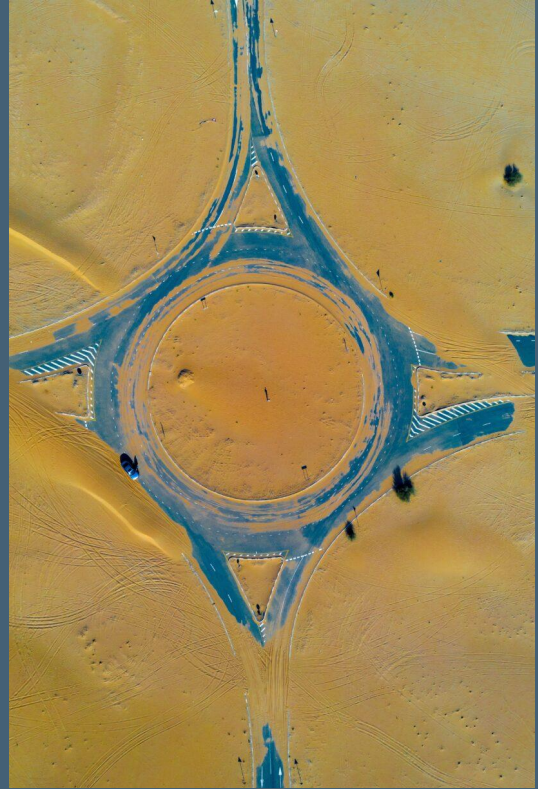


L'IA ne sera pas l'abondance, mais la rareté



AUTEUR Anton Leicht

IMAGE © Erik Krugers

DATE 22 mai 2026

Nos stratégies en matière d'Intelligence artificielle reposent toutes sur le présupposé qu'une IA de pointe américaine sera toujours largement accessible.

C'est une erreur fondamentale.

Dans les cercles de réflexion sur la politique à suivre en matière d'IA, une petite musique s'est installée : sous l'effet des pressions du marché et de marchés financiers en surchauffe, l'accès aux meilleurs modèles d'IA sera bientôt abondant. Et l'avenir appartiendra à ceux qui sauront le mieux les exploiter. Plus on s'éloigne de San Francisco, plus ce mantra résonne fort. Il atteint même une forme de paroxysme dans les périphéries, ces nombreuses puissances moyennes du monde encore prisonnières d'un projet visant à survivre à la révolution de l'IA en se fondant sur des modèles simplement « assez bons ». Cette vision suppose que les capacités *importantes* de l'IA soient largement accessibles : c'est un monde où les professionnels de la cybersécurité disposent des modèles avant les cyberpirates, et les entreprises de tous les secteurs se font concurrence sur la base d'un accès identique aux mêmes capacités d'IA.

Des événements récents sont venus bousculer cette vision irénique. Il apparaît désormais clairement que l'accès à l'IA de pointe sera bientôt limité par des contraintes économiques et de sécurité. Début avril, Anthropic a annoncé avoir développé Mythos, un modèle de cybersécurité de pointe. D'emblée, l'entreprise de Dario Amodei a annoncé qu'elle ne mettrait les capacités colossales du modèle à corriger les vulnérabilités qu'à la disposition d'une poignée d'entreprises ^①. Les start-ups de cybersécurité du quartier de Mission District à San Francisco, les intégrateurs de systèmes de la côte Est et les capitales de pays alliés de l'Atlantique au Pacifique ont tous vécu une expérience similaire ^② : en faisant défiler la page pour consulter la liste des partenaires privilégiés par Anthropic, ils n'ont trouvé qu'une liste très réduite d'entreprises, toutes basées aux États-Unis.

Certains espéraient qu'OpenAI s'en tiendrait à sa méthode de déploiement habituelle en lançant à grande échelle GPT-5.5-cyber – un modèle dont les capacités seraient, selon certaines sources, similaires à celles de Mythos. Il n'en fut rien : dans le cadre de son initiative Daybreak, OpenAI s'est elle aussi engagée à un déploiement limité ^③, dissipant ainsi l'espoir que le cas Mythos ait été le résultat d'un accident de parcours ou d'une stratégie marketing basée sur l'alarmisme. Pire encore : si nul ne sait exactement ce que le gouvernement américain compte faire à ce sujet, tout indique qu'il envisage à tout le moins d'agir, à un moment ou un autre. Et s'il est tentant d'y voir une simple confluence d'événements conjoncturels, le moment Mythos révèle en réalité des tendances de fond, qui s'amplifient depuis déjà un certain temps.

Mythos et réalité de la diffusion de l'IA

Trois d'entre elles limiteront encore davantage à l'avenir la disponibilité de l'IA à la frontière : la sécurité, la puissance de calcul et l'implication directe du gouvernement américain.

Ces dynamiques se combinent et se renforcent mutuellement. Depuis quelques semaines, elles sont entrées dans une forme d'accélération. Tous ceux qui ne font pas partie aujourd'hui du cercle restreint des développeurs basés aux États-Unis doivent se confronter à une réalité : il est de plus en plus difficile d'avoir accès à une IA de pointe.

Nous vivons dans le monde de la distillation hostile

La contrainte la plus évidente à la disponibilité généralisée des modèles est celle qu'illustre le cas Mythos : les considérations de sécurité empêchent les développeurs de mettre leurs capacités les plus avancées à la portée de tous leurs clients.

De manière schématique, le premier risque est celui du détournement : un modèle très performant semble réalistement pouvoir contribuer à mener des activités dangereuses comme des cyberattaques ou la conception d'armes biologiques. Plutôt que de le déployer immédiatement auprès du grand public, on commence par le distribuer aux opérateurs de cybergénéralité, qui profitent de cet accès anticipé pour combler des failles jusqu'alors inconnues – c'est ce qu'on a observé avec Mythos. On élargit ensuite l'accès aux seuls clients dont on est raisonnablement certain qu'ils n'en feront pas un usage criminel ; et ce n'est, dans certains cas, qu'une fois le modèle déjà dépassé technologiquement qu'on l'ouvre à tous.

Or actuellement, le gouvernement américain semble se rendre compte que ce type d'accès restreint est préférable tant pour l'intérêt national que pour la sécurité nationale. Il serait en train de commencer à envisager de faire de cet exemple vertueux une règle générale.



« Il apparaît désormais clairement que l'accès à l'IA de pointe sera bientôt limité par des contraintes économiques et de sécurité. »

Plusieurs raisons peuvent expliquer ce choix . Peut-être l'appareil sécuritaire américain ne fait-il pas confiance aux développeurs d'IA pour

empêcher des criminels, des acteurs non étatiques et des adversaires tout aussi dangereux d'accéder à des capacités dangereuses ; ou peut-être préfère-t-il savoir quelles failles les nouveaux modèles sont sur le point de révéler afin de pouvoir les exploiter lui-même en premier – comme il l'a d'ailleurs déjà fait par le passé⁵. En d'autres termes : si vous êtes la NSA et que vous avez connaissance de l'existence de failles *zero-day*, vous aimeriez vous aussi savoir lesquelles Mythos est capable de détecter afin de pouvoir les exploiter à votre avantage avant que tout le monde ne les corrige.

Mais au-delà des risques d'utilisation abusive, une autre dimension pourrait motiver des mesures de restriction encore plus directes à la disponibilité des modèles : les risques de vol de modèles, d'espionnage et de distillation, c'est-à-dire de transfert des capacités d'un modèle d'IA à la frontière appelé le modèle enseignant (*teacher*) vers un modèle distillé ou étudiant (*student*).

La possibilité du vol pourrait rendre les développeurs méfiants quant au choix de l'hébergement des modèles. Des paramètres stockés dans un centre de données non sécurisé constituent ainsi une vulnérabilité importante, d'autant que de nombreux pays en dehors des États-Unis n'ont même pas encore commencé à réfléchir sérieusement à la sécurisation de leurs centres de données.

Mais la préoccupation la plus urgente concerne la distillation hostile. De nombreux rapports indiquent qu'une partie du succès des « *fast followers* » – ces développeurs de modèles qui accusent un retard de 6 à 9 mois par rapport à la frontière technologique, comme le chinois DeepSeek – repose sur des pratiques de distillation qui nécessitent un accès plus ou moins illimité aux *tokens* API, c'est-à-dire à la capacité d'IA.

Comment éviter un futur où l'IA de pointe est capturée par quelques-uns ?

ANTON LEICHT

À long terme, la distillation constitue un risque pour les développeurs de modèles : comment sera-t-il possible de générer des revenus suffisants s'il faut rentabiliser tous ses investissements en recherche et développement dans les six mois qu'un tiers pourrait mettre à « distiller » le modèle ? Ce point est crucial pour les responsables politiques et alimente directement les inquiétudes latentes concernant la concurrence entre les États-Unis et la Chine sur fond d'espionnage industriel.

On peut donc s'attendre à des mesures répressives contre la distillation hostile. Si elles ne sont pas prises par le gouvernement, elles le seront par les entreprises développant des modèles de pointe : des procédures de

vérification d'identité plus contraignantes, des conditions d'accès par défaut plus restrictives, des critères d'ouverture ou de fermeture davantage dictés par des considérations géopolitiques.

Rien de tout cela n'augure d'un accès généralisé aux modèles à la frontière.

Pour faire face à la demande, Aodei doit déjà s'allier avec Musk

Mais le problème ne se limite pas aux préoccupations de sécurité. Plus fondamentalement, donner accès à un modèle de pointe est un jeu à somme nulle. Les vétérans de l'industrie technologique et les partisans européens de la souveraineté font souvent le parallèle avec les licences logicielles : l'innovation logicielle s'accompagnait de certaines dépendances marginales, mais la logique de la taille du marché de consommation a fini par prévaloir. Autrement dit, pour les géants comme Microsoft, les faibles coûts marginaux étaient compensés par des prix de marché standards pour le déploiement de leurs logiciels auprès du plus grand nombre.

Or il n'en va pas de même pour l'IA. Donner accès à des modèles d'IA, en particulier ceux à la frontière, nécessite d'énormes quantités de capacités de calcul. La demande marginale pour traiter mille requêtes supplémentaires est de fait tellement élevée que les principaux développeurs sont régulièrement confrontés à des pénuries de ressources de calcul^⑥. Ils réduisent leurs offres et peinent à trouver un équilibre entre le financement de leurs abonnements grand public et les contraintes réelles liées aux puces dont ils disposent. C'est pour pallier cette pénurie qu'Anthropic cherche ainsi à conclure des accords d'accès ponctuels à des centres de données moins sollicités, comme par exemple celui de sa rivale xAI^⑦. Cette situation ne va pas aller en s'améliorant et il est même probable qu'elle empire. Si les systèmes d'IA pourront réellement rivaliser avec la production des travailleurs humains d'ici quelques mois, comme certains avancent, la capacité de calcul nécessaire pour reproduire un tel volume d'activité sera colossale.

L'espoir souvent invoqué selon lequel les « courbes d'efficacité » réduiraient rapidement les coûts n'est pas ici d'un grand secours. Selon cette hypothèse, l'année prochaine, les capacités de niveau Mythos pourraient être très bon marché. Mais cela n'implique pas que Mythos 2 sera moins cher que Mythos. C'est même le contraire : les capacités à la frontière sont devenues plus chères de mois en mois depuis des années. Si l'on considère donc que la dynamique concurrentielle entre rivaux économiques, mais aussi entre acteurs de la cyberdéfense et acteurs malveillants implique non plus une IA *suffisamment bonne*, mais une *meilleure*^⑧ IA, la théorie des courbes d'efficacité n'est d'aucun secours.

Cela a une conséquence nette : donner accès à un nouvel utilisateur à un modèle de pointe, qu'il s'agisse d'un gouvernement ou d'une entreprise, implique désormais un coût marginal élevé. Les utilisateurs institutionnels ont certes toujours un intérêt à étendre leur couverture : pénétration de nouveaux marchés lorsque leur capacité s'accroît, demande accrue permettant d'augmenter les prix, bonne volonté des gouvernements, etc. Mais ces avantages sont contrebalancés par des coûts : les coûts de mise en conformité pour pénétrer de nouveaux marchés, les coûts de conception de produits adaptés à de nouveaux consommateurs et les coûts en termes de sécurité et de relations avec le gouvernement américain. Autrement dit, les effets du pouvoir de marché ne sont pas entièrement inversés mais ils sont fortement atténués : on ne peut plus se reposer simplement sur son rôle d'« acheteur intéressé » pour peser lourdement dans l'obtention d'un accès à un modèle de pointe.



« À long terme, la distillation constitue un risque pour les développeurs de modèles : comment sera-t-il possible de générer des revenus suffisants s'il faut rentabiliser tous ses investissements en recherche et développement dans les six mois qu'un tiers pourrait mettre à « distiller » le modèle ? »

La situation se complique encore pour une autre raison : face à cette tendance, une concurrence risque d'émerger autour de la question de savoir *qui* aura accès à ces capacités. Les États-Unis protégeront leur économie nationale et il y a fort à parier que nous pourrions assister à un retour de la logique qui avait motivé la proposition d'un « *GAIN Act* » il y a quelques mois ⁹. À l'époque, ses partisans au Congrès jouaient avec l'idée de donner aux Américains un droit de préemption sur les puces produites aux États-Unis ; peut-être verra-t-on bientôt les entreprises américaines être déclarées détentrices d'une sorte de droit de préemption sur les capacités d'IA produites aux États-Unis. Dans un autre cas de figure encore, la concurrence

pourrait devenir purement économique : les marges se réduiraient à peau de chagrin et, en définitive, seuls ceux qui pourraient en supporter le coût ou transformer le plus efficacement des capacités IA massives en revenus seraient en mesure de se les offrir. Or ni la plupart des gouvernements – qui n’ont pas encore intégré la logique des abonnements IA à un million de dollars –, ni les entreprises européennes – dont la capacité à générer des revenus logiciels est limitée par de très nombreuses conditions défavorables – ne sont en mesure de le faire.

À la fin, c’est l’oncle Sam qui prend le contrôle

Enfin, ce qui commence avec des restrictions motivées uniquement par des préoccupations légitimes finit toujours en politique. Une fois qu’il aura un rôle plus officiel dans la supervision du flux réel des capacités IA, le gouvernement américain pourrait arsenaliser son contrôle sur cet accès au service de ses intérêts stratégiques.

À l’origine, cette prise de contrôle serait probablement motivée par des raisons de sécurité. Pour revenir à l’exemple de la NSA, il n’est clairement ni dans l’intérêt ni dans la mission de cette agence d’assurer la diffusion *équitable* des capacités d’IA à travers le monde. Au contraire, il est plus dans l’ADN de la communauté du renseignement de limiter l’accès de tout adversaire potentiel aux modèles de pointe, même au détriment d’avantages moins tangibles comme la productivité économique ou les bonnes relations avec les alliés.

Mais cela pourrait aussi aller plus loin que les questions de sécurité. Le style Trump, qui consiste à utiliser l’influence américaine comme un levier, pourrait ici jouer à plein : les impasses dans les négociations commerciales sont débloquées en menaçant de retenir des renseignements, les accords technologiques sont bloqués en invoquant les normes de sécurité alimentaire ¹⁰. Il est difficile d’estimer *quand* une administration américaine pourrait choisir d’exercer l’autorité inévitable qu’elle aurait pour bloquer des modèles à la frontière avant leur déploiement pour garantir ses intérêts stratégiques, mais il est peu douteux qu’elle le ferait en temps voulu. Cela signifie que, même si nous faisons tout « correctement » économiquement et sur le plan de la sécurité, l’accès aux technologies de pointe risque de rester fondamentalement conditionné au bon vouloir de la puissance politique tant qu’il y aura des divergences entre les intérêts stratégiques des gouvernements – c’est-à-dire toujours.

Les asymétries qui viennent

Dans ce nouveau monde, l'accès à des capacités d'inférence illimitées est plutôt l'exception que la norme.

Un nouveau modèle de frontière pourrait d'abord être soumis à l'appareil de sécurité nationale américain, où des intérêts en place pourraient aussi bien décider de bloquer son déploiement pour des raisons de sécurité que de l'utiliser d'abord pour renforcer les défenses ou attaquer ses adversaires. Le modèle pourrait ensuite être remis aux développeurs, avec la compréhension implicite ou la demande explicite qu'il soit d'abord déployé auprès de personnes de confiance : des entreprises américaines et peut-être quelques autres multinationales choisies par l'administration. Si le modèle présente des risques en matière cyber, l'autorisation pourrait être accordée rapidement ; s'il s'agit au contraire de risques plus épineux d'ordre biologique ou liés à l'autonomie des agents, cela pourrait prendre plusieurs semaines.

Une fois cette phase terminée, le cercle des accès sans restriction pourrait s'élargir à nouveau aux entreprises ayant satisfait à des exigences suffisamment élevées en matière de vérification d'identité et aux préoccupations de sécurité des États-Unis. Tous les autres – consommateurs enthousiastes, *start-ups* ambitieuses et gouvernements inquiets du monde entier – pourraient ne jamais obtenir un accès total au modèle mais se contenter d'un accès *via* des couches de produits fondamentalement limitées comme les interfaces de *chatbot* et d'agents de codage d'aujourd'hui. Peut-être les quelques grandes *start-ups* qui ont les moyens d'engager les avocats et les lobbyistes nécessaires pourraient-elles figurer sur la liste des entreprises autorisées, et encore. Autrement dit, ce n'est que quelques mois après son développement que le modèle serait, d'une manière ou d'une autre, entre les mains de tout le monde. Le problème, c'est que personne n'aurait suffisamment de capacité pour bien utiliser cette capacité. La plupart des utilisateurs du modèle ne pourront peut-être le déployer que selon les modalités que des fournisseurs de confiance auront tracées pour eux. Ce n'est que lorsque la prochaine génération aura déjà intégré ce même dispositif que tout le monde aura alors un accès *de facto* illimité à l'IA de pointe, sur le modèle de celui dont nous profitons encore tous aujourd'hui.

Cet avenir n'est pas souhaitable. Mais il n'est pas non plus inévitable. Les capacités IA de pointe seront stratégiquement et économiquement au cœur de toutes les sociétés futures. Il est donc dans notre intérêt de permettre leur libre circulation. Si nous échouons, nous en supporterons les coûts économiques et géopolitiques.



« Nous serions naïfs de négliger les dangers d'une répartition radicalement asymétrique d'une technologie aussi transformatrice dans un ordre mondial instable. »

D'un point de vue strictement économique, les accélérationnistes ont raison de critiquer Anthropic : restreindre l'accès aux modèles de pointe aux *start-ups* et à aux entreprises ambitieuses qui voudraient les déployer va à l'encontre de l'innovation et de la croissance économique ; dans une perspective hayékienne, seul un déploiement total libère notre capacité à déterminer réellement comment nous voulons vivre et travailler avec l'IA à grande échelle et en tirer les bénéfices. Mais ce n'est pas la prétendue quête de respectabilité d'Anthropic en vue d'une potentielle nationalisation qui est ici en cause, ce sont les dynamiques de marché et les implications sécuritaires de l'IA avancée qui sont en train de créer les conditions où la diffusion massive de l'IA n'est plus possible.

Dans ce monde, il y a fort à parier que nous verrons de ce fait s'ouvrir de nouvelles fractures géopolitiques⁽¹¹⁾ : les pays se trouveront divisés entre ceux qui ont accès aux technologies de pointe et ceux qui en sont privés.

Ceux qui vivront dans les premiers pourraient être bien plus riches et en sécurité que les seconds, avec accès à de meilleurs services publics, de plus grandes opportunités économiques – et protégés par des agences de sécurité fonctionnant véritablement à la frontière technologique. Si l'IA prend l'ampleur que nous pouvons nous attendre à la voir prendre, nul ne sait quel sera l'impact de ces nouvelles asymétries sur l'ordre mondial.

Par le passé, lorsque les fruits des révolutions industrielles ont été répartis de manière inégale, les changements qui en ont résulté en termes de richesse relative, de sécurité et de puissance ont provoqué des migrations massives, ravivé des conflits latents et déstabilisé des démocraties. Certes, il existe encore de nombreuses tendances techniques et économiques favorisant une diffusion plus large de l'IA, qui pourraient nous faire échapper au scénario du pire. Mais nous serions naïfs de négliger les

dangers d'une répartition radicalement asymétrique d'une technologie aussi transformatrice dans un ordre mondial instable.

Idées reçues et solutions

Comment éviter ce futur où l'IA de pointe est capturée par quelques-uns ?

Les solutions à notre disposition ne sont pas des idées nouvelles. Mais elles sont souvent mal comprises. Les accélérationnistes – qui devraient pourtant théoriquement être d'accord avec l'idée d'éviter les restrictions à la diffusion des modèles – pensent qu'elles relèvent d'un complot des partisans de la sûreté de l'IA. Et ces derniers pensent que ces solutions ne sont que le cheval de Troie de l'accélérationnisme pour précipiter le développement de technologies fondamentalement dangereuses. Pourtant, ces politiques devraient trouver le terrain d'une convergence.

Premièrement, il faut poser le problème différemment : dans un monde moins dangereux, le besoin de restrictions motivées par la sécurité est moins pressant⁽¹²⁾. Malgré le cynisme justifié à l'égard d'une potentielle arsenalisation du contrôle d'accès à des modèles de pointe, ce sont encore des préoccupations légitimes qui laissent présager de futures restrictions d'accès. La raison pour laquelle l'affaire Mythos a poussé le monde à agir par peur est que les entreprises concernées se sentaient réellement vulnérables face aux failles que ce modèle pouvait découvrir. Cela implique, par contraste, que si nous pouvions renforcer la protection contre les voies les plus évidentes par lesquelles les agents biologiques peuvent causer des dommages – renforcer la résilience, contrôler la fabrication des structures de protéines, etc. –, la crainte d'un « moment Mythos » de la guerre bactériologique se réduirait.

Le « moment Mythos » pourrait signer la fin du « moment Warhol » de l'IA.

ANTON LEICHT

De même, de nombreux employés de laboratoires de pointe affirment que la gestion de la distillation constitue une solution technique simple aux problèmes de politique d'utilisation et de surveillance. Si tel est le cas, nous devrions peut-être commencer à déployer des solutions rapidement⁽¹³⁾, avant que d'autres ne choisissent une approche plus musclée pour répondre aux préoccupations légitimes liées à la distillation. Il en va de même pour la prolifération mondiale des modèles avancés : les importateurs potentiels auraient tout intérêt à améliorer leur propre cybersécurité, notamment la

sécurité des centres de données¹⁴ , afin de ne pas faire courir un risque énorme aux entreprises américaines qui exploitent leurs modèles en dehors des États-Unis.

Deuxièmement, la construction de nombreux *data centers* permettrait d'atténuer la pénurie de puissance de calcul à venir. Ce n'est pas compliqué, juste assez difficile – on a beaucoup parlé de la manière d'accélérer le déploiement aux États-Unis et ailleurs, et chaque GPU que nous mettons en service cette année rend plus probable une diffusion plus équitable dans trois ans. L'opposition à des déploiements rapides au nom de la minimisation des risques n'a donc, selon la logique de la rareté que nous avons développée ici, pas grand sens.

Troisièmement, les pays non américains pourraient développer leurs capacités de calcul en échange d'un accès aux modèles de pointe¹⁵ . Les alliés des États-Unis peuvent en effet offrir aux *hyperscalers* américains des conditions favorables pour la construction de centres de données en échange de garanties d'accès aux technologies de frontière.



« Tous ceux qui ne font pas partie aujourd'hui du cercle restreint des développeurs basés aux États-Unis doivent se confronter à une réalité : il est de plus en plus difficile d'avoir accès à une IA de pointe. »

Des prix énergétiques subventionnés, voire un accès direct à l'énergie, pourraient être accordés à ces centres de données en échange de garanties contractuelles de toujours fournir des capacités. Si les *hyperscalers* ou les laboratoires reviennent sur leur parole, ils devront assumer leurs dépenses d'investissement pour le centre de données désormais hors tension ; si le gouvernement américain tente d'imposer des restrictions d'accès, il devra

faire face à un lobby en colère composé d'entreprises technologiques nationales qui préféreraient s'en accommoder et percevoir les revenus de leurs investissements dans les infrastructures internationales. L'incitation à conclure ces accords devrait être à la hauteur de ce risque de perte pour les investisseurs. Mais au milieu de la frénésie actuelle pour conquérir des marchés et mettre en ligne des capacités de calcul, la possibilité de trouver un terrain d'entente sur ce terrain semble plutôt élevée.

Enfin, même si elles ne peuvent pas résoudre ce problème en construisant purement et simplement leurs propres systèmes de pointe aujourd'hui¹⁶, les puissances intermédiaires auront tout de même besoin d'options de secours pour s'assurer des capacités les plus hautes possibles dans les cas extrêmes où tout ce qui vient d'être préconisé échouerait et où l'accès à l'IA de frontière deviendrait l'apanage de quelques-uns. Leur meilleur avantage sera d'user de leur effet de levier dans la compétition entre grandes puissances¹⁷, mais certains devront également conserver une certaine capacité à construire.

L'accès à l'IA de pointe n'est pas un problème nouveau, et il ne nécessite pas de solutions particulièrement ingénieuses. Il suffit simplement de prendre beaucoup plus au sérieux ce que le cœur du débat sur la politique en matière d'IA suggère depuis longtemps : il est stratégique de construire des infrastructures capables d'héberger des systèmes d'IA avancés à grande échelle et de travailler à bâtir un monde capable de les gérer sans s'effondrer.

Le signal d'alarme est déjà là : le « moment Mythos » pourrait signer la fin du « moment Warhol » de l'IA. Si rien n'est fait, nous pourrions bientôt vivre dans un monde où les plus riches utiliseraient des IA dont les plus pauvres seraient pour toujours privés.

SOURCES

- ① Voir la page de présentation du Project Glasswing sur le site Internet d'Anthropic. ↑
- ② Pieter Haeck, Sam Clark, « European regulators sidelined on Anthropic superhacking model », Politico, 13 avril 2026. ↑
- ③ Voir la page de présentation du projet Daybreak sur le site Internet d'OpenAI. ↑
- ④ Cat Zakrzewski, Ellen Nakashima et Nitasha Tikou, « In turf battle over AI, U.S. spy agencies vie for more sway than Commerce », The Washington Post, 11 mai 2026. ↑
- ⑤ Avec le logiciel EternalBlue, par exemple. ↑
- ⑥ « The AI supply crunch is here », The Economist, 30 avril 2026. ↑
- ⑦ « New Compute Partnership with Anthropic », xAI, 6 mai 2026. ↑
- ⑧ Anton Leicht, « Import Imperatives », Threading the Needle, 6 février 2026. ↑
- ⑨ Voir la page de présentation du GAIN AI Act de 2025 sur le site Internet du Congrès américain. ↑

- ⑩ Eleni Courea, « US puts £31bn tech 'prosperity deal' with Britain on ice », The Guardian, 15 décembre 2025. ↑
- ⑪ Anton Leicht, « The Most Dangerous Time in AI Policy », Threading the Needle, 5 février 2025. ↑
- ⑫ Asad Ramzanali, Ganesh Sitaraman, « Toward a Grand Strategy for AI Resilience », Santa Monica, RAND Corporation, 2026. ↑
- ⑬ Theo Bearman, « AI Distillation Attacks : Executive and Congressional Action Can Go Further », IAPS, 12 mai 2026. ↑
- ⑭ Sella Nevo, Dan Lahav, Ajay Karpur, Yogev Bar-On, Henry Alexander Bradley, Jeff Alstott, « Securing AI Model Weights : Preventing Theft and Misuse of Frontier Models », Santa Monica, RAND Corporation, 2024. ↑
- ⑮ Anton Leicht, « Import Imperatives », Threading the Needle, 6 février 2026. ↑
- ⑯ Anton Leicht, Dean Ball, « The Race Worth Winning : Middle Powers in the Age of Machine Intelligence », Foundation for American Innovation, 13 février 2026. ↑
- ⑰ Sam Winter-Levy, Anton Leicht, « How U.S.-Chinese Competition Could Leave Most Countries Behind », Foreign Affairs, 10 février 2026. ↑