług, udany cyberatak dotykający co najmniej jedną instytucję finansową lub jej kluczowych dostawców usług może mieć istotne skutki systemowe. Organy nadzoru finansowego powinny nadać odpowiedni priorytet działaniom nadzorczym w tym obszarze, biorąc pod uwagę potencjalny wpływ takich cyberataków na stabilność, integralność i wiarygodność systemu finansowego, a także możliwe wynikające z nich szkody operacyjne, finansowe oraz szkody dotykające konsumentów.

(17) W rozporządzeniu (UE) 2024/1689 ustanowiono zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów AI i modeli AI ogólnego przeznaczenia w Unii, w tym, w pewnych okolicznościach, systemów i modeli dostarczanych przez dostawców AI mających siedzibę w państwach trzecich, w przypadku gdy wyniki działania systemu AI są wykorzystywane w Unii lub gdy model AI jest zintegrowany z systemem wprowadzonym do obrotu w Unii. W rozporządzeniu tym wprowadzono również przepisy szczegółowe, w tym bardziej rygorystyczny system regulacyjny, dotyczące modeli sklasyfikowanych jako modele AI ogólnego przeznaczenia z ryzykiem systemowym.

(18) W rozporządzeniu (UE) 2024/2847 wprowadzono obowiązkowe wymogi w zakresie cyberbezpieczeństwa dla producentów, które obejmują planowanie, projektowanie, opracowywanie i utrzymanie sprzętu i oprogramowania z elementami cyfrowymi wprowadzanych do obrotu w Unii. Wymaga to również od producentów reagowania na podatności w cyklu życia ich produktów. Po całkowitym wejściu tych przepisów w życie w grudniu 2027 r. podmioty finansowe wprowadzające takie produkty do obrotu w Unii będą również musiały zapewnić zgodność tych produktów z tymi wymogami.

(19) W zaleceniu ERRS/2021/17 zalecono opracowanie przez Europejskie Urzędy Nadzoru (ESA), wspólnie, za pośrednictwem Wspólnego Komitetu, i wraz z Europejskim Bankiem Centralnym (EBC), ERRS i odpowiednimi organami krajowymi, skutecznej skoordynowanej reakcji na poziomie Unii na wypadek poważnych transgranicznych cyberincydentów lub związanych z nimi zagrożeń, które mogą mieć systemowy wpływ na unijny sektor finansowy. Doprowadziło to do ustanowienia paneuropejskich ram koordynacji w odniesieniu do cyberincydentów o charakterze systemowym (EU-SCICF), które stanowią cenną i funkcjonalną platformę służącą wymianie informacji i koordynacji działań między organami finansowymi.

(20) W tym kontekście ERRS niniejszym wydaje ostrzeżenie o charakterze ogólnym dotyczące istotnych zagrożeń dla stabilności finansowej spotęgowanych przez rozwój modeli FAIM. Niniejsze ostrzeżenie uwzględnia pracę analityczną zawartą w nocie ERRS dotyczącej pionierskich modeli AI o zdolnościach cybernetycznych z perspektywy stabilności finansowej, opublikowanej w czerwcu 2026 r. ([9]),

PRZYJMUJE NINIEJSZE OSTRZEŻENIE:

SEKCJA 1

Ostrzeżenie

Nowy krajobraz ryzyka

Szybki rozwój pionierskich modeli AI (*Frontier AI Models* – FAIM) o zdolnościach cybernetycznych powoduje istotne zmiany w krajobrazie ryzyka dla systemu finansowego Unii. Obecne dowody wskazują, że modele FAIM są w stanie wykrywać podatności, tworzyć działające eksploity i autonomicznie przeprowadzać pełnoskalowe cyberataki, których szybkość, skala i poziom dokładności znacznie przewyższają możliwości poprzednich modeli AI. Powoduje to zmianę paradygmatu w dziedzinie cyberbezpieczeństwa i stanowi punkt zwrotny pod względem możliwości AI.

ERRS uważa, że zmiany te są źródłem ryzyka systemowego dla systemu finansowego, które może mieć istotny negatywny wpływ na cyberbezpieczeństwo z powodu przyspieszonego wykrywania podatności, skrócenia czasu dostępnego na reakcję i skuteczną obronę, zwiększenia skali i wyrafinowania cyberataków oraz wprowadzenia nowych zależności i ryzyka koncentracji w ramach systemu finansowego. Chociaż ERRS dostrzega wzmocnione zdolności obronne, które modele FAIM zapewnią instytucjom finansowym, zdolności te prawdopodobnie będą się stopniowo urzeczywistniać w ciągu najbliższych kilku lat, co sprawi, że instytucje finansowe będą zmuszone działać w okresie przejściowym charakteryzującym się podwyższonym ryzykiem, dużą niepewnością i szybko zmieniającym się krajobrazem technologicznym. Biorąc pod uwagę wysoce zdigitalizowany i cechujący się wzajemnymi powiązaniami charakter systemu finansowego, takie negatywne skutki dla cyberbezpieczeństwa mogą się szybko rozprzestrzeniać, wpływając na krytyczne i istotne funkcje we wszystkich instytucjach finansowych, prowadząc ostatecznie do zaburzeń systemowych i utraty zaufania do systemu finansowego.

([9]) Dostępna na stronie internetowej ERRS pod adresem www.esrb.europa.eu.

Pojawiające się modele FAIM zwiększają nieodłączne ryzyko związane z ICT, co prowadzi do osłabienia odporności operacyjnej w całym sektorze finansowym, w szczególności w odniesieniu do czterech obszarów: a) czasu, w tym zdolności do szybkiego wprowadzania poprawek do złożonych systemów bez powodowania awarii operacyjnych, biorąc pod uwagę załamanie się obronnych buforów czasowych pomiędzy wykryciem podatności a wykorzystaniem eksploita jako narzędzia ataku; b) możliwości podmiotów odpowiedzialnych za bezpieczeństwo, w tym ich zdolności do przeprowadzania zautomatyzowanych i ręcznych testów bezpieczeństwa wspomaganych przez modele FAIM, a także ochrony przed zagrożeniami wynikającymi ze stosowania modeli FAIM, wykrywania takich zagrożeń i reagowania na nie; c) koncentracji, w tym zależności od ograniczonej liczby dostawców AI, zależnej z kolei od dostawców usług w chmurze, komponentów otwartego oprogramowania i innego powszechnie wykorzystywanego oprogramowania; oraz d) zdolności organów, w tym kalibracji ich oczekiwań, testów warunków skrajnych i środków gotowości odpowiednich do rozwoju modeli FAIM, tak aby awarie operacyjne nie stały się źródłem ogólnej niestabilności.

Ponadto wprowadzenie i utrzymanie widoczności wdrażania AI w każdej instytucji finansowej – w tym pełne zrozumienie, gdzie i w jaki sposób AI jest wdrażana – stanowi wyzwanie, biorąc pod uwagę, że jest ona wykorzystywana w interfejsach klienta, agentach wewnętrznych, procesach biznesowych i integracji z osobami trzecimi.

Ocena systemowa

Zidentyfikowane zmiany mogą w istotny sposób zmienić zarówno skalę, jak i strukturę ryzyka cybernetycznego, zwiększając zarówno bezpośrednie, jak i pośrednie ryzyko dla stabilności finansowej. Możliwości modeli FAIM mogą wywierać znaczną presję na istniejące systemy odporności, zwłaszcza jeżeli incydenty są powszechne i występują jednocześnie. Incydenty mogą również szybko rozprzestrzeniać się między instytucjami i rynkami finansowymi, jeżeli dotyczą kluczowych zewnętrznych dostawców, wspólnych ekosystemów technologicznych lub powszechnie stosowanych komponentów otwartego oprogramowania, co zwiększa ryzyko powiązanych zakłóceń o skutkach systemowych.

Modele FAIM zmieniają trzy źródła asymetrii w sektorze finansowym: pierwsze – między jurysdykcjami, drugie – między podmiotami odpowiedzialnymi za bezpieczeństwo a sprawcami ataków i trzecie – pomiędzy instytucjami finansowymi dysponującymi większymi zasobami a tymi, które są gorzej wyposażone.

Po pierwsze, obecna koncentracja geograficzna wiodących dostawców AI spoza Unii naraża Unię na strategiczną zależność i ryzyko geopolityczne. Aby ograniczyć asymetrię wiedzy i technologii między jurysdykcjami, konieczne jest przyjęcie środków ułatwiających Unii i jej państwom członkowskim odpowiedni i proporcjonalny dostęp do nowo opracowywanych modeli FAIM. Środki takie powinny być przyjęte w odpowiednim czasie, spójne i skuteczne, zarówno pod względem polityki, jak i wdrażania, oraz powinny odpowiednio uwzględniać różne sektory finansowe Unii, przy wykorzystaniu wiedzy fachowej odpowiednich Europejskich Urzędów Nadzoru. Zmniejszy to nie tylko asymetrię między jurysdykcjami Unii i państw trzecich, ale również między instytucjami finansowymi mającymi siedzibę w różnych państwach członkowskich, co pozwoli zachować równe warunki działania w Unii i poza nią oraz zminimalizować ryzyko systemowe. Uzgodnienia ułatwiające dostęp do modeli FAIM tylko niektórym kategoriom instytucji lub w wybranych jurysdykcjach przyczyniłyby się do fragmentacji jednolitego rynku finansowego, zmniejszając jego płynność i głębokość.

Po drugie, jeżeli chodzi o asymetrię między sprawcami ataków a podmiotami odpowiedzialnymi za bezpieczeństwo, modele FAIM obniżają cenę, jaką muszą zapłacić sprawcy ataków. Sprawcy zagrożeń będą prawdopodobnie w coraz większym stopniu polegać na modelach FAIM do prowadzenia bardziej zaawansowanych technicznie i pracochłonnych części operacji ofensywnych, co obniży ich koszty. Podmioty odpowiedzialne za bezpieczeństwo są natomiast ograniczone wymogami operacyjnymi, zależnościami i obowiązkami regulacyjnymi, co ogranicza skutki i skalę korzystania z modeli FAIM w perspektywie krótko- i średnioterminowej, a ostatecznie wymaga dłuższych okresów na dostosowanie się.

Po trzecie, istnieją różnice w zakresie zasobów i środków, jakimi dysponują organizacje, aby sprostać wyzwaniom związanym z modelami FAIM. Różnice te mogą wynikać z kosztów, które mają charakter stały, a nie proporcjonalny do skali działalności, z ograniczeń, jeśli chodzi o zasoby oraz z ograniczonego dostępu do specjalistów. W przypadku asymetrii dotyczącej zdolności radzenia sobie z takimi wyzwaniami najsłabsze ogniwo łańcucha może mieć wpływ na stabilność systemu.

Skutki

Zasadnicze znaczenie ma zapewnienie, aby systemy płatności i rozrachunku o znaczeniu systemowym oraz infrastruktury rynku finansowego nadal były chronione przed podatnościami wynikającymi ze stosowania i rozwoju modeli FAIM. Podmioty publiczne i prywatne powinny przeprowadzić gruntowny przegląd i aktualizację swoich ram cyberbezpieczeństwa w celu uwzględnienia takich podatności. Organy odpowiedzialne za nadzór lub kontrolę zwierzchnią powinny przyjąć środki mające na celu zapewnienie odpowiedniej ochrony systemów. W razie potrzeby należy prowadzić współpracę między organami a prywatnymi instytucjami finansowymi w celu zwiększenia bezpieczeństwa i odporności systemu finansowego Unii.

W sprawozdaniu z 2020 r. w sprawie systemowego ryzyka cybernetycznego ([10]) ERRS wskazała szybkość, skalę i złośliwy charakter cyberzagrożeń jako możliwe źródła rozprzestrzeniania się ryzyka systemowego. Organy powinny mieć świadomość, że podczas gdy modele FAIM stanowią nowe źródło rozprzestrzeniania się tego ryzyka, wzmacniają one także istniejące, wcześniej zidentyfikowane źródła i powinny uwzględnić tę perspektywę w swoich działaniach politycznych. Biorąc pod uwagę wszystkie ryzyka dla stabilności finansowej wynikające z ekspozycji operacyjnej na ryzyko cybernetyczne w sektorze finansowym, ważne jest zapewnienie, aby obawy wskazane w niniejszym ostrzeżeniu znalazły odzwierciedlenie w pracach nadzorczych i działaniach w ramach kontroli zwierzchniej oraz stanowiskach politycznych przyjmowanych przez odpowiednie organy w ramach ich odpowiednich mandatów.

W ramach swoich odpowiednich kompetencji, a w szczególności zgodnie z postanowieniami rozporządzenia (UE) 2022/2554, odpowiednie organy powinny być świadome trzech wyżej wymienionych źródeł asymetrii wynikających z modeli FAIM w sektorze finansowym. Aby zmniejszyć te asymetrie, oprócz istniejących ram testowania należy rozważyć uzgodnienia dotyczące współpracy i koordynacji sektorowej ([11]). Organy finansowe powinny również zapewnić, aby zarządy prywatnych instytucji finansowych były w pełni zaangażowane w ograniczanie ryzyka cybernetycznego powodowanego przez modele FAIM, aby istniały jasne ramy zarządzania i odpowiedzialności oraz aby stosowne działania były odpowiednio zaplanowane, wraz z towarzyszącymi im inwestycjami wewnętrznymi.

Wiele możliwych okoliczności uwzględnionych w niniejszym ostrzeżeniu – czy to skutki systemowe, ryzyko geopolityczne czy zmieniona równowaga między sprawcami ataków a podmiotami odpowiedzialnymi za bezpieczeństwo – może mieć wpływ na funkcjonowanie systemu finansowego i zaufanie do niego. Aby dokonywać ich ciągłej oceny, ERRS rozważy potrzebę uwzględnienia takich zmian w ocenach ryzyka, ramach testowania i oczekiwaniach nadzorczych, a także przy opracowywaniu przyszłych scenariuszy. ERRS będzie również monitorować stosowanie i rozwój modeli FAIM oraz ich wpływ na sektor finansowy z perspektywy ryzyka systemowego. Ponadto ERRS będzie ponownie oceniać zachodzące zmiany w każdej kwartalnej ocenie ryzyka na poziomie Rady Generalnej i w razie potrzeby rozważy podjęcie innych działań.

SEKCJA 2

Definicje

Użyte w niniejszym ostrzeżeniu wyrażenia oznaczają:

1) „dostawca AI” – dostawcę w rozumieniu art. 3 pkt 3 rozporządzenia (UE) 2024/1689;

2) „pionierskie modele AI (FAIM)” – zaawansowane modele AI ogólnego przeznaczenia, które mogą mieć istotny wpływ na ofensywne lub defensywne cyberoperacje;

3) „cyberatak” – cyberatak w rozumieniu art. 1 rozporządzenia Rady (UE) 2019/796 ([12]), w tym cyberatak pochodzący z Unii;

4) „podatność” – podatność w rozumieniu w art. 3 pkt 16 rozporządzenia (UE) 2022/2554;

5) „eksploit” – narzędzie, technikę lub metodę stosowaną w celu wykorzystania co najmniej jednej podatności, aby uzyskać nieuprawniony dostęp do systemów, zmodyfikować je lub zakłócić ich działanie, lub też w inny sposób spowodować ryzyko związane z ICT lub incydenty związane z ICT;

6) „wykorzystanie jako narzędzia ataku” – przygotowanie lub dostosowanie eksploitów umożliwiające systematyczne lub skalowalne wykorzystanie podatności;

7) „krytyczna lub istotna funkcja” – krytyczną lub istotną funkcję w rozumieniu art. 3 pkt 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554;

8) „model AI ogólnego przeznaczenia” – model AI zdefiniowany w art. 3 pkt 63 rozporządzenia (UE) 2024/1689;

9) „model AI ogólnego przeznaczenia z ryzykiem systemowym” – model AI ogólnego przeznaczenia klasyfikowany jako stwarzający ryzyko systemowe zgodnie z art. 51 ust. 1 rozporządzenia (UE) 2024/1689;

10) „incydent związany z ICT” – incydent zdefiniowany w art. 3 pkt 8 rozporządzenia (UE) 2022/2554;

([10]) Zob. dokument pt. „Systemic cyber risk”, ERRS, luty 2020 r., dostępny na stronie internetowej ERRS pod adresem www.esrb.europa.eu.

([11]) Np. ogólnounijne zasady ramowe dotyczące przeprowadzania etycznych testów typu red teaming (TIBER), testy penetracyjne pod kątem wyszukiwania zagrożeń (TLPT), zaawansowane testy typu red teaming (ART) oraz testy warunków skrajnych w zakresie cyberodporności (CyRST).

([12]) Rozporządzenie Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz.U. L 129 I z 17.5.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11) „ryzyko związane z ICT” – ryzyko zdefiniowane w art. 3 pkt 5 rozporządzenia (UE) 2022/2554;

12) „odporność operacyjna” – operacyjną odporność cyfrową w rozumieniu art. 3 pkt 1 rozporządzenia (UE) 2022/2554.

Sporządzono we Frankfurcie nad Menem dnia 25 czerwca 2026 r.

W imieniu Rady Generalnej ERRS

Szef Sekretariatu ERRS

Francesco MAZZAFERRO