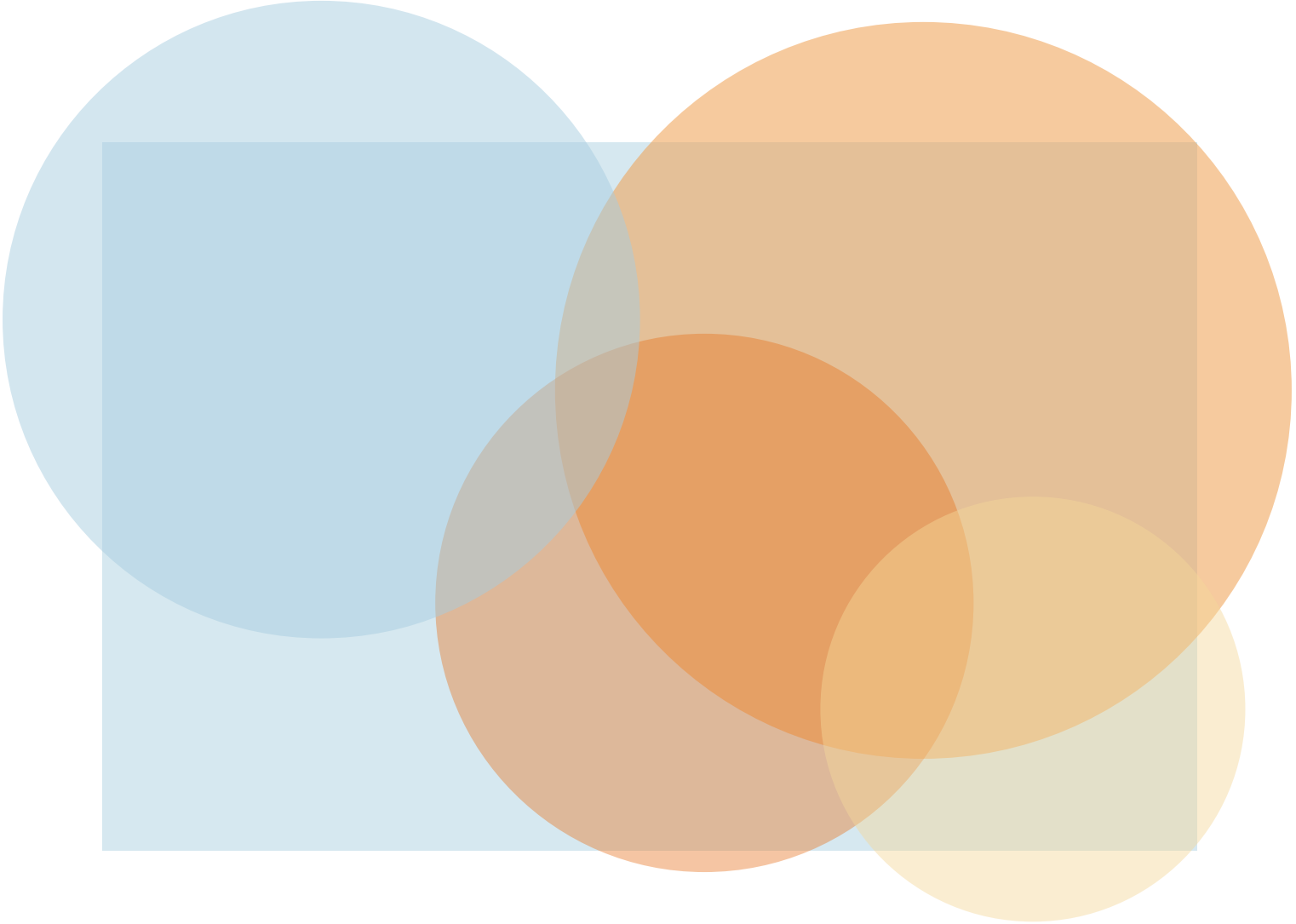

Gouvernance Démocratique de l'IA de Frontière :

Un plan directeur pour un cadre fédéral

2 juin 2026

OpenAI

Les pays qui parviendront à exploiter l'intelligence artificielle façonneront la trajectoire scientifique, économique et géopolitique du XXIe siècle. L'IA peut accélérer la découverte scientifique, élargir les opportunités économiques, renforcer la sécurité nationale et contribuer à résoudre des problèmes qui semblaient autrefois insolubles. Dans le même temps, des systèmes d'IA de plus en plus capables commencent à manifester des aptitudes suscitant des inquiétudes concernant les cyberattaques, les utilisations biologiques malveillantes, l'autonomie, l'alignement et d'autres menaces pour la sécurité nationale. Nous observons également les premiers signes d'auto-amélioration récursive (AMR) dans les systèmes actuels : le développement de l'IA est lui-même accéléré par l'IA. Nous nous attendons à ce que cela intensifie les pressions concurrentielles entre développeurs et nations, et crée des défis de gouvernance auxquels les institutions existantes ne sont pas préparées. À mesure que l'AMR émerge, les sociétés auront besoin de moyens pour orienter la trajectoire du développement de l'IA et s'assurer qu'il sert les intérêts humains.

Les démocraties sont particulièrement bien placées pour garantir que l'IA puissante est développée de manière responsable, en associant l'innovation à la responsabilité publique, à la transparence, à une surveillance indépendante et à la capacité de rectifier le tir grâce au gouvernement représentatif. Mais une gouvernance efficace nécessite une visibilité sur l'évolution des capacités de frontière, sur l'impact de l'IA sur la sécurité nationale et sur la nécessité éventuelle de garanties nationales supplémentaires, d'une coordination internationale ou d'autres mesures de précaution. Construire cette compréhension nécessite de créer des institutions capables d'évaluer l'IA de frontière, de surveiller l'évolution des capacités et de fournir aux décideurs des informations fiables.

À mesure que l'IA gagne en importance, les gouvernements démocratiques — et non les entreprises privées agissant seules — doivent in fine déterminer les règles, les garanties et les mécanismes de responsabilité. Nous estimons que les décisions relatives au rythme de l'innovation en IA ne doivent pas être laissées à un seul laboratoire, à une seule entreprise ou à un groupe d'intérêts particulier. Ces choix doivent au contraire être pris par des processus démocratiques et éclairés par une compréhension solide des capacités de frontière, des mesures d'atténuation des risques, de la résilience sociétale et des considérations géopolitiques.

Dans ce contexte, nous estimons que les États-Unis sont particulièrement bien placés pour contribuer à façonner la gouvernance mondiale. Le gouvernement fédéral américain dispose de capacités uniques qu'aucune entreprise privée ne peut reproduire, notamment l'accès aux renseignements classifiés, l'expertise en cybersécurité et en défense contre les menaces chimiques, biologiques, radiologiques et nucléaires (CBRN), des environnements informatiques sécurisés et la capacité de coordonner avec des partenaires internationaux. Par ailleurs, de nombreux éléments constitutifs d'un cadre de sécurité de frontière existent déjà aux États-Unis.

Les développeurs de frontière ont déjà adopté les engagements volontaires de la Maison Blanche et se sont associés au Center for AI Standards and Innovation (CAISI) pour des évaluations préalables au déploiement. Des entreprises américaines ont également coordonné leurs actions à l'échelle internationale, en adhérant au Code de conduite de l'AI Act de l'Union européenne et en s'associant à l'AI Security Institute du Royaume-Uni. Des États ont commencé à développer des approches harmonisées de la gouvernance de l'IA de frontière, notamment le SB 53 de Californie, le RAISE Act de New York et le SB 315 de l'Illinois, et le récent décret exécutif de la Maison Blanche sur la

promotion de l'innovation et de la sécurité de l'IA avancée constitue un pas important en avant. Le gouvernement fédéral américain doit désormais s'appuyer sur cette base et créer un cadre fédéral durable, capable d'évoluer avec la technologie elle-même.

Si l'intelligence artificielle générale doit profiter à toute l'humanité, le monde a besoin de plus que de simples engagements volontaires, de politiques d'entreprises individuelles et d'interventions réglementaires isolées. Il a besoin de cadres juridiques harmonisés et d'institutions durables capables de s'adapter à l'avancement technologique. Ce cadre doit :

- **Traiter les risques de frontière pour la sécurité nationale et la sécurité publique.** L'objectif premier de tout cadre de sécurité de frontière doit être d'atténuer les risques les plus graves posés par les systèmes d'IA avancés à usage général. Ceux-ci incluent les risques liés aux menaces cyber et CBRN, à la progression de l'AMR et aux scénarios de perte de contrôle pouvant entraîner des conséquences catastrophiques.
- **Promouvoir la gouvernance démocratique.** Les décisions sur la manière dont la société gère les risques liés à l'IA de frontière doivent être prises par le biais du gouvernement représentatif, et non par des entreprises privées agissant seules. La gouvernance de la sécurité de frontière doit refléter les forces des sociétés libres : transparence, responsabilité publique, surveillance indépendante et primauté du droit.
- **Promouvoir la transparence.** Les gouvernements, les chercheurs, les entreprises et le public ont besoin d'informations fiables sur la manière dont l'IA de frontière est développée, évaluée et déployée. La transparence crée la responsabilité, favorise l'examen indépendant et contribue à garantir que les décisions politiques sont fondées sur des preuves.
- **Protéger l'innovation.** Un cadre de sécurité de frontière doit se concentrer sur les risques aux conséquences les plus graves sans créer de barrières inutiles pour les start-ups, les chercheurs et les développeurs qui construisent sur les capacités de frontière. Il doit réduire les risques sans figer la structure industrielle actuelle dans la loi.
- **Construire des institutions adaptatives.** L'IA progresse rapidement, et la gouvernance de frontière doit être capable d'évoluer avec la technologie. Les décideurs doivent créer des institutions capables d'apprendre, d'expérimenter, d'intégrer de nouvelles preuves et de mettre à jour les normes au fil du temps.

La mise en œuvre d'un cadre de sécurité de frontière nécessitera des actions à plusieurs niveaux de gouvernement, ainsi qu'une coopération internationale. Les États peuvent continuer à servir de laboratoires de la démocratie en développant des lois harmonisées sur la sécurité de frontière. Le gouvernement fédéral américain doit s'appuyer sur cette base en créant des institutions capables d'évaluer les systèmes de frontière, d'identifier les risques émergents et d'éclairer les décisions sur la gouvernance de l'IA. Et à mesure que l'IA gagne en puissance, les décideurs auront besoin d'un plan gouvernemental global pour renforcer la résilience sociétale.

Ce plan directeur définit une stratégie en trois volets pour atteindre ces objectifs : 1) construire un cadre national qui s'appuie sur le consensus émergent reflété dans les lois étatiques sur la sécurité de frontière ; 2) renforcer le CAISI en tant qu'institution principale du gouvernement fédéral américain pour la sécurité de l'IA de frontière ; et 3) mobiliser un plan de résilience plus large à l'échelle du gouvernement pour faire face aux défis de sécurité nationale et de sécurité publique posés par l'IA de frontière.

1. Construire un cadre national par le fédéralisme inversé

Les États ont été de précieux laboratoires pour les politiques d'IA, contribuant à développer et tester de nombreuses idées qui forment désormais un consensus émergent sur la sécurité de frontière. Mais à mesure que l'IA gagne en capacité, les défis de sécurité de frontière les plus importants seront de portée nationale — et souvent internationale. Les décideurs doivent s'appuyer sur cette base et transformer le consensus émergent d'aujourd'hui en un cadre fédéral complet.

Cette approche, que nous appelons *fédéralisme inversé*, a permis aux États de développer et d'affiner en premier des cadres juridiques communs, créant des modèles que le Congrès devrait désormais adopter au niveau national. Le SB 53 de Californie, le RAISE Act de New York et le SB 315 de l'Illinois démontrent qu'un consensus significatif a émergé autour des éléments fondamentaux de la gouvernance de l'IA de frontière. Ces cadres partagent des exigences communes, s'alignent sur les approches internationales et constituent un point de départ pratique pour la législation fédérale.

Les décideurs doivent s'appuyer sur ce consensus en établissant un cadre national de sécurité de frontière qui offre à la fois des garanties solides et une certitude réglementaire. Au minimum, ce cadre doit inclure :

- **Évaluations et atténuations des risques graves.** Les entreprises doivent évaluer les capacités de frontière pour les risques liés aux cybermenaces, aux menaces CBRN, à la perte de contrôle, au désalignement et à la progression vers l'AMR ; mettre en œuvre des garanties appropriées ; et expliquer pourquoi les risques résiduels sont gérés de manière appropriée. Les évaluations et atténuations des risques doivent être adaptées au contexte de déploiement du modèle.
- **Exigences de transparence.** Les entreprises doivent publier des cadres publics de sécurité de frontière et des rapports de transparence décrivant comment elles évaluent les risques graves, mettent en œuvre des garanties, prennent des décisions de déploiement et suivent de manière responsable la progression vers l'AMR, avec les caviardages appropriés pour protéger la sécurité, les secrets commerciaux et les informations propriétaires.
- **Évaluation indépendante et audit.** Les grands développeurs de frontière doivent annuellement faire appel à un tiers indépendant pour auditer la conformité aux exigences de sécurité de frontière, notamment la mise en œuvre du cadre d'IA de frontière du développeur, des contrôles internes et des structures de gouvernance. Ces audits doivent reposer sur un ensemble de normes communes permettant des audits interopérables entre les juridictions.
- **Détection et signalement des incidents de sécurité critiques.** Les entreprises doivent signaler les incidents de sécurité critiques impliquant des modèles déployés, notamment les incidents liés aux risques couverts par le cadre de sécurité de frontière, les comportements dangereux des modèles ou l'accès non autorisé aux poids sensibles des modèles.
- **Exigences de sécurité des poids des modèles.** Les entreprises doivent mettre en œuvre des protections en matière de cybersécurité et contre les menaces internes afin de sécuriser les poids des modèles non publiés.
- **Protections des lanceurs d'alerte.** Les employés doivent être protégés contre les représailles lorsqu'ils signalent des préoccupations crédibles concernant des risques graves, des défaillances de sécurité, des incidents de sécurité critiques ou des violations de la loi à la direction de l'entreprise, aux

régulateurs ou à d'autres autorités compétentes.

- **Mécanismes de responsabilité significatifs.** Les entreprises doivent faire face à des conséquences applicables en cas de non-conformité aux obligations de transparence, de signalement et de sécurité. Les cadres de responsabilité doivent préserver la responsabilité pour les dommages graves et ne doivent pas offrir de refuges sûrs globaux contre la responsabilité.

Les exigences reflétées dans le SB 53, le RAISE et le SB 315 doivent servir de base à la législation fédérale sur la sécurité de frontière — et non de point final. Les décideurs doivent aller au-delà en établissant un rôle formel pour le CAISI, en renforçant les capacités fédérales d'évaluation et en faisant avancer les mesures de résilience plus larges décrites ci-après. Une fois ce cadre fédéral complet en place, les décideurs devraient également préempter les lois étatiques qui cherchent à réglementer les mêmes risques de sécurité de frontière, créant ainsi un cadre national unique qui associe des garanties solides à une certitude réglementaire. Les États doivent continuer à servir de laboratoires de la démocratie dans des domaines au-delà de la sécurité de frontière, notamment la protection de la jeunesse, les politiques énergétiques et environnementales, ainsi que l'éducation et la culture numérique en matière d'IA.

2. Renforcer la sécurité par des institutions solides

À mesure que l'IA gagne en capacité, les États-Unis auront besoin d'une institution de confiance chargée d'évaluer l'IA de frontière, de surveiller les risques émergents et de fournir aux décideurs des conseils techniques indépendants. L'AMR exacerbe la question fondamentale de gouvernance de savoir si les humains peuvent conserver la capacité de comprendre, de guider et d'orienter la trajectoire de l'IA avancée : ce qui en fait potentiellement le défi le plus conséquent de la sécurité de frontière de la décennie à venir. Pourtant, les décideurs ont actuellement une visibilité limitée sur la progression de l'AMR, sur l'adéquation des garanties ou sur les indicateurs qui devraient guider les futures décisions politiques. Une institution comme le CAISI peut contribuer à combler ce fossé.

Les décideurs doivent renforcer le CAISI et en faire la première institution mondiale pour l'évaluation de l'IA de frontière, le développement de normes, la certification d'évaluations indépendantes et la coordination au sein du gouvernement et avec les partenaires internationaux. Sa mission doit être de fournir les informations et les analyses dont les décideurs ont besoin pour prendre des décisions éclairées sur la sécurité nationale, la coordination internationale, l'adéquation des garanties et le rythme du développement de l'IA. Une priorité particulière doit être accordée à la compréhension de la progression vers l'AMR, au développement de mesures fiables de cette progression et à la garantie que les gouvernements disposent des informations nécessaires pour répondre. À mesure que les capacités progressent, le CAISI doit rester flexible et adaptable, avec la capacité d'assumer de nouvelles responsabilités à mesure que les risques émergents et les besoins de gouvernance deviennent plus clairs.

Dans le même temps, les décideurs doivent être réalistes quant aux défis de la construction d'une nouvelle institution. Leur priorité immédiate doit être de développer l'expertise technique du CAISI, sa capacité opérationnelle et sa crédibilité institutionnelle. De nouvelles responsabilités doivent être introduites de manière progressive et accompagnées du personnel, des infrastructures, des financements et des autorités nécessaires à leur exécution réussie. L'efficacité de tout cadre dépendra en fin de compte de la manière dont il est conçu, financé et exécuté dans la pratique, et nous nous attendons à ce que ces détails soient affinés grâce à un engagement continu entre les décideurs, l'industrie et les experts techniques. Les recommandations qui suivent suggèrent des principes directeurs pour la conception institutionnelle plutôt que de prescrire chaque détail de mise en œuvre, et proposent une approche progressive pour construire une institution capable de soutenir les décideurs tout en maintenant la rapidité, la rigueur et la sophistication technique attendues par le secteur privé.

Construire les fondations du CAISI.

Avant que le CAISI puisse assumer d'importantes nouvelles responsabilités, les décideurs doivent s'assurer qu'il dispose des ressources, des autorités et du soutien institutionnel nécessaires pour réussir. Les décideurs doivent :

- **Autoriser le CAISI et allouer des financements appropriés.** Établir le CAISI comme une institution permanente dotée d'autorités statutaires claires et de financements suffisants pour mener des évaluations de modèles de frontière, développer des normes de sécurité, certifier des évaluateurs tiers et coordonner avec les agences de sécurité nationale et scientifiques, ainsi qu'avec les partenaires internationaux.
- **Élever l'autorité du CAISI et coordonner le soutien gouvernemental.** Le Directeur du CAISI doit rendre compte directement au Secrétaire au Commerce des États-Unis ou à un autre responsable de niveau ministériel, et la Maison Blanche doit coordonner les effectifs, les ressources, l'expertise et le soutien opérationnel des ministères et agences de l'ensemble du gouvernement fédéral.
- **Prévoir des modalités de recrutement flexibles et des voies de service public.** Adopter des modalités de recrutement similaires à celles utilisées par CHIPS for America, permettant au CAISI de recruter rapidement des talents techniques et d'offrir une rémunération compétitive, tout en créant des voies pour que des chercheurs en IA expérimentés, des ingénieurs et des experts en sécurité effectuent des périodes temporaires de service au sein du gouvernement.
- **Mobiliser l'expertise en sécurité nationale et les données.** Charger les ministères et agences de sécurité nationale et scientifiques de soutenir les évaluations dans ces domaines en coordination avec le CAISI et de mettre immédiatement à disposition le personnel et les données liés aux domaines cyber, CBRN et autres domaines de sécurité nationale pour renforcer la capacité du CAISI à évaluer et à atténuer les risques.
- **Sécuriser l'accès aux infrastructures informatiques classifiées.** Le CAISI doit avoir accès à des environnements informatiques classifiés capables de mener des évaluations de modèles de frontière, que ce soit par le biais d'infrastructures dédiées, de partenariats interagences ou d'accords formels avec des agences ou des fournisseurs commerciaux.

Créer un processus d'évaluation obligatoire.

Une fois que le CAISI aura acquis une expertise technique et une capacité opérationnelle suffisantes, les décideurs devraient exiger que les modèles de frontière les plus capables subissent une évaluation du CAISI avant leur diffusion publique. Ces évaluations doivent évaluer les capacités de frontière, l'efficacité des garanties et atténuations associées, et le profil de risque résultant du système déployé. L'exigence doit cibler étroitement les systèmes les plus capables et permettre un déploiement itératif en établissant des seuils clairs pour déterminer quand les versions ultérieures du modèle nécessitent une réévaluation. Le rôle du CAISI doit être de mener des évaluations et de recommander des atténuations — et non d'approuver ou de bloquer les déploiements. Les développeurs doivent demeurer responsables des décisions de déploiement, divulguer publiquement les résultats des évaluations et la manière dont ils y ont répondu, et demeurer responsables grâce aux exigences de transparence et de signalement.

Les décideurs doivent également s'assurer que les évaluations sont effectuées dans un délai statutaire défini et que le processus d'évaluation ne décourage pas le processus bénéfique de déploiement itératif. Si le CAISI ne parvient pas à finaliser une évaluation dans le délai défini en raison de contraintes de bande passante, de matériel, de personnel ou d'autres contraintes, les développeurs doivent être autorisés à déployer sans pénalité. Les entreprises doivent également rester libres de partager des modèles avec des

évaluateurs tiers de confiance, des chercheurs indépendants, des équipes de test et des partenaires de test avant ou parallèlement à l'examen du CAISI. Un solide écosystème d'évaluation nécessite de multiples sources d'expertise plutôt qu'un seul organisme institutionnel de contrôle.

Soutenir les évaluations techniques indépendantes.

Les évaluations déclenchées par le déploiement seules peuvent ne pas fournir aux gouvernements une visibilité suffisante sur l'évolution des capacités de frontière au fil du temps. Les décideurs doivent donc charger le CAISI de développer des normes pour les évaluations techniques indépendantes, d'établir un processus de certification pour les évaluateurs tiers qualifiés et de contribuer à la construction d'un écosystème plus large capable de mener ces examens, notamment en utilisant l'IA elle-même. Les décideurs doivent également exiger que les développeurs de frontière dépassant des seuils de capacité spécifiés subissent des évaluations techniques indépendantes périodiques menées par des organisations certifiées par le CAISI.

Une priorité initiale pour ces évaluations doit être de fournir aux décideurs une visibilité continue sur la progression vers l'AMR, les déploiements internes très capables, la sécurité des modèles de frontière, les pratiques de surveillance interne et l'efficacité des garanties associées. L'AMR pourrait devenir le défi définissant la sécurité de frontière et la gouvernance de la décennie à venir, mais les décideurs manquent actuellement de moyens fiables pour mesurer la progression vers celle-ci ou pour en comprendre les implications. Le CAISI doit donc travailler avec les développeurs de frontière, les chercheurs académiques, les agences de sécurité nationale et les partenaires internationaux pour développer rapidement des méthodologies, des repères et des indicateurs pour mesurer l'AMR et évaluer ce qui fonctionne en matière de gouvernance. Compte tenu du rythme du développement de l'IA, nous encourageons le CAISI à traiter l'AMR comme une priorité urgente.

En s'appuyant sur ce travail, le CAISI doit développer des normes communes pour les évaluations techniques indépendantes et soutenir la création d'un écosystème plus large capable de surveiller la progression de l'AMR et les garanties au fil du temps. Les développeurs de frontière doivent partager les mesures appropriées liées à l'AMR avec le CAISI, et des évaluateurs tiers qualifiés doivent périodiquement évaluer ces mesures à l'aide des méthodologies développées par le CAISI. Les résultats des évaluations techniques doivent être fournis au CAISI, qui doit utiliser ces informations pour aider les décideurs à comprendre la progression, à évaluer si les atténuations suivent le rythme et à coordonner avec les agences de sécurité nationale et les partenaires internationaux sur les implications de la progression de l'IA et la nécessité éventuelle de garanties ou de réponses politiques supplémentaires.

Les décideurs doivent également attribuer au CAISI les ressources et les autorités nécessaires pour contribuer à la construction de l'écosystème d'évaluation lui-même. Le CAISI doit être autorisé à fournir des subventions, des accords de coopération et d'autres formes de soutien aux organisations d'évaluation émergentes, aux centres académiques et aux institutions techniques développant des capacités d'évaluation, d'évaluation technique et d'audit.

3. Mobiliser une stratégie de résilience gouvernementale globale

Des institutions solides sont nécessaires, mais elles ne sont pas suffisantes. Aucun processus d'évaluation, régime d'évaluation ou organisation unique ne peut éliminer chaque risque. À mesure que l'IA gagne en capacité, les sociétés démocratiques devront s'assurer que les capacités défensives, les institutions publiques et la résilience sociétale s'améliorent parallèlement.

L'IA de frontière doit donc être traitée comme une priorité nationale nécessitant une coordination entre les agences de sécurité nationale, de santé publique, de cybersécurité, scientifiques, diplomatiques et

économiques, ainsi qu'avec les partenaires internationaux. Les décideurs doivent poursuivre une stratégie de résilience qui non seulement réduit les risques, mais renforce également la capacité de la société à répondre aux défis émergents, à s'adapter aux conditions changeantes et à continuer de bénéficier de l'IA.

Faciliter la collaboration et la coordination internationale sur la sécurité de l'IA de frontière.

Les risques de frontière ne seront pas traités par une seule organisation ou un seul pays agissant seul. Les décideurs doivent offrir une certitude juridique permettant aux développeurs de frontière de collaborer sur des questions liées à la sécurité, notamment le partage de renseignements sur les menaces, de méthodologies d'évaluation, de retours d'expérience sur les incidents et de meilleures pratiques. Les nations démocratiques doivent également travailler ensemble pour développer des cadres de sécurité compatibles, des canaux de partage d'informations de confiance et des réponses coordonnées aux incidents graves. Une priorité particulière doit être accordée au développement d'approches partagées pour évaluer et communiquer de manière responsable la progression vers l'AMR, où un manque de mesures partagées et de transparence pourrait intensifier les pressions concurrentielles entre les développeurs et rendre plus difficile la détermination du moment où des garanties supplémentaires sont justifiées. Le réseau émergent d'instituts de sécurité de l'IA pourrait contribuer à construire cette compréhension technique partagée et fournir une base pour une action coordonnée si des garanties supplémentaires deviennent nécessaires.

Protéger l'avantage informatique de l'Amérique.

Les capacités avancées d'IA dépendent de l'accès à des semi-conducteurs de pointe et à des infrastructures informatiques à grande échelle. Les décideurs doivent renforcer les contrôles à l'exportation, combler les lacunes connues et investir dans les infrastructures informatiques, énergétiques et technologiques nécessaires pour maintenir le leadership américain. Une capacité informatique stratégique donnerait aux États-Unis la capacité d'évaluer, de gouverner et de déployer des systèmes d'IA de frontière lorsque la sécurité nationale l'exige. Maintenir le leadership dans les infrastructures informatiques avancées n'est pas seulement une priorité économique et de sécurité nationale — c'est aussi une stratégie de sécurité de frontière.

Restreindre l'adoption de systèmes d'IA de frontière non évalués.

Les agences fédérales doivent interdire l'utilisation de systèmes d'IA de frontière n'ayant pas subi une évaluation de sécurité reconnue sur les systèmes et appareils appartenant au gouvernement. Ces évaluations doivent porter sur les systèmes tels que déployés, y compris les garanties et contrôles associés, plutôt que sur le modèle sous-jacent de manière isolée. Les agences doivent également interdire l'achat de produits et de services qui s'appuient sur des modèles de frontière non évalués dans des contextes gouvernementaux sensibles. Des processus d'évaluation fiables sont essentiels pour garantir que les systèmes de frontière déployés au sein du gouvernement répondent aux normes de sécurité et de sûreté appropriées.

Garantir que les capacités défensives progressent plus vite que les capacités offensives.

L'IA de frontière renforcera à la fois les défenseurs et les attaquants. Les décideurs doivent investir dans la biodéfense assistée par l'IA, la cybersécurité, la protection des infrastructures critiques et des systèmes de réponse rapide qui réduisent les conséquences des utilisations abusives quelle que soit leur origine. Le Cyber Action Plan d'OpenAI fournit des exemples de la façon dont l'IA avancée peut renforcer la résilience en aidant les défenseurs de confiance à identifier les menaces plus tôt, à répondre plus rapidement et à protéger les systèmes critiques plus efficacement. L'IA doit renforcer les institutions et les systèmes qui protègent la société, garantissant que la résilience croît avec les capacités.

Se préparer aux futurs défis de résilience.

La gouvernance de l'IA de frontière continuera d'évoluer à mesure que les capacités progresseront. Dans *La politique industrielle pour l'ère de l'intelligence*, nous avons présenté plusieurs approches pour renforcer la résilience sociétale, notamment les infrastructures de confiance en IA, les guides de confinement des modèles, les systèmes de sécurité pour les risques cyber et biologiques émergents, et de nouvelles approches de coordination internationale. Les décideurs doivent charger les agences concernées d'évaluer la faisabilité, les coûts, les avantages et les défis de mise en œuvre associés à ces propositions et à d'autres, et d'identifier les autorités ou ressources supplémentaires qui pourraient être nécessaires. Construire des institutions résilientes aujourd'hui aidera les sociétés démocratiques à s'adapter à mesure qu'émergent de futurs défis de gouvernance.

Construire les institutions de la gouvernance démocratique

L'IA de frontière contribuera à façonner l'équilibre des pouvoirs économiques, scientifiques et géopolitiques au XXIe siècle. Les sociétés démocratiques ont une fenêtre de temps qui se rétrécit pour construire les institutions nécessaires à la gouvernance de systèmes d'IA de plus en plus capables avant que les capacités de frontière ne dépassent les cadres existants. Les États ont contribué à établir un référentiel de sécurité de frontière émergent. Les décideurs doivent désormais s'appuyer sur cette base en créant un cadre national, en renforçant le CAISI en tant qu'institution principale de l'IA de frontière du gouvernement fédéral américain, et en mobilisant une stratégie de résilience plus large.

Parce que l'IA de frontière est une technologie mondiale, les nations démocratiques doivent également travailler ensemble pour renforcer les institutions techniques, développer des approches de gouvernance compatibles et coordonner les réponses aux risques émergents. Le cadre présenté ici n'est pas destiné à être le dernier mot sur la gouvernance de l'IA de frontière. L'IA progresse rapidement, et de nombreuses questions importantes restent non résolues. L'objectif est de construire les institutions, les normes et la résilience nécessaires aux sociétés démocratiques pour comprendre, s'adapter et gouverner des systèmes d'IA de plus en plus capables.