C/2026/3795

16.7.2026

SEGNALAZIONE DEL COMITATO EUROPEO PER IL RISCHIO SISTEMICO

del 25 giugno 2026

sui rischi informatici sistemici derivanti dai modelli di intelligenza artificiale di frontiera

(CERS/2026/3)

(C/2026/3795)

IL CONSIGLIO GENERALE DEL COMITATO EUROPEO PER IL RISCHIO SISTEMICO,

visto il trattato sul funzionamento dell'Unione europea,

visto l'accordo sullo Spazio economico europeo ([1]), e in particolare l'allegato IX,

visto il regolamento (UE) n.1092/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, relativo alla vigilanza macroprudenziale del sistema finanziario nell'Unione europea e che istituisce il Comitato europeo per il rischio sistemico ([2]) e in particolare l'articolo 3, paragrafo 2, lettera c) e gli articoli 16 e 18,

vista la decisione CERS/2011/1 del Comitato europeo per il rischio sistemico, del 20 gennaio 2011, che adotta il regolamento interno del Comitato europeo per il rischio sistemico ([3]), e in particolare gli articoli 18 e 19,

considerando quanto segue:

(1) I principali fornitori di intelligenza artificiale (IA) hanno sviluppato modelli di IA di frontiera (Frontier AI Models, FAIM), che possiedono un'elevata capacità nel settore della cibersicurezza e sono in grado di effettuare attacchi informatici completamente automatizzati contro sistemi complessi, anche scoprendo vulnerabilità e sviluppando e avvalendosi di exploit come arma, modificando così radicalmente il panorama delle minacce informatiche.

(2) I FAIM sono notevolmente migliori rispetto ai modelli di IA precedenti nella ricerca di modi per compiere attacchi informatici, superando i modelli precedenti in termini di costi, velocità e accuratezza, rivaleggiando ormai con esperti umani di spicco.

(3) I FAIM hanno la capacità di minacciare i sistemi alla base degli ambienti delle tecnologie dell'informazione e della comunicazione (TIC) su cui si basa l'infrastruttura finanziaria, aumentando la probabilità e la gravità di incidenti informatici con un impatto sistemico.

(4) I FAIM hanno dimostrato di essere capaci di scoprire vulnerabilità e di creare nuovi exploit, esponendo così al rischio di attacchi informatici i principali sistemi operativi e software utilizzati in quasi tutti gli ambienti TIC delle organizzazioni.

(5) Storicamente, la scoperta di tali vulnerabilità è stata rara e spesso effettuata da ricercatori in materia di sicurezza, consentendo di rimediarvi in maniera mirata. In tali casi, ai fornitori di software è spesso concesso un periodo di tempo standardizzato, di solito 90 giorni, per correggere la vulnerabilità prima della sua divulgazione al pubblico. È tuttavia probabile che i FAIM aumentino il volume delle vulnerabilità riscontrate.

(6) Le attuali pratiche di patching nel sistema finanziario sono prevalentemente reattive e si basano su aggiornamenti periodici e risposte ad hoc alle vulnerabilità divulgate. Tale approccio funziona in un contesto di minacce in cui vi è tempo perché la scoperta della vulnerabilità rimanga gestibile. Tuttavia, con un aumento del volume delle vulnerabilità, le pratiche attuali potrebbero diventare insufficienti per conservare la resilienza operativa.

(7) Tale aumento di volume, inoltre, espone inoltre gli attuali processi di patching a sovraccarico, in quanto danno priorità alle misure correttive basate sul rischio e richiedono la verifica del patch software prima dell'applicazione per garantire la stabilità operativa. Qualora, in un breve lasso di tempo, siano individuate troppe vulnerabilità con un impatto critico, così da aumentare notevolmente il numero di patch software critici necessari, le istituzioni finanziarie potrebbero dover decidere se esporsi a rischi informatici significativi o se ridurre i requisiti per i test di patch, rischiando in tal modo incidenti operativi e interruzioni.

([1]) GU L 1 del 3.1.1994, pag. 3, ELI: http://data.europa.eu/eli/reg/2013/1024/oj.
([2]) GU L 331 del 15.12.2010, pag. 1, ELI: http://data.europa.eu/eli/reg/2010/1092/oj.
([3]) GU C 58 del 24.2.2011, pag. 4.

(8) L'elaborazione di exploit utilizzati come arma era in precedenza effettuata perlopiù manualmente e richiedeva giorni o settimane da parte di umani esperti, mentre ora può essere effettuata dai FAIM in pochi minuti o in poche ore. Ciò costituisce un crollo dei margini temporali di difesa, necessari per mantenere la continuità delle funzioni essenziali e importanti durante l'azione correttiva.

(9) Con la proliferazione di exploit utilizzati come arma, corrispondenti a vulnerabilità critiche e alimentati dall'IA e la corrispondente riduzione dei margini temporali di difesa, il rischio per singole funzioni critiche o importanti e per le istituzioni aumenta drasticamente. Qualora tali rischi si concretizzino simultaneamente in tutte le funzioni e le istituzioni, ciò potrebbe comportare un aumento permanente del rischio informatico sistemico per il quale, al momento, non è disponibile un quadro di mitigazione pienamente efficace. A causa della forte interconnessione all'interno del settore finanziario dell'Unione, nonché tra tale settore e altri settori e ordinamenti, tale situazione rappresenta un rischio sistematico e ha il potenziale di creare fragilità sistemiche.

(10) Inoltre, i FAIM sono sviluppati attualmente solo da un numero limitato di fornitori di IA, molti dei quali hanno espresso preoccupazione per il fatto che i prossimi FAIM potrebbero essere troppo potenti per un accesso pubblico illimitato.

(11) L'IA è già utilizzata da soggetti malintenzionati per potenziare gli attacchi informatici. È probabile che tali soggetti alla fine otterranno, attraverso fughe di notizie, furti, sviluppo indipendente o accesso aperto, modelli di IA con capacità comparabili a quelli attualmente utilizzati in contesti difensivi controllati.

(12) Sebbene possano aumentare in modo significativo le capacità offensive e la probabilità di attacchi informatici sofisticati, i FAIM rafforzeranno anche le capacità difensive, in particolare per quanto riguarda la scoperta di vulnerabilità, la correlazione dei dati e le azioni correttive da parte delle singole istituzioni. Tuttavia, nel breve e medio termine, l'aumento della velocità, della portata e dell'accuratezza delle capacità offensive sarà probabilmente superiore ai benefici.

(13) Il rapido sviluppo dei FAIM rende necessario affrontare senza indugio i rischi individuati per la stabilità finanziaria in modo da prevenirne il concretizzarsi o almeno attenuarne il possibile impatto. Per garantire la stabilità finanziaria dei mercati finanziari dell'Unione, tutti i membri del Comitato europeo per il rischio sistemico (CERS) dovrebbero considerare le implicazioni dei FAIM sulla capacità e la resilienza operativa delle istituzioni finanziarie nel contesto delle loro azioni di politica macroprudenziale e microprudenziale. Ciò non pregiudica i mandati di politica monetaria delle banche centrali dell'Unione. A titolo di esempio, e tra le iniziative attualmente in corso da parte di altre autorità, la BCE, nel suo ruolo di autorità di vigilanza bancaria, ha chiesto agli enti significativi di valutare tempestivamente l'impatto dell'evoluzione del panorama delle minacce e di elaborare, entro il 31 ottobre 2026, un piano d'azione di ampia portata che delinei misure concrete volte ad affrontare tali rischi ([4]).

(14) Con la proliferazione della tecnologia di IA, è importante garantire che tutte le infrastrutture critiche, e in particolare le istituzioni finanziarie, siano preparate a far fronte agli attacchi informatici supportati dai FAIM e ad adottare misure preparatorie tempestive e adeguate. Tuttavia, tali sforzi difensivi da parte di singole entità sarebbero insufficienti. Una reazione e un'attenuazione dei rischi efficaci richiedono una risposta coordinata che coinvolga tutte le parti interessate, compresi i fornitori di IA, i fornitori di software, le imprese che si occupano di sicurezza, i responsabili della manutenzione open source, le istituzioni finanziarie e le autorità a livello sia nazionale che dell'Unione.

(15) Nell'affrontare le questioni di cui sopra, è importante ricordare i pertinenti quadri giuridici e strategici dell'Unione, in particolare il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio ([5]), il regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio ([6]), il regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio ([7]) e la raccomandazione del Comitato europeo per il rischio sistemico (CERS/2021/17) ([8]).

([4]) La lettera indirizzata agli enti significativi è disponibile sul sito Internet dedicato alla vigilanza bancaria della BCE all'indirizzo www.bankingsupervision.europa.eu.

([5]) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag.1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza) (GU L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Raccomandazione del Comitato europeo per il rischio sistemico, del 2 dicembre 2021, relativa a un quadro paneuropeo di coordinamento sistemico degli incidenti informatici per le autorità competenti (CERS/2021/17) (GU C 134 del 25.3.2022, pag.1).

(16) Il regolamento (UE) 2022/2554 fornisce alle istituzioni finanziarie un quadro completo per individuare, gestire, monitorare e attenuare i rischi relativi alle TIC, tra cui i rischi derivanti da attacchi informatici. Data l'interconnessione del settore finanziario e la sua dipendenza dai sistemi TIC e da fornitori terzi di servizi, un attacco informatico riuscito che colpisce una o più istituzioni finanziarie o i loro fornitori di servizi critici potrebbe avere implicazioni sistemiche significative. Le autorità di vigilanza finanziaria dovrebbero dare adeguata priorità alle attività di vigilanza in questo settore, tenendo conto del possibile impatto di tali attacchi informatici sulla stabilità, l'integrità e l'affidabilità del sistema finanziario, nonché dei danni operativi, finanziari e ai consumatori che potrebbero derivarne.

(17) Il regolamento (UE) 2024/1689 stabilisce regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso di sistemi di IA e di modelli di IA per finalità generali nell'Unione, compresi, in determinate circostanze, i sistemi e i modelli forniti da fornitori di IA stabiliti in paesi terzi in cui l'output prodotto dal sistema di IA è utilizzato nell'Unione o un modello di IA è integrato in un sistema immesso sul mercato dell'Unione. Tale regolamento prevede inoltre norme specifiche, compreso un regime normativo più rigoroso, per i modelli classificati come modelli di IA per finalità generali con rischio sistemico.

(18) Il regolamento (UE) 2024/2847 introduce requisiti obbligatori in materia di cibersicurezza per i fabbricanti che riguardano la pianificazione, la progettazione, lo sviluppo e la manutenzione di prodotti hardware e software con elementi digitali immessi sul mercato dell'Unione. Impone inoltre ai fabbricanti di gestire le vulnerabilità durante il ciclo di vita dei loro prodotti. Una volta pienamente applicabili nel dicembre 2027, anche le entità finanziarie che immettono tali prodotti sul mercato dell'Unione dovranno garantire che siano conformi a tali requisiti.

(19) La raccomandazione CERS/2021/17 ha raccomandato l'elaborazione, da parte delle autorità europee di vigilanza (AEV), congiuntamente attraverso il comitato congiunto e insieme alla Banca centrale europea (BCE), al CERS e alle autorità nazionali competenti, di una risposta efficace coordinata a livello dell'Unione in caso di grave incidente informatico transfrontaliero o di minaccia connessa che potrebbe avere un impatto sistemico sul settore finanziario dell'Unione. Ciò ha portato all'istituzione del quadro paneuropeo di coordinamento sistemico degli incidenti informatici (EU-SCICF), che fornisce una piattaforma preziosa e operativa per lo scambio di informazioni e il coordinamento tra le autorità finanziarie.

(20) In tale contesto, il CERS adotta una segnalazione di carattere generale che affronta i rischi per la stabilità finanziaria significativi amplificati dallo sviluppo dei FAIM. La segnalazione tiene conto del lavoro analitico svolto nella nota del CERS dal titolo «Addressing Frontier AI Models with cyber capabilities from a financial stability perspective» (Affrontare i modelli di IA di frontiera con capacità informatiche dal punto di vista della stabilità finanziaria), pubblicata nel giugno 2026 ([9]),

HA ADOTTATO LA PRESENTE SEGNALAZIONE;

SEZIONE 1

Segnalazione

Nuovo panorama dei rischi

Il rapido sviluppo di modelli di IA di frontiera (Frontier AI Models, FAIM) con capacità informatiche comporta cambiamenti sostanziali nel panorama dei rischi per il sistema finanziario dell'Unione. I dati attuali indicano che i FAIM sono in grado di scoprire vulnerabilità, generare exploit operativi ed eseguire autonomamente attacchi informatici su vasta scala a una velocità, una portata e un livello di precisione di gran lunga superiori ai precedenti modelli di IA. Ciò costituisce un cambio di paradigma nel settore della cibersicurezza e un punto di svolta in termini di capacità dell'IA.

Il CERS ritiene che tali sviluppi siano una fonte di rischi sistemici per il sistema finanziario, con il potenziale di generare effetti negativi significativi sulla cibersicurezza attraverso la scoperta più rapida di vulnerabilità, la riduzione del tempo disponibile per una risposta e una difesa efficaci, l'aumento della portata e della sofisticazione degli attacchi informatici e l'introduzione di nuove dipendenze e rischi di concentrazione all'interno del sistema finanziario. Se da un lato il CERS riconosce le capacità di difesa rafforzate che i FAIM offriranno alle istituzioni finanziarie, è anche probabile che tali capacità si concretizzino gradualmente nei prossimi anni, richiedendo alle istituzioni finanziarie di operare nel corso di un periodo transitorio caratterizzato da un rischio elevato, un'elevata incertezza e un panorama tecnologico in rapida evoluzione. Data la natura altamente digitalizzata e interconnessa del sistema finanziario, tali effetti negativi sulla cibersicurezza potrebbero propagarsi rapidamente, colpendo funzioni essenziali e importanti in tutte le istituzioni finanziarie, con conseguenti perturbazioni sistemiche e perdita di fiducia nel sistema finanziario.

([9]) Disponibile sul sito del CERS all'indirizzo www.esrb.europa.eu.

I FAIM emergenti aumentano il rischio intrinseco relativo alle TIC, con conseguente indebolimento della resilienza operativa in tutto il settore finanziario, in particolare in quattro settori: a) tempo, tra cui la capacità di correggere attraverso un patch rapidamente sistemi complessi senza causare interruzioni operative, tenendo conto del crollo dei margini temporali di difesa tra la scoperta delle vulnerabilità e l'utilizzo degli exploit come arma; b) la capacità degli esperti di difesa nel campo della cibersicurezza, tra cui la loro abilità nel condurre test di sicurezza automatizzati e manuali assistiti da FAIM, così come la loro capacità di proteggere, rilevare e rispondere alle minacce derivanti dall'uso antagonista di FAIM; c) la concentrazione, tra cui la dipendenza da un numero limitato di fornitori di IA, a loro volta dipendenti da fornitori di servizi cloud, componenti open source e altri software ampiamente utilizzati; e d) la capacità delle autorità, tra cui la loro calibrazione delle aspettative, le misure di prova di stress e di preparazione in linea con lo sviluppo delle FAIM, affinché le interruzioni operative non diventino una fonte di instabilità più ampia.

Inoltre, è difficile stabilire e mantenere visibilità della diffusione dell'IA all'interno di qualsiasi istituzione finanziaria, compresa la piena comprensione del luogo e delle modalità di impiego dell'IA, tenendo conto del fatto che è utilizzata nelle interfacce con i clienti, negli agenti interni, nei processi aziendali e nell'integrazione con terzi.

Valutazione sistemica

Gli sviluppi individuati possono alterare sostanzialmente sia la portata che la struttura del rischio di cybersicurezza, aumentando i rischi diretti e indiretti per la stabilità finanziaria. Le capacità dei FAIM possono mettere sotto forte pressione i quadri in materia di resilienza esistenti, soprattutto se gli incidenti sono diffusi e si verificano contemporaneamente. Gli incidenti possono inoltre propagarsi rapidamente tra le istituzioni finanziarie e i mercati se sono interessati fornitori terzi critici, ecosistemi tecnologici condivisi o componenti open source ampiamente utilizzati, aumentando il rischio di perturbazioni correlate con implicazioni sistemiche.

I FAIM alterano tre fonti di asimmetria nel settore finanziario: la prima tra giurisdizioni, la seconda tra esperti di difesa e aggressori nel campo della cibersicurezza e la terza tra istituzioni finanziarie dotate di risorse migliori e istituzioni finanziarie meno attrezzate.

In primo luogo, l'attuale concentrazione geografica dei principali fornitori di IA al di fuori dell'Unione espone l'Unione a una dipendenza strategica e a un rischio geopolitico. Al fine di attenuare l'asimmetria delle conoscenze e tecnologica tra le giurisdizioni, è necessaria l'adozione di misure volte a facilitare un accesso adeguato e proporzionato dell'Unione e dei suoi Stati membri ai FAIM di recente elaborazione. Tali misure dovrebbero essere tempestive, coerenti ed efficienti, sia in termini di politiche che di attuazione e dovrebbero tenere adeguatamente conto dei diversi settori finanziari dell'Unione, beneficiando delle competenze delle corrispondenti AEV. Ciò attenuerà non solo l'asimmetria tra le giurisdizioni dell'Unione e dei paesi terzi, ma anche tra le istituzioni finanziarie stabilite in diversi Stati membri, preservando condizioni di parità all'interno e all'esterno dell'Unione e riducendo al minimo il rischio sistemico. Disposizioni che agevolino l'accesso ai FAIM solo per determinate categorie di enti o in determinate giurisdizioni contribuirebbero alla frammentazione del mercato unico dei finanziamenti, riducendone la liquidità e la profondità.

In secondo luogo, per quanto riguarda l'asimmetria tra aggressori ed esperti di difesa nel campo della cibersicurezza, i FAIM riducono il prezzo di accesso per gli aggressori. È probabile che gli autori delle minacce facciano sempre più affidamento sui FAIM per condurre le parti più avanzate dal punto di vista tecnico e ad alta intensità di attività delle operazioni offensive, riducendo i costi. Gli esperti di difesa, invece, sono vincolati da requisiti operativi, dipendenze e obblighi normativi, il che limita l'effetto e la portata dei benefici che possono trarre dai FAIM nel breve e medio termine e, in ultima analisi, richiede periodi più lunghi per adeguarsi.

In terzo luogo, vi sono differenze nel modo in cui le istituzioni finanziarie sono dotate delle risorse e degli strumenti necessari per far fronte alle sfide poste dai FAIM. Tali differenze possono essere generate da costi che sono fissi invece che variabili, da vincoli in termini di risorse e da un accesso limitato agli specialisti. In caso di asimmetria nella capacità di far fronte a tali sfide, l'anello più debole della catena può incidere sulla stabilità del sistema.

Implicazioni

È essenziale garantire che i sistemi di pagamento e di regolamento di importanza sistemica e le infrastrutture dei mercati finanziari continuino a essere protetti dalle vulnerabilità derivanti dall'uso e dallo sviluppo del FAIM. Gli operatori pubblici e privati dovrebbero riesaminare e aggiornare approfonditamente i loro quadri in materia di cibersicurezza per tenere conto di tali vulnerabilità. Le autorità incaricate della vigilanza o della sorveglianza dovrebbero adottare misure per garantire che i sistemi siano adeguatamente protetti. La cooperazione tra le autorità e gli istituti finanziari privati dovrebbe essere perseguita ogniqualvolta necessario per aumentare la sicurezza e la resilienza del sistema finanziario dell'Unione.

Nella sua relazione del 2020 sul rischio informatico sistemico ([10]), il CERS ha identificato la velocità, la portata e l'intenzione malevola delle minacce informatiche quali possibili fonti di propagazione del rischio sistemico. Le autorità dovrebbero essere consapevoli del fatto che, sebbene i FAIM rappresentino una nuova fonte di propagazione, essi amplificano anche le fonti esistenti precedentemente individuate, e dovrebbero integrare questa consapevolezza nella loro azione politica. Considerando tutti i rischi per la stabilità finanziaria derivanti dall'esposizione operativa al rischio informatico nel settore finanziario, è importante garantire che i timori individuati nella presente segnalazione si riflettano nell'attività di vigilanza e sorveglianza e nelle posizioni strategiche adottate dalle autorità competenti, nell'ambito dei rispettivi mandati.

Le autorità competenti, nell'ambito delle rispettive competenze e in particolare del quadro istituito dal regolamento (UE) 2022/2554, dovrebbero essere consapevoli delle tre fonti di asimmetria precedentemente menzionate introdotte dai FAIM nel settore finanziario. Per ridurre tali asimmetrie, dovrebbero essere presi in considerazione accordi di cooperazione e coordinamento settoriale unitamente ai quadri relativi ai test già esistenti ([11]). Le autorità finanziarie dovrebbero inoltre garantire che i consigli di amministrazione delle istituzioni finanziarie private si impegnino appieno ad attenuare i rischi di cybersicurezza indotti dalle FAIM, che siano posti in essere quadri chiari in materia di governance e responsabilità e che siano pianificate in modo adeguato risposte tempestive, unitamente ai corrispondenti investimenti interni.

Diversi possibili sviluppi presi in considerazione nella presente segnalazione, che si tratti dell'impatto sistemico, del rischio geopolitico o del mutato equilibrio tra aggressori ed esperti di difesa nel campo della cibersicurezza, possono incidere sul funzionamento del sistema finanziario e sulla fiducia in esso. Per valutarli costantemente, il CERS prenderà in considerazione la necessità di tenere conto di tali sviluppi nelle valutazioni dei rischi, nei quadri relativi alle prove e nelle aspettative di vigilanza, nonché nell'elaborazione di scenari futuri. Il CERS monitorerà inoltre l'uso e lo sviluppo dei FAIM e il loro impatto sul settore finanziario dal punto di vista del rischio sistemico. Inoltre, il CERS riesaminerà gli sviluppi di ciascuna valutazione trimestrale dei rischi a livello del Consiglio generale e prenderà in considerazione altre azioni, ove necessario.

SEZIONE 2

Definizioni

Ai fini della presente segnalazione si applicano le seguenti definizioni:

1) per «fornitore di IA» si intende un fornitore come definito all'articolo 3, punto 3, del regolamento (UE) 2024/1689;

2) per «modelli di IA di frontiera (FAIM)» si intende modelli avanzati di IA per finalità generali in grado di incidere materialmente sulle operazioni informatiche offensive o difensive;

3) per «attacco informatico» si intende un attacco informatico quale definito all'articolo 1 del regolamento (UE) 2019/796 del Consiglio ([12]), anche se proveniente dall'interno dell'Unione;

4) per «vulnerabilità» si intende una vulnerabilità quale definita all'articolo 3, punto 16, del regolamento (UE) 2022/2554;

5) per «exploit» si intende uno strumento, una tecnica o un metodo utilizzato per sfruttare una o più vulnerabilità al fine di ottenere un accesso non autorizzato ai sistemi, modificarli, perturbarli o altrimenti comportare rischi relativi alle TIC o incidenti connessi alle TIC;

6) per «utilizzo come arma» si intende la preparazione o l'adattamento di exploit che consentono lo sfruttamento sistematico o scalabile delle vulnerabilità;

7) per «funzione essenziale o importante» si intende una funzione essenziale o importante quale definita all'articolo 3, punto 22, del regolamento (UE) 2022/2554;

8) per «modello di IA per finalità generali» si intende un modello di IA quale definito all'articolo 3, punto 63, del regolamento (UE) 2024/1689;

9) per «modello di IA per finalità generali con rischio sistemico» si intende un modello di IA per finalità generali classificato come modello che presenta un rischio sistemico in conformità all'articolo 51, paragrafo 1, del regolamento (UE) 2024/1689;

10) per «incidente connesso alle TIC» si intende un incidente quale definito all'articolo 3, punto 8, del regolamento (UE) 2022/2554;

([10]) Cfr. Systemic cyber risk, CERS, febbraio 2020, disponibile sul sito web del CERS all'indirizzo www.esrb.europa.eu.

([11]) Ad esempio, il quadro di riferimento per i test di red-team etici basati sui dati sulle minacce (European Framework for Threat Intelligence Based Ethical Red-teaming, TIBER-EU) (i test di penetrazione guidati dalle minacce (threat-led penetration testing, TLPT), il red teaming avanzato (ART) e le prove di stress sulla ciberresilienza (cyber resilience stress testing, CyRST).

([12]) Regolamento (UE) 2019/796 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri (GU L 129 I del 17.5.2019, pag.1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11) per «rischio informatico» si intende un rischio quale definito all'articolo 3, punto 5, del regolamento (UE) 2022/2554;

12) per «resilienza operativa» si intende la resilienza operativa digitale quale definita all'articolo 3, punto 1, del regolamento (UE) 2022/2554.

Fatto a Francoforte sul Meno, il 25 giugno 2026

Il capo del segretariato del CERS,
per conto del Consiglio generale del CERS
Francesco MAZZAFERRO