Journal officiel
de l'Union européenne

FR
Série C

C/2026/3795

16.7.2026

ALERTE DU COMITÉ EUROPÉEN DU RISQUE SYSTÉMIQUE

du 25 juin 2026

sur les cyberrisques systémiques résultant des modèles d'intelligence artificielle de pointe

(CERS/2026/3)

(C/2026/3795)

LE CONSEIL GÉNÉRAL DU COMITÉ EUROPÉEN DU RISQUE SYSTÉMIQUE,

vu le traité sur le fonctionnement de l'Union européenne,

vu l'accord sur l'Espace économique européen ([1]), et notamment son annexe IX,

vu le règlement (UE) nº 1092/2010 du Parlement européen et du Conseil du 24 novembre 2010 relatif à la surveillance macroprudentielle du système financier dans l'Union européenne et instituant un Comité européen du risque systémique ([2]), et notamment son article 3, paragraphe 2, point c), et ses articles 16 et 18,

vu la décision CERS/2011/1 du Comité européen du risque systémique du 20 janvier 2011 portant adoption du règlement intérieur du Comité européen du risque systémique ([3]), et notamment ses articles 18 et 19,

considérant ce qui suit:

(1) Les principaux fournisseurs d'intelligence artificielle (IA) ont mis au point des modèles d'IA de pointe, (*Frontier AI Models* — FAIM), qui sont très performants dans le domaine de la cybersécurité et capables de mener des cyberattaques entièrement automatisées contre des systèmes complexes, y compris par la détection de vulnérabilités et le développement et la transformation en arme de codes d'exploitation, modifiant ainsi fondamentalement le paysage des cybermenaces.

(2) Les FAIM sont nettement plus performants que les modèles d'IA antérieurs pour trouver des moyens de mener des cyberattaques, surpassant ainsi les modèles antérieurs en termes de coût, de rapidité et de précision, rivalisant désormais avec les meilleurs experts humains.

(3) Les FAIM ont la capacité de menacer les systèmes qui sous-tendent les environnements des technologies de l'information et de la communication (TIC) sur lesquels reposent les infrastructures financières, augmentant ainsi la probabilité et la gravité des cyberincidents ayant une incidence systémique.

(4) Les FAIM ont démontré leur capacité à détecter les vulnérabilités et à concevoir de nouveaux codes d'exploitation, exposant ainsi les principaux systèmes d'exploitation et logiciels utilisés dans les environnements TIC de la quasi-totalité des organisations au risque de cyberattaques.

(5) Historiquement, la détection de ces vulnérabilités a été rare et souvent le fait de chercheurs dans le domaine de la sécurité, ce qui a permis d'y remédier de manière ciblée. Dans ces cas, les fournisseurs de logiciels disposent généralement d'un délai standard — généralement de 90 jours — pour corriger la vulnérabilité avant sa divulgation. Cependant, les FAIM sont susceptibles d'accroître le volume des vulnérabilités détectées.

(6) Les pratiques actuelles de correction des vulnérabilités dans le système financier sont principalement réactives, reposant sur des mises à jour périodiques et des réponses ad hoc aux vulnérabilités divulguées. Cette approche fonctionne dans un environnement de menaces où le les délais disponibles permettent de maintenir la détection des vulnérabilités à un niveau gérable. Toutefois, l'augmentation du nombre de vulnérabilités pourrait rendre ces pratiques insuffisantes pour maintenir la résilience opérationnelle.

(7) Cette augmentation de volume expose également les processus de correction actuels à une saturation, étant donné qu'ils hiérarchisent les mesures correctives en fonction des risques et nécessitent de tester les correctifs logiciels avant leur mise en œuvre afin de garantir la stabilité opérationnelle. Si un trop grand nombre de vulnérabilités ayant une incidence critique sont détectées dans un court laps de temps, entraînant une augmentation considérable du nombre de correctifs logiciels critiques à appliquer, les établissements financiers pourraient être amenés à choisir entre maintenir leur exposition à des cyberrisques importants ou réduire les exigences en matière de tests des correctifs, au risque d'entraîner des incidents opérationnels et des interruptions de services.

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

(8) La conception de codes d'exploitation transformés en armes était auparavant réalisée en grande partie manuellement et prenait des journées ou des semaines à des d'experts humains, alors qu'elle peut désormais être réalisée par des FAIM en quelques minutes ou quelques heures. Cela entraîne un effondrement des marges temporelles de défense, qui sont nécessaires pour assurer la continuité des fonctions critiques et importantes pendant la correction des vulnérabilités.

(9) Avec la prolifération, renforcée par l'IA, des codes d'exploitation transformés en armes, correspondant à des vulnérabilités critiques, et la réduction correspondante des marges temporelles de défense, les risques pesant sur les différentes fonctions critiques ou importantes et sur les établissements augmentent fortement. Si ces risques se matérialisaient simultanément pour l'ensemble de ces fonctions et établissements, cela pourrait entraîner une augmentation durable du cyberrisque systémique pour lequel, à l'heure actuelle, il n'existe pas de cadre d'atténuation pleinement efficace. En raison de la forte interdépendance au sein du secteur financier de l'Union, ainsi qu'entre ce secteur et d'autres secteurs et juridictions, cette situation présente un risque systématique et est susceptible de créer des fragilités systémiques.

(10) En outre, les FAIM ne sont actuellement mis au point que par un nombre limité de fournisseurs d'IA, dont plusieurs ont fait part de leurs préoccupations quant au fait que les futurs FAIM pourraient être trop puissants pour faire l'objet d'un accès public illimité.

(11) L'IA est déjà utilisée par des acteurs malveillants pour renforcer les cyberattaques. Il est probable que ces acteurs finiront par se procurer, que ce soit par des fuites, des vols, un développement indépendant ou un accès libre, des modèles d'IA dotés de capacités comparables à celles actuellement déployées dans des environnements défensifs contrôlés.

(12) Si les FAIM sont susceptibles d'accroître considérablement les capacités offensives et la probabilité de cyberattaques sophistiquées, ils renforceront également les capacités défensives, notamment en ce qui concerne la détection des vulnérabilités, la corrélation des données et les mesures correctives prises par les différents établissements. Toutefois, à court et moyen terme, l'augmentation de la rapidité, de l'ampleur et de la précision des capacités offensives devrait l'emporter sur les avantages.

(13) Le développement rapide des FAIM rend nécessaire de traiter sans délai les risques identifiés pesant sur la stabilité financière, afin d'empêcher leur matérialisation ou, à tout le moins, d'atténuer leur incidence potentielle. Afin de garantir la stabilité financière sur les marchés financiers de l'Union, il convient que l'ensemble des membres du Comité européen du risque systémique (CERS) examinent les effets des FAIM sur la capacité opérationnelle et la résilience des établissements financiers dans le cadre de leurs mesures de politique macroprudentielle et microprudentielle. Cela est sans préjudice des mandats de politique monétaire des banques centrales de l'Union. À titre d'exemple, et parmi les initiatives actuelles d'autres autorités, la BCE, en sa qualité d'autorité de surveillance bancaire, a demandé aux établissements importants d'évaluer sans délai l'incidence de l'évolution du paysage des menaces et d'élaborer, au plus tard le 31 octobre 2026, un plan d'action global exposant des mesures concrètes visant à faire face à ces risques ([4]).

(14) À mesure que la technologie de l'IA se généralise, il importe de veiller à ce que toutes les infrastructures critiques, et notamment les établissements financiers, soient préparées à faire face aux cyberattaques renforcées par des FAIM, et prennent en temps utile les mesures appropriées. Toutefois, de tels efforts en matière de défense menés par des entités isolées seraient insuffisants. Une réponse efficace et une atténuation des risques nécessitent une action coordonnée associant l'ensemble des parties concernées, y compris les fournisseurs d'IA, les éditeurs de logiciels, les entreprises de sécurité, les personnes chargées de la maintenance des logiciels à codes source ouverts, les établissements financiers et les autorités tant au niveau national qu'au niveau de l'Union.

(15) Lors de l'examen des questions susmentionnées, il importe de rappeler le cadre juridique et politique pertinent de l'Union, notamment le règlement (UE) 2022/2554 du Parlement européen et du Conseil ([5]), le règlement (UE) 2024/1689 du Parlement européen et du Conseil ([6]), le règlement (UE) 2024/2847 du Parlement européen et du Conseil ([7]) ainsi que la recommandation du Comité européen du risque systémique (CERS/2021/17) ([8]).

([4]) La lettre adressée aux établissements importants est disponible sur le site internet de la BCE consacré à la supervision bancaire à l'adresse suivante: www.bankingsupervision.europa.eu.

([5]) Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011(JO L 333 du 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689 du 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) nº 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L 2847 du 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Recommandation du Comité européen du risque systémique du 2 décembre 2021 sur un cadre paneuropéen de coordination des cyberincidents systémiques pour les autorités concernées CERS/2021/17) (JO C 134 du 25.3.2022, p. 1).

(16) Le règlement (UE) 2022/2554 fixe un cadre global permettant aux établissements financiers d'identifier, de gérer, de suivre et d'atténuer les risques liés aux TIC, y compris les risques résultant des cyberattaques. Compte tenu de l'interconnexion du secteur financier et de sa dépendance à l'égard des systèmes liés aux TIC et des prestataires de services tiers, une cyberattaque réussie touchant un ou plusieurs établissements financiers ou leurs prestataires de services essentiels pourrait avoir des incidences systémiques importantes. Il convient que les autorités de surveillance financière donnent une priorité appropriée aux activités de surveillance dans ce domaine, compte tenu de l'incidence potentielle de telles cyberattaques sur la stabilité, l'intégrité et la fiabilité du système financier, ainsi que des préjudices opérationnels, financiers et causés aux consommateurs qui pourraient en résulter.

(17) Le règlement (UE) 2024/1689 établit des règles harmonisées pour la mise sur le marché, la mise en service et l'utilisation de systèmes d'IA et de modèles d'IA à usage général dans l'Union, y compris, dans certaines circonstances, les systèmes et modèles fournis par des fournisseurs d'IA établis dans des pays tiers lorsque les résultats produits par le système d'IA sont utilisés dans l'Union, ou lorsqu'un modèle d'IA est intégré dans un système mis sur le marché de l'Union. Ce règlement prévoit également des règles spécifiques, y compris un régime réglementaire plus strict, pour les modèles classés comme modèles d'IA à usage général présentant un risque systémique.

(18) Le règlement (UE) 2024/2847 introduit des exigences obligatoires en matière de cybersécurité pour les fabricants qui couvrent la planification, la conception, le développement et la maintenance des produits matériels et logiciels mis sur le marché de l'Union. Il impose également aux fabricants de traiter les vulnérabilités tout au long du cycle de vie de leurs produits. Une fois pleinement applicable en décembre 2027, les entités financières qui mettent de tels produits sur le marché de l'Union devront également veiller à ce que ces produits soient conformes à ces exigences.

(19) La recommandation CERS/2021/17 a recommandé l'élaboration, par les autorités européennes de surveillance (AES), agissant conjointement par l'intermédiaire du comité mixte et en collaboration avec la Banque centrale européenne (BCE), le CERS et les autorités nationales concernées, d'une réponse efficace et coordonnée au niveau de l'Union en cas de cyberincident transfrontalier majeur ou de menace connexe susceptible d'avoir une incidence systémique sur le secteur financier de l'Union. Cela a conduit à la mise en place du cadre paneuropéen de coordination des cyberincidents systémiques (EU-SCICF) qui constitue une plateforme précieuse et opérationnelle d'échange d'informations et de coordination entre les autorités financières.

(20) Dans ce contexte, le CERS adopte par la présente une alerte de portée générale concernant les risques importants pesant sur la stabilité financière amplifiés par le développement des FAIM. Cette alerte tient compte des travaux analytiques présentés dans la note du CERS intitulée «*Addressing Frontier AI Models with cyber capabilities from a financial stability perspective*» (Traiter les modèles d'IA de pointe dotés de cybercapacités sous l'angle de la stabilité financière), publiée en juin 2026 ([9]),

A ADOPTÉ LA PRÉSENTE ALERTE:

SECTION 1

Alerte

Nouveau paysage des risques

Le développement rapide des modèles d'IA de pointe (*Frontier AI Models* — FAIM) dotés de cybercapacités entraîne des changements importants dans le paysage des risques pesant sur le système financier de l'Union. Les données actuelles indiquent que les FAIM sont capables de détecter des vulnérabilités, de générer des codes d'exploitation opérationnels et d'exécuter de manière autonome des cyberattaques à grande échelle, avec une rapidité, une ampleur et un niveau de précision dépassant largement ceux des modèles d'IA antérieurs. Il s'agit d'un changement de paradigme dans le domaine de la cybersécurité et d'un moment charnière en termes de capacité d'IA.

Le CERS considère ces évolutions comme une source de risques systémiques pour le système financier, susceptibles d'engendrer des effets négatifs importants sur la cybersécurité en raison de l'accélération de la détection des vulnérabilités, de la réduction du temps disponible pour réagir et assurer une défense efficace, de l'ampleur et de la sophistication accrues des cyberattaques, ainsi que de l'apparition de nouvelles dépendances et de nouveaux risques de concentration au sein du système financier. Bien que le CERS reconnaisse les capacités défensives renforcées que les FAIM offriront aux établissements financiers, ces capacités ne devraient se concrétiser que progressivement au cours des prochaines années, obligeant les établissements financiers à traverser une période de transition caractérisée par un niveau de risque élevé, une forte incertitude et un paysage technologique en évolution rapide. Compte tenu de la nature hautement numérisée et interconnectée du système financier, ces effets négatifs sur la cybersécurité pourraient se propager rapidement, touchant des fonctions critiques et importantes dans l'ensemble des établissements financiers, ce qui, à terme, entraînerait une perturbation systémique et une perte de confiance dans le système financier.

([9]) Disponible sur le site Internet du CERS à l'adresse suivante: www.esrb.europa.eu.

Les FAIM émergents accroissent le risque inhérent lié aux TIC, ce qui affaiblit la résilience opérationnelle dans l'ensemble du secteur financier, en particulier dans quatre domaines: a) le temps, y compris la capacité à corriger rapidement des systèmes complexes sans provoquer de défaillance opérationnelle, compte tenu de l'effondrement des marges temporelles de défense entre la détection de vulnérabilités et la transformation en arme des codes d'exploitation; b) les capacités des défenseurs, y compris leur aptitude à réaliser des tests de sécurité automatisés et manuels assistés par des FAIM, ainsi que leur capacité à se protéger contre les menaces résultant d'une utilisation malveillante des FAIM, à les détecter et à y répondre; c) la concentration, y compris les dépendances à l'égard d'un nombre limité de fournisseurs d'IA, eux-mêmes dépendants de fournisseurs de services d'informatique en nuage, de composantes de logiciels libres et d'autres logiciels largement utilisés; et d) la capacité des autorités, y compris leur capacité à ajuster leurs attentes, leurs tests de résistance et leurs mesures de préparation en fonction du développement des FAIM, afin que les défaillances opérationnelles ne deviennent pas une source d'instabilité à plus grande échelle.

En outre, il est difficile d'assurer et de maintenir la visibilité du déploiement de l'IA au sein de tout établissement financier, y compris de comprendre pleinement où et comment l'IA est déployée, compte tenu de son utilisation dans les interfaces clients, les agents internes, les processus opérationnels et l'intégration avec des tiers.

Évaluation systémique

Les évolutions recensées pourraient modifier sensiblement à la fois l'ampleur et la structure du cyberrisque, augmentant ainsi les risques directs et indirects pesant sur la stabilité financière. Les capacités des FAIM pourraient soumettre les cadres de résilience existants à une pression considérable, en particulier lorsque les incidents sont de grande ampleur et se produisent simultanément. Les incidents pourraient également se propager rapidement entre les établissements financiers et sur les marchés si des prestataires tiers essentiels, des écosystèmes technologiques partagés, ou des composantes de logiciels libres largement utilisées, sont touchés, ce qui accroît le risque de perturbations connexes ayant des incidences systémiques.

Les FAIM modifient trois sources d'asymétrie dans le secteur financier: la première entre les juridictions, la deuxième entre les défenseurs et les attaquants, et la troisième entre les établissement financiers mieux dotés en ressources et ceux qui le sont moins.

Premièrement, la concentration géographique actuelle des principaux fournisseurs d'IA en dehors de l'Union expose cette dernière à une dépendance stratégique et à des risques géopolitiques. Afin d'atténuer l'asymétrie des connaissances et des technologies entre les juridictions, il est nécessaire d'adopter des mesures visant à faciliter un accès adéquat et proportionné de l'Union et de ses États membres aux FAIM nouvellement développés. Il convient que ces mesures soient prises en temps utile, qu'elles soient cohérentes et efficaces, tant en termes de conception que de mise en œuvre, et qu'elles tiennent dûment compte des différents secteurs financiers de l'Union, en s'appuyant sur l'expertise des AES correspondantes. Cela permettra d'atténuer non seulement une asymétrie entre l'Union et les juridictions de pays tiers, mais aussi entre les établissements financiers établis dans différents États membres, en préservant des conditions de concurrence équitables au sein de l'Union et au-delà, tout en limitant le risque systémique. Des dispositions facilitant l'accès aux FAIM uniquement pour certaines catégories d'établissements ou dans certaines juridictions contribueraient à la fragmentation du marché unique des services financiers, en réduisant sa liquidité et sa profondeur.

Deuxièmement, en ce qui concerne l'asymétrie entre les attaquants et les défenseurs, les FAIM réduisent le coût d'entrée pour les attaquants. Les acteurs malveillants devraient s'appuyer de plus en plus sur les FAIM pour mener les phases les plus avancées sur le plan technique et les plus exigeantes en termes de main-d'œuvre des opérations offensives, ce qui en diminue les coûts. Les défenseurs, en revanche, sont contraints par des exigences opérationnelles, des dépendances et des obligations réglementaires, ce qui limite, à court et à moyen terme, la mesure dans laquelle ils peuvent bénéficier des FAIM, et nécessite en fin de compte des périodes d'adaptation plus longues.

Troisièmement, il existe des différences dans la manière dont les établissements financiers sont dotés en ressources et moyens pour faire face aux défis posés par les FAIM. Ces différences peuvent résulter de coûts fixes plutôt que proportionnels, de contraintes en matière de ressources et d'un accès limité aux spécialistes. En cas d'asymétrie dans la capacité à faire face à ces défis, le maillon le plus faible de la chaîne peut compromettre la stabilité du système.

Incidences

Il est essentiel de veiller à ce que les systèmes de paiement et de règlement d'importance systémique ainsi que les infrastructures des marchés financiers demeurent protégés contre les vulnérabilités résultant de l'utilisation et du développement des FAIM. Il convient que les opérateurs publics et privés procèdent à un examen approfondi et à une mise à jour de leurs cadres de cybersécurité afin de tenir compte de ces vulnérabilités. Il convient que les autorités chargées de la surveillance ou de la supervision adoptent des mesures afin de garantir une protection adéquate des systèmes. Il convient de renforcer la coopération entre les autorités et les établissements financiers privés chaque fois que cela est nécessaire afin d'accroître la sécurité et la résilience du système financier de l'Union.

Dans son rapport de 2020 sur le cyberrisque systémique ([10]), le CERS a identifié la rapidité, l'ampleur et l'intention malveillante des cybermenaces comme des sources possibles de propagation du risque systémique. Les autorités devraient être conscientes du fait que, si les FAIM constituent une nouvelle source de propagation, elles amplifient également les sources existantes précédemment identifiées, et elles devraient intégrer cet élément dans les mesures prises dans le cadre de leur politique. Compte tenu de l'ensemble des risques pesant sur la stabilité financière résultant de l'exposition opérationnelle au cyberrisque dans le secteur financier, il importe de veiller à ce que les préoccupations identifiées dans la présente alerte soient prises en compte dans les travaux de surveillance et de supervision ainsi que dans les orientations adoptées par les autorités compétentes, dans le cadre de leurs mandats respectifs.

Il convient que les autorités compétentes, dans le cadre de leurs compétences respectives et notamment dans le cadre établi par le règlement (UE) 2022/2554, tiennent compte des trois sources d'asymétrie susmentionnées introduites par les FAIM dans le secteur financier. Afin de réduire ces asymétries, il convient d'envisager des accords de coopération et une coordination sectorielle parallèlement aux cadres de tests existants ([11]). Il convient également que les autorités financières s'assurent que les organes de direction des établissements financiers privés s'engagent pleinement à atténuer les cyberrisques induits par les FAIM, que des cadres clairs de gouvernance et de responsabilité soient en place et que des réponses en temps utile soient dûment planifiées, ainsi que les investissements internes correspondants.

Plusieurs évolutions possibles examinées dans la présente alerte — qu'il s'agisse de l'incidence systémique, du risque géopolitique ou de la modification de l'équilibre entre attaquants et défenseurs — sont susceptibles d'avoir une incidence sur le fonctionnement du système financier et sur la confiance placée dans celui-ci. Afin de les évaluer en continu, le CERS examinera la nécessité de tenir compte de ces évolutions dans les évaluations des risques, les cadres de tests et les attentes prudentielles, ainsi que dans l'élaboration de futurs scénarios. LE CERS suivra également l'utilisation et le développement des FAIM ainsi que leur incidence sur le secteur financier sous l'angle du risque systémique. En outre, le CERS réévaluera les évolutions lors de chaque évaluation trimestrielle des risques au niveau du conseil général et envisagera d'autres actions si nécessaire.

SECTION 2

Définitions

Aux fins de la présente alerte, on entend par:

1) «fournisseur d'IA», un fournisseur au sens de l'article 3, point 3), du règlement (UE) 2024/1689;

2) «modèles d'IA de pointe» (*Frontier AI Models* — FAIM) », des modèles avancés d'IA à usage général susceptibles d'avoir une incidence notable sur les cyberopérations offensives ou défensives;

3) «cyberattaque», une cyberattaque au sens de l'article 1er du règlement (UE) 2019/796 ([12]), notamment lorsqu'elle a son origine à l'intérieur de l'Union;

4) «vulnérabilité», une vulnérabilité au sens de l'article 3, point 16), du règlement (UE) 2022/2554;

5) «code d'exploitation», un outil, une technique ou une méthode utilisé pour tirer parti d'une ou de plusieurs vulnérabilités afin d'obtenir un accès non autorisé aux systèmes, les modifier, les perturber ou générer de toute autre manière un risque lié aux TIC ou des incidents liés aux TIC.

6) «transformation en arme», la préparation ou l'adaptation de codes d'exploitations permettant l'exploitation systématique ou à grande échelle de vulnérabilités;

7) «fonction critique ou importante», une fonction critique ou importante au sens de l'article 3, point 22), du règlement (UE) 2022/2554;

8) «modèles d'IA à usage général», un modèle d'IA au sens de l'article 3, point 63), du règlement (UE) 2024/1689;

9) «modèle d'IA à usage général présentant un risque systémique», un modèle d'IA à usage général classé comme présentant un risque systémique conformément à l'article 51, paragraphe 1, du règlement (UE) 2024/1689;

10) «incident lié aux TIC», un incident au sens de l'article 3, point 8), du règlement (UE) 2022/2554;

([10]) Voir Systemic cyber risk, CERS, février 2020, disponible sur le site internet du CERS à l'adresse suivante: ww.esrb.europa.eu.

([11]) Par exemple, le cadre de tests pour un cyberpiratage éthique fondé sur les renseignements sur les menaces (*Threat Intelligence-based Ethical Red Teaming* — TIBER), les tests d'intrusion fondés sur la menace (*threat-led penetration testing* — TLPT), le cyberpiratage avancé (*advanced red teaming* — ART) et le test de résistance évaluant la cyberrésilience (*cyber resilience stress testing* — CyRST).

([12]) Règlement (UE) 2019/796 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres (JO L 129 I du 17.05.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11) «risque lié aux TIC», un risque au sens de l'article 3, point 5), du règlement (UE) 2022/2554;

12) «résilience opérationnelle», la résilience opérationnelle numérique au sens de l'article 3, point 1), du règlement (UE) 2022/2554;

Fait à Francfort-sur-le-Main, le 25 juin 2026.

Le chef du secrétariat du CERS,
au nom du conseil général du CERS,
Francesco MAZZAFERRO