COMMISSION
EUROPÉENNE

Strasbourg, le 7.7.2026
COM(2026) 577 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

Plan d'action en matière de cybersécurité et d'intelligence artificielle

1. Introduction

L'intelligence artificielle (IA) d'avant-garde marque un tournant dans le domaine de la cybersécurité. Les modèles d'IA d'avant-garde (c'est-à-dire les plus avancés disponibles ou en cours de développement) apportent des capacités accrues pour renforcer l'état de préparation et améliorer la détection des menaces et la réaction à celles-ci, créant ainsi **des possibilités sans précédent d'accroître la cyberrésilience**. À mesure que ces capacités continueront de progresser[1], l'IA permettra aux équipes de cybersécurité d'agir plus rapidement et à plus grande échelle, ce qui donnera aux entreprises les moyens de faire face plus efficacement aux menaces émergentes. Dans le même temps, **les capacités avancées en matière d'IA qui sont déjà disponibles aujourd'hui,** y compris en source ouverte, **peuvent déjà être utilisées pour renforcer la cyberrésilience de l'UE**[2].

L'IA est déjà devenue **un élément déterminant du paysage des menaces**, permettant des cyberopérations offensives plus automatisées, à échelle plus évolutive et plus sophistiquées, y compris dans la cybercriminalité.[3] Alors que les capacités de pointe sont actuellement concentrées dans un petit nombre de modèles et de systèmes d'IA (c'est-à-dire des modèles et des systèmes capables d'exécuter une grande variété de tâches et qui se rapprochent, atteignent ou dépassent l'état actuel de la technique)[4], le déficit de capacités se réduit à mesure que les modèles à source ouverte continuent de s'améliorer. En conséquence, les capacités d'avant-garde réelles devraient devenir de plus en plus accessibles au fil du temps, y compris aux acteurs malveillants tels que les cybercriminels, qui peuvent exploiter ces capacités pour mener des attaques plus complexes.

Pour aborder ce nouveau paradigme, l'UE s'est dotée des moyens nécessaires. Ces dernières années, elle a mis en place les fondamentaux suivants: les bases juridiques et opérationnelles pour aborder la cybersécurité à l'ère de l'IA. Le **règlement sur l'IA** constitue le premier cadre juridiquement contraignant au monde pour gérer les risques découlant des systèmes et modèles d'IA, notamment les risques systémiques liés aux modèles d'IA à usage général les plus avancés, tels que les risques d'utilisation abusive en ligne[5]. Le **règlement sur la cyberrésilience**, qui devrait être pleinement applicable d'ici à la fin de 2027, traite de la sécurité des chaînes d'approvisionnement en rendant obligatoires la sécurité dès la conception et la gestion des vulnérabilités tout au long du cycle de vie des produits logiciels et matériels sur le marché de l'UE.[6] Le règlement sur l'IA et le règlement sur la cyberrésilience contribuent conjointement à faire en sorte que les modèles, systèmes et produits d'IA comportant des éléments numériques soient construits et entretenus dans un souci constant de sécurité. Parallèlement, la **directive SRI 2**[7], associée au **règlement sur la résilience opérationnelle**

[1] De récents travaux de recherche de l'AISI (l'institut britannique de sécurité en matière d'IA) tendent à indiquer que, dans le cadre de tests de cybersécurité contrôlés, les modèles d'IA les plus avancés sont en mesure d'accomplir des tâches de plus en plus longues sans aide humaine. La durée estimée des tâches qu'ils peuvent effectuer double désormais en seulement quelques mois et non plus quelques années, et de récentes études semblent indiquer que ce rythme pourrait s'accélérer.

[2] «L'IA modifie l'économie de la détection des vulnérabilités. Les acteurs du secteur de la cybersécurité devraient s'adapter maintenant», CERT-UE, avril 2026.

[3] ENISA, *ENISA Threat landscape 2025 (Le paysage des menaces 2025 selon l'ENISA),* octobre 2025.

[4] Tel que défini à l'article 2, point 4, de la proposition d'acte législatif sur le développement de l'informatique en nuage et de l'IA (CADA), COM (2026) 502 final.

[5] Règlement (UE) 2024/1689.

[6] Règlement (UE) 2024/2847.

[7] Directive (UE) 2022/2555 — couvrant onze secteurs hautement critiques (l'énergie, les transports, le secteur bancaire, les infrastructures des marchés financiers, la santé, l'eau potable, les eaux usées, l'infrastructure numérique, la gestion des services TIC, l'administration publique et l'espace) et sept autres secteurs critiques (les services postaux et d'expédition; la gestion des déchets; la fabrication, la production et la distribution de produits

numérique[8] du secteur financier, fournit un cadre fondé sur les risques pour la cybersécurité des secteurs critiques. Ces législations offrent un cadre solide qui, s'il est mis en œuvre efficacement, résiste à l'évolution des technologies et des menaces. Le **règlement sur la cybersolidarité** complète ce cadre par des mécanismes opérationnels visant à soutenir les États membres dans la préparation, la détection et la réaction aux incidents importants et majeurs[9]. Ensemble, ces mesures contribuent à la réalisation des objectifs de la **stratégie pour une union de la préparation**[10] et de la **stratégie ProtectEU**[11],

Les cybercapacités avancées fondées sur l'IA constituent également un atout essentiel pour garantir la sécurité de notre Union. Si ces capacités, disponibles au moyen de différents modèles, y compris les modèles ouverts, peuvent déjà renforcer la cyberrésilience de l'UE, les capacités d'avant-garde sont principalement développées en dehors de l'UE, et leur disponibilité est souvent déterminée par des processus non transparents contrôlés depuis l'étranger. La connaissance de ces capacités et l'accès à celles-ci sont donc pertinents non seulement pour la résilience numérique, mais aussi pour la souveraineté technologique de l'Europe. Pour préserver cette souveraineté, l'UE doit veiller à ce que l'adoption de capacités avancées de cybersécurité fondées sur l'IA ne crée pas de nouvelles dépendances stratégiques. Dans le même temps, l'Europe doit accélérer le développement de sa résilience afin de pouvoir suivre le rythme de cette évolution rapide du paysage des menaces.

L'UE a déjà pris des **mesures stratégiques en vue de réduire les dépendances à l'égard des technologies critiques et d'accroître les capacités locales**. Par l'intermédiaire du programme Horizon Europe et du programme pour une Europe numérique, l'UE finance déjà le développement de cybercapacités avancées fondées sur l'IA et le Fonds du Conseil européen de l'innovation est devenu un investisseur important dans la *deep tech* en Europe, notamment en ce qui concerne les investissements dans les start-up et les scale-up dans le domaine de la cybersécurité et des technologies de l'IA[12]. En outre, la proposition récente d'**acte législatif sur le développement de l'informatique en nuage et de l'IA**[13] **(CADA)** accroîtrait la capacité des centres de données de l'UE et l'autonomie de l'informatique en nuage et de l'IA, en contribuant au déploiement plus large de l'IA, y compris des outils et applications liés au cyberespace. Cela permettrait à l'UE de s'appuyer sur des capacités critiques en matière d'informatique en nuage et d'IA, réduisant ainsi les dépendances à l'égard des risques géopolitiques et de sécurité. La proposition s'appuie sur la **stratégie pour l'application de l'IA** et le **plan d'action pour un continent de l'IA**, reconnaissant notamment la nécessité de lancer de grands défis pour soutenir et développer l'IA d'avant-garde.

En s'appuyant sur ces bases solides, **l'UE doit à présent prendre de nouvelles mesures pour s'attaquer aux problèmes sous-jacents immédiats et tirer parti des possibilités offertes par l'IA dans le domaine de la cybersécurité**.

Le présent plan d'action fournit une **réponse initiale et ciblée pour aider les États membres et les organisations de l'Union à faire face à cette nouvelle réalité**.

---

chimiques; la production, la transformation et la distribution des denrées alimentaires; la fabrication; les fournisseurs numériques et la recherche).

[8] Règlement (UE) 2022/2554.

[9] Règlement (UE) 2025/38.

[10] JOIN(2025) 130 final.

[11] COM (2025) 148 final.

[12] Sifted, 20 mars 2026: Europe's most active deep tech investors in 2025 (Les investisseurs de la deep tech les plus actifs d'Europe en 2025); rapport d'impact 2025 du CEI.

[13] COM(2026) 502 final.

Premièrement, afin que l'IA d'avant-garde soit adoptée de manière sûre et responsable, l'UE renforcera sa capacité à évaluer l'IA d'avant-garde avant son déploiement, y compris en ce qui concerne la cybersécurité. Cela favorisera un processus d'évaluation externe rigoureux et des capacités d'évaluation de haut niveau de l'IA dans l'UE. L'UE facilitera également l'accès des acteurs européens aux cybercapacités avancées fondées sur l'IA et soutiendra les efforts visant à tester les modèles d'IA disponibles pour les cas d'utilisation de la cybersécurité.

Deuxièmement, l'UE intensifiera ses efforts pour aider les secteurs critiques et les PME à se préparer aux cybermenaces fondées sur l'IA, y compris par la mise en œuvre des fondamentaux de la cybersécurité. En s'appuyant sur l'ensemble de l'IA disponible, l'UE soutiendra son utilisation pour renforcer la cyberrésilience et remédier aux vulnérabilités les plus critiques.

Troisièmement, l'UE renforcera sa capacité à mettre au point et à déployer des solutions fondées sur l'IA en stimulant un écosystème européen autour de celles-ci et en continuant à renforcer sa propre capacité de développement d'avant-garde. Pour atteindre ce dernier objectif, il faudra réaliser d'urgence des investissements en fonds propres à grande échelle pour renforcer les capacités propres de l'Europe en matière d'IA d'avant-garde afin de stimuler les solutions européennes répondant à nos besoins.

Enfin, pour tous ces objectifs, l'UE collaborera avec des partenaires partageant les mêmes valeurs afin de promouvoir une approche mondiale fiable et sûre de l'IA d'avant-garde et de la cybersécurité.

2. Pilier 1: Rendre l'IA d'avant-garde sûre, accessible et déployable pour la cybersécurité européenne

Étant donné que les cybercapacités avancées fondées sur l'IA pourraient, dans un avenir proche, être instrumentalisées contre nos infrastructures critiques et notre société, l'UE doit en priorité assurer une sensibilisation précoce à ces capacités, renforcer les capacités techniques pour évaluer leurs risques, façonner les possibilités de tester leur potentiel de déploiement dans le domaine de la cybersécurité et définir des voies d'accès plus claires à des fins légitimes de cybersécurité en Europe. À cette fin, et en s'appuyant sur le cadre juridique prévu par le règlement sur l'IA, l'UE étendra les capacités européennes d'évaluation préalable au déploiement, stimulera une approche européenne commune en matière d'accès et coordonnera les activités de test afin que l'IA d'avant-garde puisse être accessible et utilisée en toute sécurité pour la cybersécurité en Europe.

2.1. Évaluer et atténuer les risques posés par l'IA d'avant-garde

Le règlement sur l'IA fixe des exigences en matière de cybersécurité des **systèmes d'IA**[14] et **impose aux fournisseurs des modèles d'IA à usage général les plus avancés d'évaluer et d'atténuer les risques systémiques**, y compris ceux liés à l'utilisation abusive de l'IA dans le domaine du cyberespace.[15]

[14] Dans le cadre de l'annexe III du règlement sur l'IA, les systèmes d'IA utilisés dans les infrastructures critiques seront considérés comme étant à haut risque et feront l'objet de dispositions spécifiques, y compris en matière de cybersécurité.

[15] Le règlement sur l'IA définit un «risque systémique» comme «un risque spécifique aux capacités à fort impact des modèles d'IA à usage général, ayant une incidence significative sur le marché de l'Union en raison de leur portée ou d'effets négatifs réels ou raisonnablement prévisibles sur la santé publique, la sûreté, la sécurité publique, les droits fondamentaux ou la société dans son ensemble, pouvant être propagé à grande échelle tout au long de la chaîne de valeur» (article 3, point 65, du règlement sur l'IA).

À partir du 2 août 2026, la Commission exercera les pouvoirs de surveillance et d'exécution prévus par le règlement sur l'IA afin de garantir un contrôle efficace des systèmes d'IA ainsi que des modèles d'IA à usage général, y compris les modèles qui présentent des risques systémiques liés à la cybersécurité.[16] Au titre de ce contrôle, le recensement, par les fournisseurs, des risques associés aux capacités du modèle et les mesures qu'ils ont mises en œuvre pour atténuer ces risques font l'objet d'une évaluation. Ces exigences restent proportionnées aux capacités de la technologie en question.

Les pouvoirs de surveillance et d'exécution seront soutenus par le **groupe scientifique qui conseille le Bureau de l'IA de la Commission**, **par des canaux de signalement sécurisés** et par le **code de bonnes pratiques en matière d'IA à usage général**.

2.2. Renforcer l'excellence européenne dans l'évaluation de l'IA d'avant-garde avant son déploiement

Afin de favoriser l'adoption sûre et responsable de l'IA pour la cybersécurité dans l'UE, l'action réglementaire doit être complétée par des **capacités d'évaluation européennes renforcées**. À mesure que les capacités d'IA progressent et compte tenu du fait que les risques systémiques peuvent concerner d'autres domaines que celui du cyberespace[17], la réalisation d'évaluations externes apparaît comme une bonne pratique pour garantir la sécurité de l'IA d'avant-garde, conformément aux approches établies dans d'autres secteurs porteurs de risques. Le règlement sur l'IA souligne également l'**importance de l'évaluation préalable au déploiement** par l'intermédiaire d'entités tierces afin d'évaluer et d'atténuer les risques systémiques, le cas échéant. À ce jour, la plupart des entités de premier plan effectuant des évaluations par des tiers avant le déploiement de modèles d'IA sont établies en dehors de l'UE. Compte tenu de leur importance croissante, il devient urgent qu'une partie de cette expertise en matière d'évaluation et des infrastructures qui y sont associées soit présente au sein de l'UE.

L'UE doit donc renforcer l'expertise disponible afin de créer un écosystème crédible et compétitif d'évaluateurs tiers pour évaluer les capacités avancées en matière d'IA et les mesures d'atténuation des risques, en favorisant la confiance dans le cadre de gouvernance européen de l'IA. À cette fin, la Commission proposera **des critères pour les évaluateurs tiers aux fins du code de bonnes pratiques en matière d'IA à usage général et encouragera le développement d'un écosystème d'évaluation plus large**. Il s'agira notamment de faciliter des échanges constructifs entre les évaluateurs et les experts concernés afin d'améliorer les méthodes d'évaluation et de clarifier les exigences en matière de qualifications.

En ce qui concerne **l'évaluation des modèles d'IA spécifiquement destinés à la cybersécurité**, l'Europe a le potentiel de jouer un rôle de premier plan dans ce domaine avec des spécialistes de haut niveau en matière de cybersécurité. Compte tenu du contexte d'urgence, l'UE devrait tirer parti de cette expertise et la renforcer. Pour atteindre cet objectif, la Commission lancera un appel spécifique en vue de **la mise en place d'une capacité d'évaluation de l'UE pour les modèles d'IA, qui doit inclure la cybersécurité.** Cette capacité contribuerait fortement à l'écosystème naissant de l'UE et s'appuierait sur le savoir-

[16] Les pouvoirs d'exécution à l'égard des fournisseurs de modèles d'IA à usage général présentant un risque systémique qui ne respectent pas les dispositions relatives à l'atténuation du risque systémique consistent notamment à demander des informations sur le modèle, à demander l'accès au modèle pour effectuer des évaluations, à exiger des mesures d'atténuation des risques et, en dernier ressort, à infliger des amendes allant jusqu'à 3 % du chiffre d'affaires annuel mondial ou à demander à un fournisseur de restreindre la mise à disposition sur le marché, de retirer ou de rappeler le modèle.

[17] À titre d'exemple, la biologie est un autre domaine dans lequel les capacités des modèles d'IA à usage général ne cessent d'augmenter et pourraient être utilisées à mauvais escient, ce qui présente un risque pour la santé publique et la sécurité publique.

faire émergent en matière d'évaluation de l'IA dans les États membres. Elle soutiendra également les activités réglementaires de la Commission menées par l'intermédiaire du Bureau de l'IA[18] en offrant une option européenne pour les évaluations par des tiers des modèles d'IA et de leurs mesures d'atténuation. Elle éclairera la gestion des risques par les fournisseurs en évaluant de manière indépendante les capacités des modèles et l'efficacité des mesures d'atténuation prises par les fournisseurs de modèles[19].

Cette capacité européenne aidera les fournisseurs de modèles d'IA à usage général à respecter les obligations pertinentes du règlement sur l'IA et le code de bonnes pratiques pour les modèles d'IA à usage général[20]. Elle garantira un processus d'évaluation externe crédible et rigoureux. Les capacités d'évaluation de haut niveau dans l'UE éclaireront également la compréhension des risques systémiques potentiels, y compris dans le domaine de la cybersécurité, mais aussi dans les biotechnologies et d'autres domaines, en produisant des signaux d'alerte précoce lorsque des risques sont recensés.

2.3.Faciliter l'accès à des cybercapacités avancées fondées sur l'IA dans l'UE

L'accès à l'IA d'avant-garde dotée de cybercapacités avancées est de plus en plus régi par des décisions propres aux fournisseurs et souvent non européennes, certains fournisseurs limitant l'accès à la gestion des risques d'utilisation abusive au moyen de **programmes d'accès structurés** (par exemple, l'échelonnement du déploiement des versions de modèles). Bien qu'une telle restriction puisse être justifiée par des raisons de sécurité, cette pratique manque souvent de transparence en ce qui concerne les critères appliqués pour déterminer quelles sont les organisations, notamment les entreprises, auxquelles l'accès est octroyé, et par quel procédé il est accordé. Cela peut compromettre la capacité des acteurs européens, y compris les autorités compétentes et les opérateurs d'infrastructures critiques, à utiliser en temps voulu ces capacités d'IA et à renforcer leur résilience.

Il est urgent d'adopter une approche coordonnée au niveau de l'UE afin de permettre aux **acteurs publics et privés européens** concernés d'accéder à cette IA d'avant-garde en toute sécurité et sans retard injustifié. À cette fin, l'UE encouragera un processus de pointe, fondé sur les risques, assorti de critères clairs et conçu pour atténuer efficacement les risques d'utilisation abusive.

La Commission, en coordination avec l'Agence de l'Union européenne pour la cybersécurité (ENISA), élaborera un **cadre européen de référence pour un accès structuré aux capacités avancées d'IA destinées à la cybersécurité.**, qui servira de document d'orientation pour préciser comment les fournisseurs d'IA dotés de cybercapacités avancées peuvent accorder un accès aux organisations européennes, y compris aux entreprises, et soutenir ainsi leur atténuation des risques cyber.

[18] Le chapitre sur la sûreté et la sécurité du code de bonnes pratiques en matière d'IA à usage général impose aux fournisseurs de procéder à des évaluations de modèles également par l'intermédiaire d'évaluateurs externes indépendants dûment qualifiés (appendice 3.5). Ces rapports soutiendront ensuite les activités réglementaires du Bureau de l'IA, étant donné que les fournisseurs sont tenus de fournir au Bureau de l'IA tout rapport disponible provenant d'évaluations externes avec le rapport type (mesure 7.4).

[19] Les évaluations réalisées par cette capacité seront différentes de celles réalisées sur la plateforme de test visée à la section 2.4. La plateforme sera principalement utilisée pour tester les applications de cybersécurité des modèles d'IA, tandis que la capacité sera axée sur l'évaluation et l'atténuation du risque systémique afin de favoriser le respect du code de bonnes pratiques.

[20] La capacité ne sera pas un organisme d'évaluation de la conformité et ne soutiendra que le respect des obligations par ses évaluations.

Dans ce document d'orientation figureront **les critères qui devraient être pris en considération** pour accorder aux acteurs européens l'accès à l'IA dotée de cybercapacités avancées. Le cadre devrait couvrir les critères pertinents pour différents types d'organisations (par exemple, les institutions de l'UE, les autorités des États membres, les opérateurs d'infrastructures critiques, les fournisseurs de cybersécurité et les acteurs de la recherche) et décrire la manière dont ces acteurs seraient identifiés. Il devrait également inclure des critères de sécurité afin que l'accès accordé par son intermédiaire ne présente pas de risque excessif, ainsi qu'**un mécanisme visant à rationaliser la fourniture d'un accès** aux entités éligibles. Ce mécanisme devrait également faciliter l'**information** précoce par les fournisseurs sur les programmes d'accès de confiance prévus ainsi que le partage des connaissances entre les organisations de l'UE auxquelles l'accès à un modèle ou à un système donné a été accordé.

Bien qu'**il n'introduise pas de nouvelles obligations pour les fournisseurs**, le schéma directeur soutiendra les objectifs du code de bonnes pratiques en matière d'IA à usage général en recensant d'éventuelles mesures d'atténuation de la sécurité susceptibles de compléter **la gestion des risques systémiques** à mettre en œuvre par les fournisseurs de modèles d'IA à usage général présentant un risque systémique[21][22]. **Ce cadre de référence européen** servira de base à la poursuite de la coopération internationale.

Le cadre de référence devrait inclure **des mesures d'urgence en cas d'accès restreint ou retiré à l'IA dotée de cybercapacités avancées** afin de définir les actions à exécuter au niveau de l'UE lorsque l'accès à un modèle ou à un système pertinent est restreint ou retiré par un fournisseur ou une autorité d'un pays tiers. En outre, quand un accès rapide à des technologies d'IA d'avant-garde est nécessaire pour un usage général, la Commission, en coopération avec les États membres, étudiera la possibilité de recourir aux instruments de financement disponibles, y compris les marchés publics conjoints, afin d'**obtenir conjointement l'accès à ces modèles ou systèmes**.

2.4. Tester l'IA à l'aide de cybercapacités avancées en vue d'un déploiement rapide et sécurisé de l'IA dans le domaine de la cybersécurité

L'accès à une IA d'avant-garde sûre et digne de confiance doit aller de pair avec la mise à l'essai de ses capacités en vue de son utilisation dans le cadre d'opérations de cybersécurité, telles que l'analyse des vulnérabilités, la remédiation et la réaction aux incidents. Pour tirer parti de ses avantages, les opérateurs d'infrastructures critiques et les pouvoirs publics doivent rapidement comprendre comment l'IA dotée de cybercapacités avancées fonctionne dans des contextes de cybersécurité réalistes avant d'être déployée dans des environnements sensibles. Ces essais devraient avoir lieu dans **des environnements sûrs et contrôlés**.

Afin de créer des synergies au niveau européen, l'**ENISA** et le **Centre commun de recherche de la Commission européenne (JRC)**, en coopération avec d'autres services concernés de la Commission et d'autres entités de l'Union, telles que le service de cybersécurité pour les institutions, organes et organismes de l'Union (CERT-UE), Europol et les autorités sectorielles, ainsi qu'avec les États membres, organiseront donc **une plateforme de test sécurisée pour l'IA dans les cas d'utilisation de la cybersécurité[23].** La plateforme permettra aux participants d'utiliser leurs propres clés d'accès au modèle dans le cadre de règles de sécurité et de confidentialité partagées, chacun couvrant ses propres coûts, utilisant ses propres outils et

[21] Conformément à l'article 55, paragraphe 1, point b), du règlement sur l'IA.
[22] Par exemple, le chapitre sur la sûreté et sécurité du code de bonnes pratiques en matière d'IA à usage général mentionne «l'échelonnement de l'accès au modèle» comme exemple de mesure d'atténuation des risques dans la mesure 5.1.
[23] La plateforme existante gérée par le JRC pourrait être mise à niveau pour permettre ce type de test.

conservant la responsabilité de ses méthodes de test. L'ENISA, en coordination avec le JRC, devrait régir l'accès à la plateforme de test et les résultats agrégés.

Cette plateforme européenne de test sécurisée permettra également de **tester le déploiement de cybercapacités avancées en matière d'IA dans les systèmes des infrastructures critiques** sans exposer les infrastructures réelles à des risques («**plateformes de simulation cyber**»[24]). Cette initiative privilégiera **l'adaptation et l'extension des plateformes de simulation cyber existantes** plutôt que la duplication des environnements. En particulier, alors que le développement de nouvelles plateformes de simulation cyber sera limité aux secteurs où de telles capacités ne sont pas actuellement disponibles, tous les secteurs économiques pourraient soutenir cette initiative en fournissant des environnements existants à intégrer au moyen d'engagements spécifiques. Les acteurs du secteur concernés peuvent recevoir des informations agrégées issues des activités de test pertinentes, sous réserve des règles de confidentialité applicables.

Cet environnement sera utilisé pour tester l'IA à des fins de renforcement de la cyberrésilience et non pour évaluer la conformité des modèles d'IA à usage général avec le règlement sur l'IA[25]. Les activités réalisées dans cet environnement favoriseront et accéléreront l'expérience opérationnelle de l'utilisation de l'IA au service de la cyberrésilience, notamment en matière de détection, de triage, de renseignements sur les menaces et de réaction, afin de devancer les attaquants. Afin de garantir un niveau élevé de cybersécurité dans l'ensemble de l'Union, l'**ENISA** s'appuiera sur ses connaissances pour publier et tenir à jour **des orientations et des conseils sur l'utilisation sécurisée des modèles et systèmes d'IA disponibles** pour l'écosystème au sens large.

Actions clés:

- **Action clé nº 1 — La Commission soutiendra la mise en place d'une capacité d'évaluation de l'UE pour les modèles d'IA, qui doit inclure la cybersécurité (2027).**
- **Action clé nº 2 — La Commission, en coordination avec l'ENISA, définira un schéma directeur européen pour un accès structuré aux capacités avancées en matière d'IA à des fins de cybersécurité afin de garantir que les organisations européennes puissent accéder à ces capacités en toute sécurité et en temps utile (T4 2026).**
- **Action clé nº 3 — L'ENISA et le Centre commun de recherche de la Commission européenne (JRC) mettront au point une plateforme de test sécurisée pour l'IA dotée de cybercapacités avancées pour les cas d'utilisation en matière de cybersécurité afin de stimuler le déploiement rapide et sécurisé de l'IA dans le domaine de la cybersécurité (T4 2026).**

[24] Les plateformes de simulation cyber sont des environnements sécurisés et contrôlés qui reproduisent, sous une forme simulée, des systèmes, réseaux ou infrastructures numériques. Elles permettent des essais dans des conditions réalistes, tout en veillant à ce que toute activité menée dans l'environnement n'affecte pas les systèmes ou services réels.

[25] Tester l'IA au service de la cyberrésilience vise à comprendre l'adéquation opérationnelle d'un modèle d'IA ou d'un système d'IA pour l'exécution d'une tâche spécifique en matière de cybersécurité, tandis que l'évaluation des modèles d'IA pour soutenir le respect du règlement sur l'IA vise à fournir une évaluation des risques découlant du modèle et de l'efficacité des mesures d'atténuation des risques mises en œuvre par le fournisseur du modèle. Tester l'IA au service de la cyberrésilience doit donc être distingué de l'évaluation des modèles d'IA pour soutenir le respect du règlement sur l'IA et nécessite des compétences et des ressources différentes.

3. Pilier 2: Préparer le cyberécosystème de l'UE à l'ère de l'IA

Alors que les cybercapacités avancées en matière d'IA deviennent de plus en plus accessibles et largement déployées, l'UE doit être prête à la fois à faire face à leur éventuelle utilisation abusive contre son économie et sa société, ainsi qu'à les utiliser en toute sécurité à des fins de cyberrésilience. L'IA peut accélérer la découverte de vulnérabilités avec un degré élevé d'automatisation et à plus grande échelle, tout en réduisant l'expertise, le temps et les ressources nécessaires aux acteurs malveillants pour mener des attaques sophistiquées. Pour l'UE, la priorité immédiate est de renforcer sa préparation et d'aider les secteurs critiques à s'adapter à ces menaces. Il s'agit notamment d'intégrer les solutions d'IA disponibles dans les opérations de cybersécurité, en s'appuyant sur l'ensemble des modèles d'IA et en particulier ceux qui sont à source ouverte, tout en accélérant les efforts visant à recenser et à corriger les vulnérabilités les plus critiques. L'ENISA est particulièrement bien placée pour soutenir cette transition du cyberécosystème de l'UE à l'ère de l'IA.

3.1. Appliquer les fondamentaux et la préparation de l'UE en matière de cybersécurité

Dans ce nouveau paysage des technologies et de la sécurité, **les fondamentaux et la préparation en matière de cybersécurité sont plus importants que jamais**, et les outils et instruments existants de l'UE en matière de cybersécurité doivent être pleinement utilisés.

Le cadre réglementaire de l'UE en matière de cybersécurité, notamment la **directive SRI 2[26] et le règlement sur la résilience opérationnelle numérique du secteur financier**, fournit une base solide pour la préparation des infrastructures critiques à tous les types de risques en matière de cybersécurité, y compris ceux liés à l'IA. Ces règles doivent donc être transposées et mises en œuvre d'urgence par les États membres. En outre, les États membres doivent tenir compte des risques liés à l'IA avancée dans leurs travaux de surveillance. De même, les opérateurs des secteurs critiques et les entités financières devraient revoir leur cadre de gestion des risques et l'adapter aux nouvelles réalités, en anticipant les cyberattaques utilisant l'IA à une fréquence et à une échelle plus élevées, et raccourcir le délai de correction en accélérant la cadence de correction et en se donnant les moyens d'appliquer rapidement des correctifs sur des systèmes complexes.

Afin de renforcer encore la préparation, les entités devraient appliquer systématiquement **des mesures de base en matière de cyberhygiène** et mettre en œuvre un renforcement des réseaux et des systèmes (y compris au moyen d'approches «confiance zéro», le cas échéant). Elles devraient également commencer à **utiliser les capacités d'IA déjà disponibles**, y compris au moyen de modèles à source ouverte, afin de détecter les vulnérabilités et d'améliorer la détection et la prévention des cyberattaques. **Les entités de l'Union**, avec le soutien du CERT-UE et les orientations du conseil interinstitutionnel de cybersécurité (IICB), peuvent montrer l'exemple à cet égard pour renforcer la posture cyber globale de l'Union, conformément au règlement sur la cybersécurité des entités de l'Union[27]. Les États membres sont également vivement encouragés à tirer pleinement parti des possibilités de conversion offertes par la **réserve de cybersécurité de l'Union** afin de renforcer la résilience face aux cybermenaces liées à l'IA, notamment par le biais d'analyses de vulnérabilité, de tests d'intrusion automatisés

[26] La directive SRI 2 définit la base de référence pour la gestion des risques en matière de cybersécurité, en exigeant des entités essentielles et importantes actives dans 18 secteurs critiques qu'elles protègent leurs réseaux et systèmes d'information et qu'elles préviennent et réduisent au minimum l'impact des incidents.
[27] Règlement (UE, Euratom) 2023/2841.

et de la surveillance des risques, avec un accompagnement pour la mise en œuvre des recommandations de correctifs.

En outre, comme indiqué dans le **règlement sur la cyberrésilience**, qui sera pleinement applicable à partir du 11 décembre 2027, les pratiques de développement sécurisé dès la conception, la gestion systématique des vulnérabilités, les correctifs en temps utile et les pratiques de codage sécurisé, y compris les approches qui éliminent des classes entières de vulnérabilités, telles que le développement de logiciels sans risque pour les mémoires, restent essentielles. Les risques de cybersécurité spécifiques à l'IA, y compris l'empoisonnement de données et de modèle, les attaques contradictoires et les attaques par injection de prompt, doivent également être soigneusement évalués et atténués conformément aux dispositions pertinentes du règlement sur l'IA.

Afin de soutenir ces efforts, l'**ENISA**, en coopération avec les autorités européennes de surveillance et d'autres entités compétentes de l'Union, mettra à disposition et tiendra à jour **des orientations, des recommandations, des conseils et des bonnes pratiques appropriés afin de rester protégée contre les menaces fondées sur l'IA[28] et de favoriser l'intégration sécurisée des outils d'IA dans les opérations de cybersécurité**. Ces orientations et conseils devraient également tenir compte des besoins des PME, qui sont les plus vulnérables aux attaques. Le cas échéant, ces efforts pourraient être renforcés et enrichis par des initiatives sectorielles et des mécanismes de coopération dans des domaines tels que la finance, les transports, l'énergie, l'agroalimentaire, les soins de santé[29] et l'espace.

Étant donné que les technologies et les risques associés continueront d'évoluer, **une connaissance collective de la situation et un partage structuré des informations sur les menaces de cybersécurité liées à l'IA**, par le biais des réseaux pertinents de l'Union, tant au niveau horizontal que sectoriel, joueront un rôle déterminant dans le renforcement de cette connaissance de la situation. L'ENISA devrait étudier les moyens de favoriser la coopération avec les fournisseurs d'IA afin d'améliorer le partage de renseignements sur les menaces.

De même, les États membres devraient tirer parti des structures existantes au niveau de l'Union dans le domaine de la cybersécurité pour **évaluer la préparation des infrastructures critiques**, en collaborant en particulier au sein du groupe de coopération SRI et, le cas échéant, en coopération avec le Comité IA institué en vertu du règlement sur l'IA.

3.2. Accélérer le processus correctif: améliorer la gestion des vulnérabilités pour une détection à la vitesse de l'IA

Le défi immédiat pour la posture cyber de l'UE consiste à **remédier aux vulnérabilités existantes avant qu'elles ne puissent être exploitées à grande échelle**. Étant donné que l'IA réduit le temps nécessaire aux acteurs malveillants pour exploiter les vulnérabilités, les entités concernées doivent également accélérer leur capacité à analyser, hiérarchiser, corriger et déployer des solutions suffisamment rapidement pour empêcher l'exploitation des vulnérabilités.

Les processus existants de gestion des vulnérabilités doivent être mis à niveau pour être efficaces à l'ère de la découverte assistée par l'IA. L'ENISA devrait veiller à ce que

[28] Un exemple de ces conseils est l'article du blog CERT EU: *AI is changing the economics of vulnerability discovery. Defenders should adapt now* (L'IA modifie l'économie de la découverte des vulnérabilités. Les défenseurs devraient s'adapter dès maintenant), daté du 21 avril 2026.

[29] Plan d'action européen sur la cybersécurité des hôpitaux et des prestataires de soins de santé: COM(2025)10 final.

l'infrastructure et les services européens de gestion des vulnérabilités, y compris la base de données européenne des vulnérabilités (EUVD) et la plateforme unique de signalement au titre du règlement sur la cyberrésilience, soient adaptés à l'ère de la détection des vulnérabilités assistée par l'IA et, conjointement avec les États membres, renforcent l'interopérabilité entre les plateformes et bases de données de l'UE, nationales et mondiales sur les vulnérabilités.

À mesure que le nombre de rapports de vulnérabilité augmente, les fabricants doivent décider quelles sont les lacunes à corriger en premier lieu sur l'ensemble des lignes de produits, tandis que les utilisateurs, en particulier les entités essentielles et critiques importantes, doivent déterminer quelles mises à jour doivent être déployées en premier lieu, souvent avec des ressources limitées. Les organisations doivent pouvoir s'appuyer sur des orientations claires à l'échelle de l'UE, fondées sur les risques et alignées sur le règlement sur la cyberrésilience et la directive SRI 2, afin de contribuer à réduire les risques là où ils sont les plus élevés.

Dans le cadre des obligations qui leur incombent en vertu de la directive SRI 2, **les États membres devraient également mettre à jour leurs politiques nationales de divulgation coordonnée des vulnérabilités** afin de lutter contre l'exploitation assistée par l'IA. Le groupe de coopération SRI devrait réviser ses orientations sur la mise en œuvre des politiques de divulgation coordonnée des vulnérabilités, et l'UE devrait également examiner si les normes ISO/CEI qui sous-tendent les cadres en matière de divulgation coordonnée des vulnérabilités restent adaptées à leur finalité compte tenu des menaces actuelles. La coopération internationale est également essentielle à cet égard, étant donné que ces pratiques sont façonnées à l'échelle mondiale.

Enfin, la sécurisation des infrastructures critiques ne se résume pas à la divulgation de vulnérabilités ou à la publication de solutions. Le plus grand défi consiste à **appliquer les solutions**. À mesure que l'IA accélère la détection des vulnérabilités, le goulet d'étranglement lié au déploiement des correctifs prend de plus en plus d'ampleur. Avec le soutien de l'ENISA, les États membres devraient tirer parti des réseaux existants, tels que le groupe de coopération SRI, pour relever ce défi, qui est de la plus haute urgence.

3.3. Mise en pratique: déterminer ce qui compte le plus

L'UE ne doit pas se contenter de développer les connaissances sur la manière dont l'IA peut renforcer la cyberrésilience; elle doit **appliquer ces connaissances là où le besoin est le plus urgent**. Le défi consiste donc non seulement à trouver plus rapidement les vulnérabilités, mais aussi à les analyser, à les corriger et à coordonner le déploiement à grande échelle. **Les logiciels libres critiques constituent le domaine par excellence où il convient d'agir en priorité**, en raison de leur forte présence dans les secteurs des infrastructures critiques. Selon certaines informations, 98 % de la base de codes totale contient des sources ouvertes, le secteur des infrastructures critiques représentant en moyenne environ 80 % des bases de codes à haut risque ou à risque critique[30].

La **stratégie de l'UE en matière d'open source**[31], publiée dans le cadre du paquet «souveraineté technologique», comprend une série de mesures visant à accroître la sécurité et à soutenir le maintien des composants à source ouverte critiques. Dans ce contexte, la

[30] Blackduck, 2026 *Open Source Security and Risk Analysis Report* (Rapport sur la sécurité et l'analyse des risques liés aux sources ouvertes): par exemple, pour l'aérospatiale, l'aviation, l'automobile, les transports et la logistique: 87 %; la fabrication: 88 %; la santé: 88 %; l'énergie: 89 %; internet et les infrastructures logicielles: 80 %.

[31] COM(2026) 503 final.

Commission collaborera avec l'ENISA, les États membres[32] et les communautés à source ouverte, afin de piloter certaines actions spécifiquement ciblées sur le cyberespace et l'IA.

L'ENISA, en coopération avec la Commission, les États membres et les communautés à source ouverte, accélérera la cartographie des composants à source ouverte critiques prévue dans le cadre de la stratégie et, sur la base d'une liste préliminaire fondée sur des critères convenus, **pilotera une campagne pour la résilience des composants à source ouverte critiques** pertinents pour les infrastructures critiques. Les résultats de la campagne serviront de base à la mise en œuvre de l'instrument de maintenance à source ouverte. La campagne consistera en un programme de parrainage volontaire visant à mettre en relation des projets à source ouverte avec des organisations disposées à travailler en partenariat étroit avec les responsables de la maintenance des projets afin de soutenir leur maintenance et leur sécurité. Parmi les promoteurs peuvent figurer les États membres, des entités de l'Union telles que le CERT-EU, des exploitants d'infrastructures critiques, des fabricants et d'autres entités publiques ou privées en mesure d'apporter leur soutien, par exemple en mettant à la disposition des responsables de projets à source ouverte du personnel qualifié, ou encore des modèles et des outils d'IA. Les États membres et les autres utilisateurs éligibles peuvent bénéficier du soutien de fournisseurs privés de confiance au sein de la **réserve de cybersécurité de l'Union** pour l'analyse des vulnérabilités liées à la dépendance à l'égard des sources ouvertes dans les infrastructures critiques. En outre, l'ENISA élaborera un **catalogue de services fondés sur l'IA**, visant à soutenir la correction des vulnérabilités de source ouverte et leur remédiation.

Les responsables de la maintenance à source ouverte pourront bénéficier du programme de parrainage et du catalogue de services afin d'accroître la rapidité et l'efficacité de leur travail et de réduire les cyberrisques, accélérés par l'évolution des modèles d'IA. L'initiative renforcera la gouvernance et les flux de travail existants en matière de source ouverte et constituera un terrain d'expérimentation pour l'action plus large de l'Europe en faveur de la remédiation assistée par l'IA, ce qui renforcera encore le savoir-faire opérationnel de l'Union. Elle contribuera à renforcer la cyberrésilience dans tous les secteurs, y compris les infrastructures critiques et les PME. Une première campagne pilote sera lancée en 2026, en vue d'une nouvelle mise à l'échelle, si elle s'avère fructueuse, y compris dans le cadre de la stratégie en matière d'open source.

Actions clés

- **Action clé nº 4 — L'ENISA, en coopération avec les entités compétentes de l'Union, publiera des orientations, des recommandations, des conseils et des bonnes pratiques sur la protection contre les menaces assistées par l'IA et pour l'intégration sécurisée de l'IA dans les opérations de cybersécurité (à partir du T3 2026)**
- **Action clé nº 5 — La Commission, les États membres, l'ENISA et l'industrie coopéreront en vue de rendre les pratiques et outils de gestion des vulnérabilités existants adaptés à l'ère de l'IA (à partir du T3 2026)**
- **Action clé nº 6 — L'ENISA, en coopération avec la Commission, les États membres, les communautés de logiciel libre, les entités de l'Union et l'industrie, lancera un premier projet pilote de campagne sur la résilience des sources ouvertes critiques afin d'accélérer les correctifs, notamment en tirant parti de l'IA (T4 2026)**

[32] En particulier, s'il y a lieu, en coordination avec le consortium pour une infrastructure numérique européenne (EDIC) sur les communs numériques.

4. Pilier 3: Renforcer les capacités européennes en matière d'IA pour le cyberespace

Dans un contexte où les cyberopérations défensives et offensives reposent de plus en plus sur une IA avancée, la capacité à développer et à déployer des solutions de cybersécurité fondées sur l'IA devient un catalyseur stratégique de la cyberrésilience et de la souveraineté. En particulier, pour les cas d'utilisation sensibles, l'UE doit pouvoir s'appuyer sur des capacités souveraines en matière d'IA qui répondent aux besoins en matière de sécurité, y compris dans le domaine de la défense. L'UE doit désormais permettre aux fournisseurs européens, y compris aux innovateurs de rupture, de développer, de déployer et d'étendre cette IA avancée en Europe. En complément de sa stratégie d'investissement dans les domaines de la cybersécurité et de l'IA, l'UE doit mobiliser son écosystème technologique afin de répondre aux besoins opérationnels les plus urgents en matière de cybersécurité, d'encourager les investissements dans le développement et l'adoption de capacités européennes de pointe en matière d'IA, et de développer les compétences nécessaires à leur déploiement dans tous les secteurs.

4.1. Stimuler l'écosystème européen autour de solutions de cybersécurité fondées sur l'IA

Étant donné que l'IA est déjà exploitée à des fins malveillantes, les organisations doivent se mobiliser plus rapidement que les attaquants pour déployer les solutions de cybersécurité disponibles utilisant l'IA afin de protéger les infrastructures critiques dans tous les secteurs. L'UE doit encourager le marché européen à mettre ces outils à disposition à la vitesse et à l'échelle nécessaires et encourager leur adoption dans nos infrastructures critiques.

Des investissements importants sont déjà réalisés par l'UE pour **soutenir la recherche et le développement de technologies de cybersécurité avancées locales fondées sur l'IA** et pour la cybersécurité de l'IA, avec notamment 200 millions d'EUR d'ici à la fin de l'actuel cadre financier pluriannuel au titre du programme Horizon Europe et du programme pour une Europe numérique. Par exemple, trois projets phares d'Horizon Europe seront lancés à la fin de 2026 afin de soutenir le développement, l'entraînement et les essais de l'IA pour les capacités de surveillance, de détection, de réaction et d'autoréparation dans les processus et systèmes numériques contre les cyberattaques, y compris les attaques par exemples contradictoires, ainsi que le développement d'outils et de technologies d'IA générative pour la surveillance continue, la conformité et la rémédiation automatisée. L'UE finance également l'ensemble du cycle des capacités en matière d'IA en ce qui concerne les services répressifs, de la recherche aux essais, à la validation et au déploiement opérationnel par l'intermédiaire d'Horizon Europe, du Fonds pour la sécurité intérieure, du programme pour une Europe numérique et du CERIS. De même, l'UE investit par l'intermédiaire du Conseil européen de l'innovation (CEI), y compris au moyen d'investissements directs du Fonds du CEI, dans des entreprises européennes spécialisées dans la deep tech, la cybersécurité et l'IA, ce qui va s'étendre également, en 2026 et 2027, aux technologies de défense stratégiques et à double usage pertinentes[33]. Plus précisément, d'ici à la fin de 2026, la Commission permettra aux investissements du Fonds du CEI dans des entreprises technologiques du cyberespace et de l'IA, qui s'élèvent à 100 millions d'EUR, d'être investis dans des start-up et des scale-up stratégiques dans le domaine des technologies de défense et de poursuivre un soutien similaire en 2027. Le Fonds «Scale-up Europe» réalisera ses premiers investissements dans des entreprises stratégiques en phase de croissance dès 2026. En s'appuyant sur la stratégie numérique internationale de l'Union, l'UE

[33] Le Fonds du CEI — Conseil européen de l'innovation — Commission européenne.

et les États membres tireront également parti de l'offre de l'UE pour les entreprises technologiques afin de soutenir le déploiement de l'IA et des solutions logicielles.

En complément de ces investissements, l'Union devrait s'efforcer d'**accélérer encore le partage de connaissances sur les capacités avancées de cybersécurité fondées sur l'IA pour lutter contre les cyberattaques à grande échelle utilisant l'IA**. Aujourd'hui, l'UE dispose d'un riche écosystème et d'une base de connaissances dans l'ensemble du monde universitaire, de l'industrie et des pouvoirs publics, mais les solutions fondées sur l'IA pour la cybersécurité restent fragmentées, insuffisamment testées dans des environnements opérationnels et loin d'être déployées à grande échelle dans tous les secteurs[34]. La remédiation automatisée des vulnérabilités, qui est l'un des principaux goulets d'étranglement opérationnels en matière de cybersécurité à l'ère de l'IA, en est un exemple: aujourd'hui, la détection des vulnérabilités fondée sur l'IA progresse plus rapidement que la remédiation assistée par l'IA, ce qui crée un déséquilibre structurel au profit des attaquants. En réponse aux appels lancés pour faire face aux menaces posées par l'IA offensive[35], la Commission, avec le soutien du Centre de compétences européen en matière de cybersécurité (CECC) et en coopération avec l'ENISA, lancera donc **un grand défi spécifique de l'Union sur la remédiation aux vulnérabilités assistée par l'IA**. Réunissant des entreprises européennes de cybersécurité et d'IA, des organismes de recherche, des opérateurs d'infrastructures critiques et des communautés de logiciel libre autour de cette mission commune, le grand défi soutiendra le développement d'un système d'IA capable d'aider les équipes de cybersécurité tout au long du cycle de vie de la remédiation. En reliant la recherche et le déploiement, le grand défi permettra de tester des solutions prometteuses dans des environnements opérationnels réalistes et, en fin de compte, de les mettre à la disposition d'organisations dans toute l'Europe, contribuant ainsi à réduire les goulets d'étranglement opérationnels qui empêchent une remédiation rapide. Les États membres intéressés seront invités à soutenir ces efforts de partage des connaissances.

4.2. Renforcer les capacités de pointe européennes

Si les modèles et systèmes d'IA existants dotés de capacités en matière de cybersécurité offrent déjà des possibilités importantes pour les opérations de cybersécurité, les cybercapacités fondées sur l'IA d'avant-garde ont également des implications majeures pour la souveraineté technologique, la sécurité et la défense de l'Europe. Par conséquent, l'UE doit **développer ses propres capacités souveraines en matière d'IA d'avant-garde à usage général** afin d'atténuer le risque de nouvelles dépendances à l'égard de ce qui est désormais devenu un atout stratégique critique, le double usage potentiel de l'IA d'avant-garde prenant de plus en plus d'importance et ne se limitant plus du tout au domaine de la cybersécurité. Il s'agit d'un défi intersectoriel plus large pour notre économie et notre société, que la Commission continuera de suivre de près et de relever au fur et à mesure de son évolution.

La Commission a déjà pris des mesures concrètes pour aider les principaux acteurs européens à repousser les limites des capacités d'IA.

- Récemment, la Commission a désigné le lauréat du grand défi de l'IA d'avant-garde, qui bénéficiera d'un accès à la capacité de calcul d'EuroHPC afin de contribuer au développement d'un modèle européen d'IA avancée à code source ouvert[36].

[34] Public Letter of Support for a European Grand Challenge in AI and Security (Lettre publique de soutien à un grand défi européen en matière d'IA et de sécurité) - Google Docs.
[35] Idem.
[36] La Commission sélectionne le consortium EUROPA comme lauréat du grand défi de l'IA d'avant-garde, un projet visant à construire un modèle européen d'IA d'avant-garde à source ouverte dans les 24 langues de l'Union | Bâtir l'avenir numérique de l'Europe.

- Dans le cadre de l'initiative RAISE (Resource for AI Science in Europe), la Commission finance un réseau de laboratoires d'IA d'avant-garde afin de faire progresser la recherche dans ce domaine également.
- Dans le cadre d'Horizon Europe, la Commission finance des activités visant à développer une IA d'avant-garde sûre et sécurisée.
- La Commission continuera de collaborer avec la France et l'Allemagne pour mettre en place un effort collaboratif (l'«initiative européenne sur l'IA d'avant-garde») visant à promouvoir la recherche et l'innovation, à attirer les talents et à faciliter l'essaimage.
- La Commission bénéficie de conseils techniques par l'intermédiaire du forum sur l'IA d'avant-garde[37].

Ces premières étapes jettent des bases importantes. Toutefois, **un changement de paradigme en matière d'ambition et de ressources est nécessaire** pour transformer les aspirations de l'Europe en matière d'IA d'avant-garde en une capacité souveraine et un avantage concurrentiel durables. Compte tenu de l'ampleur sans précédent des ressources nécessaires au développement de l'IA d'avant-garde, les projets d'avant-garde nécessitent une approche collaborative à l'échelle de l'Union. L'acte législatif proposé sur le développement de l'informatique en nuage et de l'IA les considère comme des projets prioritaires et alloue les ressources de calcul de l'Union en complément de celles allouées par les États membres. Il faut tirer parti **des fabriques d'IA existantes et des futures gigafabriques d'IA** et les intégrer au sein d'une infrastructure européenne souveraine pour l'IA et la cybersécurité, comprenant la puissance de calcul, les données et la connectivité, et positionner l'UE comme un continent de l'IA de premier plan. Cette connectivité est une condition préalable au partage fiable d'ensembles de données prêts pour l'IA, à la fédération de ressources par-delà les frontières, au fonctionnement sécurisé d'environnements contrôlés et au développement, aux essais, au déploiement et à l'accès à des cybercapacités fondées sur l'IA à la fois solides, fiables et hautement performantes. Les fabriques d'IA pertinentes axées sur le cyberespace devraient faciliter l'accès à des ensembles de données de haute qualité prêts pour l'IA, allant des données publiques aux données industrielles[38] et de cybersécurité sensibles, au moyen de mécanismes de partage de données fiables, sécurisés et résilients, et soutenir le développement et la validation de modèles d'IA dans un environnement contrôlé, responsable et vérifiable par l'intermédiaire de leurs laboratoires de données.

La Commission soutiendra également le développement de cybercapacités européennes souveraines en matière d'IA, y compris pour la défense, par l'intermédiaire du Fonds européen pour la compétitivité, en veillant à ce que l'Europe soit mieux équipée pour protéger ses intérêts stratégiques et réduire les dépendances critiques. Dans ce contexte, la Commission mettra en place un groupe de travail spécifique avec les agences concernées, y compris l'ENISA et l'Agence européenne de défense (AED), et les États membres afin de faire face aux risques pour la sécurité liés au déploiement de modèles d'IA d'avant-garde dans les systèmes critiques pour la défense et les systèmes critiques à double usage.

Le développement de capacités d'avant-garde souveraines entraînera **des besoins d'investissement de centaines de milliards d'euros** qui ne pourront être que partiellement couverts par les finances publiques. Il est donc urgent d'attirer de grands volumes d'investissements privés, en particulier du capital-risque et des fonds propres, afin de mettre au point et de développer des solutions européennes innovantes. Si elle ne dispose pas de puissance de calcul, de modèles et d'infrastructure de données, l'Europe restera inévitablement

[37] Commission seeks experts for forum on Frontier AI | Shaping Europe's digital future (La Commission recherche des experts pour le forum sur l'IA d'avant garde | Bâtir l'avenir numérique de l'Europe).
[38] Sous réserve du respect de la législation applicable, y compris le droit de la concurrence de l'UE.

un utilisateur vulnérable de systèmes d'IA d'avant-garde fabriqués ailleurs, qui pourraient être soudainement désactivés, ce qui aura d'énormes répercussions sur le plan économique et de la (cyber) sécurité. Et si le coût de la construction de sa propre capacité d'IA d'avant-garde peut être très élevé pour l'Europe, le coût de la non-construction de cette capacité peut être encore plus élevé et augmenter chaque année à mesure que l'écart en matière de capacités d'IA se creuse.

Avec son paquet «souveraineté technologique» du 3 juin 2026, la Commission a lancé **des consultations avec les États membres, le groupe BEI et d'autres parties prenantes clés sur la proposition de création d'une nouvelle capacité européenne en fonds propres** pour la gestion d'un portefeuille d'investissements en fonds propres à grande échelle dans des technologies et infrastructures avancées essentielles à notre souveraineté technologique, y compris les technologies numériques telles que l'IA d'avant-garde, mais aussi les technologies énergétiques propres, les biotechnologies et, potentiellement, les technologies de défense. Le principal avantage de ce mécanisme serait de créer un «point d'ancrage de co-investissement» en capitaux propres, dont le besoin se fait cruellement sentir, afin d'attirer d'importants volumes d'investissements privés, en agissant en synergie avec des instruments financiers déjà existants au niveau de l'UE, tels que le fonds «Scale-up Europe», ou en y investissant. Ce nouveau mécanisme de fonds propres pour les technologies stratégiques changerait la donne en apportant une réponse à ce dernier appel à d'importants investissements de l'UE dans l'IA d'avant-garde. En ce qui concerne l'instrument InvestEU du Fonds, ce mécanisme pourrait devenir un acteur majeur dans le domaine des investissements stratégiques en capitaux propres pour des montants importants dans les technologies de pointe et les infrastructures.

4.3.Renforcer les compétences en matière de cybersécurité à l'ère de l'IA

La réussite de l'Europe ne dépendra pas exclusivement de la technologie. La capacité à déployer une IA avancée de manière efficace et sécurisée dans les opérations de cybersécurité dépendra également de la **disponibilité de professionnels qualifiés capables de comprendre et d'utiliser en toute sécurité des modèles d'IA dotés de cybercapacités avancées**, ainsi que de gérer les risques spécifiques à l'IA. Étant donné que les équipes de cybersécurité intégreront de plus en plus l'IA avancée, cela pourrait encore aggraver le déficit existant de compétences en matière de cybersécurité. L'UE doit donc renforcer sa main-d'œuvre dans le domaine de la cybersécurité, en la dotant des compétences appropriées en matière d'IA pour la cybersécurité.

L'**académie européenne des compétences en matière de cybersécurité**, qui réunit l'industrie, les prestataires de formation et les établissements universitaires autour d'engagements et de partenariats concrets en matière de formation à la cybersécurité, fournit le cadre approprié pour répondre à ce besoin au niveau de l'Union. La Commission, en collaboration avec les États membres, tirera parti de cet écosystème en expansion pour lancer une action spécifique dans le cadre de l'académie des compétences en matière de cybersécurité afin d'élaborer des programmes de formation permettant aux professionnels de la cybersécurité d'utiliser les outils d'IA. Elle devrait également étudier les synergies potentielles avec la future académie des compétences en matière d'IA. En outre, l'ENISA mettra à jour le **cadre européen des compétences en matière de cybersécurité**, en intégrant les compétences liées à l'IA dans les profils professionnels existants et en définissant de nouveaux rôles si nécessaire.

Actions clés:

- **Action clé nº 7 — La Commission, avec le soutien du Centre de compétences européen en matière de cybersécurité et en coopération avec l'ENISA, lancera un grand défi de l'UE visant à contribuer à l'expansion des solutions européennes de cybersécurité fondées sur l'IA (T4 2026).**

- **Action clé nº 8 — La <u>Commission, conjointement avec les États membres</u>, s'efforcera de mettre à disposition l'accès à la capacité informatique des fabriques d'IA pour tester, entraîner et déployer des modèles d'IA avancés et d'avant-garde disponibles en vue de renforcer la cyberrésilience sur des infrastructures informatiques souveraines.**
- **Action clé nº 9 — La <u>Commission collaborera avec les États membres et l'industrie</u> (dans le cadre de l'académie des compétences en matière de cybersécurité) pour élaborer des modules de formation à l'intention des professionnels de la cybersécurité sur l'utilisation de l'IA pour la cybersécurité (T4 2026).**

5. Travailler avec des partenaires partageant les mêmes valeurs en vue d'une approche mondiale de la cybersécurité à l'ère de l'IA

Les implications de l'IA en matière de cybersécurité sont intrinsèquement mondiales, étant donné que les modèles et systèmes d'IA, les chaînes d'approvisionnement logicielles et les écosystèmes open source opèrent par-delà les frontières. La publication d'un modèle d'IA doté de cybercapacités développées sur un territoire donné peut avoir des conséquences importantes sur la sécurité des infrastructures critiques et des entreprises dans le monde entier. Les gouvernements, les organisations internationales et l'industrie sont donc confrontés à **un défi commun, et la coopération internationale est essentielle** pour éviter la fragmentation, promouvoir l'interopérabilité entre les partenaires de confiance et mettre en commun les efforts visant à atténuer les risques en matière de cybersécurité associés à l'IA.

L'UE devrait jouer un rôle de premier plan dans l'élaboration de pratiques mondiales en matière d'IA digne de confiance et de cyberrésilience en tirant parti du **cadre réglementaire de l'Union en matière d'IA et de cybersécurité**. En particulier, une coopération plus étroite entre les partenaires partageant les mêmes valeurs est nécessaire pour veiller à ce que les capacités d'IA d'avant-garde restent à la fois sûres et disponibles pour des utilisations de confiance, tout en prévenant leur utilisation abusive par des acteurs malveillants. Le présent plan d'action invite également nos partenaires internationaux à se joindre aux efforts déployés pour amplifier l'impact des mesures proposées sur la sécurité de l'IA et la cyberrésilience.

En particulier, la Commission poursuivra ces objectifs dans les enceintes bilatérales et multilatérales. Elle continuera de participer activement au **G7 pour promouvoir son approche**, notamment par l'intermédiaire du **groupe de travail sur la cybersécurité et du groupe de travail numérique et technologique**, afin de soutenir les activités visant à parvenir à une compréhension commune des risques en matière de cybersécurité découlant des capacités avancées en matière d'IA. La Commission encouragera la coopération du G7 en matière de normes et d'évaluation de ces modèles. Elle invite également les membres du G7 et d'autres partenaires internationaux à participer aux travaux destinés à contribuer à la sécurité des logiciels libres et à coopérer en vue d'adapter les pratiques de gestion des vulnérabilités. L'UE continuera également de participer aux travaux des Nations unies.

Sur le plan bilatéral, l'UE approfondira les échanges avec les pays partenaires sur l'IA avancée et la cybersécurité, y compris au moyen de partenariats numériques, de dialogues numériques ou de dialogues sur le cyberespace, et accordera la priorité à l'évaluation des modèles, à la protection des infrastructures critiques, à l'atténuation des vulnérabilités et à l'amélioration de la cyberrésilience en tant que domaines de coopération essentiels, le cas échéant.

Par ailleurs, le **réseau pour la mesure, l'évaluation et la recherche en matière d'IA avancée, coordonné par l'institut britannique de sécurité de l'IA (AISI)** et en étroite collaboration avec les instituts chargés de la sûreté et de la sécurité des pays partenaires ainsi qu'avec **le Bureau de l'IA de la Commission**, constitue une plateforme importante pour l'élaboration de méthodologies communes d'évaluation des modèles d'IA d'avant-garde, l'échange de bonnes pratiques et le soutien à une coopération internationale fiable en matière de sûreté et de sécurité de l'IA.

La Commission encouragera également un dialogue structuré entre les gouvernements et les principaux développeurs d'IA d'avant-garde afin de promouvoir des approches communes en matière de sécurité, d'évaluation et de déploiement responsable de l'IA d'avant-garde.

Enfin, compte tenu des implications mentionnées pour la sécurité européenne et nationale, l'UE renforcera les échanges existants avec l'**OTAN** sur les possibilités et les risques associés aux capacités d'IA d'avant-garde dans le domaine du cyberespace, notamment en tirant parti du futur centre d'excellence de l'OTAN en matière d'intelligence artificielle.

6. Conclusion

Le présent plan d'action marque la poursuite d'un effort européen soutenu et coordonné. Étant donné que le développement de capacités avancées en matière d'IA continuera de s'accélérer, et qu'il s'accompagnera de l'apparition de nouvelles possibilités et de nouveaux risques, la Commission évaluera régulièrement la mise en œuvre du plan d'action et adaptera les actions si nécessaire, afin de veiller à ce qu'il contribue efficacement au développement d'un écosystème européen sûr et résilient à l'ère de l'IA.