



Institut
EGA

***La nationalité stratégique de l'intelligence artificielle :
contrôle de l'accès au savoir, de la guerre froide à la
coupure d'Anthropic***

Alexandre Negrus

Président fondateur de l'Institut d'études de géopolitique appliquée (Iega)

17 juin 2026

Les opinions exprimées dans ce texte n'engagent que la responsabilité de l'auteur.

ISSN : 2739-3283

© Tous droits réservés, Paris, Institut d'études de géopolitique appliquée, 2026.

Comment citer cette publication :

Alexandre Negrus, *La nationalité stratégique de l'intelligence artificielle : contrôle de l'accès au savoir, de la guerre froide à la coupure d'Anthropic*, Institut d'études de géopolitique appliquée, Paris, 17 juin 2026.

66 avenue des Champs-Élysées, 75008 Paris

Courriel : secretariat@institut-ega.org

Site internet : www.institut-ega.org

SOMMAIRE

Résumé.....	1
L'extinction de l'interrupteur stratégique	3
Généalogie du contrôle des savoirs stratégiques	4
Du contrôle des moyens au contrôle de la capacité	5
L'arme de l'interdépendance	6
Diffuser ou refuser, la contradiction américaine.....	7
L'effet de démonstration.....	8
L'Union européenne au pied du mur	8

Résumé

Le 12 juin 2026, à dix-sept heures vingt et une, heure de Washington, le département du Commerce a ordonné à Anthropic de fermer l'accès à ses deux modèles les plus avancés, Fable 5 et Mythos 5, à toute personne dépourvue de la nationalité américaine, qu'elle réside ou non sur le sol des États-Unis, ses propres salariés étrangers compris. Incapable de trier ses utilisateurs par passeport sur une infrastructure d'inférence mutualisée, l'entreprise a éteint les deux systèmes pour le monde entier dans la nuit. C'est la première fois qu'un modèle de frontière et non la machine qui le produit, tombe sous le régime du contrôle des exportations. La portée de l'épisode excède l'incident technique et la question, déjà usée, de l'autonomie européenne. Cet ordre du pouvoir américain fait réapparaître une compétition déjà bien connue : les puissances règlent l'accès au savoir qui procure l'avantage. Reconstituer la lignée de ce contrôle permet de comprendre la nature exacte du basculement et les rapports de force qu'il redessine. L'illusion d'une technologie sans frontières s'est dissipée. L'intelligence a désormais une nationalité et les entreprises qui la produisent sont devenues, qu'elles le veuillent ou non, des instruments de la puissance des États.

L'extinction de l'interrupteur stratégique

L'ordre est tombé trois jours après le lancement public de Fable 5. Anthropic affirme avoir reçu une lettre du secrétaire au Commerce sans exposé détaillé du motif de sécurité nationale. L'entreprise dit comprendre que l'administration croit avoir identifié une méthode permettant de débrider le modèle, de le « jailbreaker », pour atteindre ses capacités de cybersécurité¹. La société conteste qu'un contournement étroit justifie le rappel d'un produit déjà déployé auprès de centaines de millions d'utilisateurs, parle d'un malentendu et promet un rétablissement rapide. Au-delà de la question du rétablissement, l'important est ailleurs.

Jusqu'alors, Washington avait soumis au contrôle des exportations les puces qui entraînent et font tourner les modèles, mais jamais les modèles eux-mêmes². La barrière portait sur l'outil de production. Elle porte désormais sur le produit fini et la capacité cognitive livrée à distance. Ce déplacement conceptuel change la donne. On aurait tort de réduire cette nouvelle étape à une querelle entre une entreprise et une administration. Selon plusieurs reconstitutions de presse, l'alerte est partie d'Amazon, dont les chercheurs auraient obtenu du modèle des informations offensives censées être verrouillées, avant que le dirigeant du groupe n'en saisisse la Maison-Blanche³. D'autres sources évoquent la crainte qu'un acteur lié à la Chine ait accédé à Mythos et la possibilité d'une réplique par distillation, c'est-à-dire la reconstitution d'un modèle à partir des réponses d'un autre⁴. Ces récits restent partiellement étayés. Ils importent moins que le geste lui-même car pour la première fois, un État a démontré, en public, qu'il pouvait éteindre à distance une faculté technique sur laquelle le reste du monde commençait à bâtir.

¹ Anthropic, « Statement on the US government directive to suspend access to Fable 5 and Mythos 5 », anthropic.com, 12 juin 2026. L'entreprise y indique avoir reçu la directive à 17 h 21, heure de l'Est, sans exposé détaillé du motif invoqué, et conteste qu'un contournement supposé du modèle justifie le retrait d'un produit déjà largement déployé.

² « Anthropic Pulls Its Most Powerful AI Models After U.S. Bars Foreign Access », Time, 13 juin 2026 ; « US orders Anthropic to disable AI models for all foreign nationals », Al Jazeera, 13 juin 2026. Plusieurs observateurs relèvent qu'il s'agit du premier recours au contrôle des exportations visant un modèle d'IA lui-même, et non les semi-conducteurs qui l'alimentent.

³ « How a warning from Amazon led the White House to shut down Anthropic's Mythos model », Fortune, 14 juin 2026, recoupant des éléments du Wall Street Journal et de Politico. La valorisation de l'entreprise à l'occasion de son projet d'introduction en Bourse, située autour de 965 milliards de dollars, y est rapportée.

⁴ « White House move to limit Anthropic linked to concerns about Chinese access to Mythos », Semafor, 13 juin 2026. L'hypothèse d'un accès lié à la Chine et d'une réplique par distillation, ainsi que le récit attribué à David Sacks, demeurent partiellement étayés et sont contestés par l'entreprise.

Généalogie du contrôle des savoirs stratégiques

Le réflexe de fermer l'accès au savoir qui fait la puissance est très ancien, si bien qu'il traverse toutes les rivalités entre cités et entre États. Sa forme a toujours épousé la forme du savoir lui-même. Tant que la connaissance technique vivait dans la main des artisans, on a retenu les artisans. Venise enfermait ses maîtres verriers sur l'île de Murano et frappait de lourdes peines ceux qui tentaient d'emporter ailleurs le secret du cristallo. L'Angleterre de la première industrialisation a interdit l'émigration des ouvriers qualifiés, puis l'exportation des machines et de leurs plans, par une série de lois maintenues près d'un siècle avant d'être abrogées dans les années 1820 et 1840, quand l'avance britannique parut assez solide pour s'en passer. Le savoir tenait dans des gestes et dans des machines, si bien que c'est leur circulation que l'on s'employait à empêcher.

La connaissance stratégique s'est peu à peu logée dans des documents. L'instrument a changé. Les États-Unis ont inventé pour l'arme nucléaire une catégorie juridique singulière : la donnée née classifiée. En vertu de la loi de 1946, toute information relative à la conception des armes atomiques était secrète dès sa création, indépendamment de son auteur et de la manière dont elle avait été trouvée⁵. La logique en fut poussée jusqu'à l'absurde apparent en 1979, lorsque le gouvernement obtint d'un juge l'interdiction provisoire de publier un article de revue sur le principe de la bombe à hydrogène, article pourtant composé à partir de sources ouvertes⁶. L'affaire devint sans objet quand la même information parut ailleurs. Elle avait posé un principe lourd de conséquences. Un savoir pouvait appartenir à l'État avant même d'avoir été énoncé.

La guerre froide a généralisé le contrôle à l'échelle d'un bloc entier. À partir de 1949, les pays occidentaux ont coordonné leur embargo stratégique vers l'Est au sein d'un comité discret installé à Paris, le CoCom, qui dressait la liste des biens et des technologies interdits à l'exportation et arbitrait les rares dérogations⁷. L'arrangement a soudé un camp autour d'une discipline commune et fait de l'accès à la technologie un privilège réservé aux alliés. Le CoCom a disparu en 1994. Son esprit a survécu dans l'arrangement de Wassenaar et, surtout, dans la matrice mentale des administrations américaines.

Restait le cas du savoir devenu pur code. Les années 1990 ont vu se livrer, autour de la cryptographie, une bataille directement liée à la situation présente. Washington rangeait alors

⁵ Atomic Energy Act de 1946 (loi McMahon), à l'origine de la doctrine dite des « restricted data » ou de la « donnée née classifiée », selon laquelle l'information relative à la conception des armes atomiques est secrète dès sa création.

⁶ United States v. The Progressive, Inc. (1979). Le gouvernement obtint une interdiction provisoire de publication d'un article sur le principe de la bombe à hydrogène, rédigé à partir de sources ouvertes, avant que l'affaire ne devienne sans objet.

⁷ Coordinating Committee for Multilateral Export Controls (CoCom), actif de 1949-1950 à 1994, installé à Paris, remplacé par l'arrangement de Wassenaar en 1996.

les logiciels de chiffrement puissants parmi les munitions, au même titre qu'un canon. Diffuser un tel programme à l'étranger revenait à exporter une arme sans licence. Le créateur du logiciel PGP, poursuivi à ce titre, fit publier le code source de son programme sous la forme d'un livre imprimé, protégé par la liberté d'expression, exportable légalement puis recomposé de l'autre côté de la frontière. La justice américaine reconnut peu après que le code était une forme d'expression⁸. L'État finit par desserrer la contrainte et transférer le sujet du registre des armes vers celui du commerce. Lorsque le savoir se réduit à de l'information pure, le contrôle frontalier devient une fiction difficile à tenir.

Le droit américain considère depuis longtemps que livrer une technologie contrôlée à un ressortissant étranger sur le sol des États-Unis équivaut à l'exporter vers le pays de cet individu. C'est la règle dite de l'« exportation réputée »⁹. Le doctorant étranger d'un laboratoire travaillant sur une technologie sensible, l'ingénieur non citoyen d'une entreprise de défense, tous tombent sous cette logique. La directive qui frappe les salariés étrangers d'Anthropic n'a donc rien d'une invention. Elle applique à un modèle de langage une règle déjà appliquée à d'autres secteurs.

Du contrôle des moyens au contrôle de la capacité

Pendant deux ans, la politique américaine de l'intelligence artificielle a reposé sur le verrouillage de l'accès aux processeurs les plus avancés et aux machines qui les fabriquent. Les autorités américaines pensaient alors verrouiller l'accès à l'intelligence artificielle de pointe. Les contrôles successifs sur les puces destinées à la Chine, l'extension de la règle du produit direct étranger qui place sous juridiction américaine tout composant fabriqué à l'aide de technologies américaines ou encore la surveillance des équipements de lithographie ; tout cela visait l'amont de la chaîne¹⁰. Le raisonnement se tenait. Maîtriser le silicium permettait d'espérer maîtriser le calcul et donc le modèle qui en sort.

La directive du 12 juin opère un déplacement crucial. Elle ne s'intéresse plus à la machine mais à ce qu'elle produit, à la capacité elle-même, accessible à distance par une simple interface. Le bien stratégique n'est plus l'objet expédié dans un conteneur mais une faculté immatérielle que l'on consomme à la demande, sans jamais la posséder. En la soumettant au contrôle des exportations, l'administration requalifie un produit commercial déployé à grande

⁸ Bernstein c. United States (cour d'appel du 9^e circuit, 1999), reconnaissant le code source comme une forme d'expression protégée ; affaire PGP et poursuites visant Phil Zimmermann dans les années 1990, classées en 1996.

⁹ Règle dite de l'« exportation réputée » (deemed export) du droit américain des exportations : la communication d'une technologie contrôlée à un ressortissant étranger sur le sol des États-Unis équivaut à une exportation vers son pays de nationalité.

¹⁰ Extension de la règle du produit direct étranger appliquée à Huawei en 2020, puis contrôles du Bureau of Industry and Security sur les puces avancées et les équipements de fabrication à destination de la Chine à partir d'octobre 2022.

échelle en technologie quasi militaire. Le modèle de frontière entre dans la catégorie des choses dont l'État règle l'usage au nom de la sécurité.

Cette requalification a une conséquence pratique : on ne sait pas trier les utilisateurs d'un service en nuage selon leur nationalité. L'inférence tourne sur une infrastructure mutualisée, indifférente au passeport de celui qui la sollicite. Sommée de couper l'accès aux seuls étrangers, Anthropic n'avait pas d'autre issue que de tout éteindre, pour tout le monde et d'un coup. La granularité de la règle juridique excédait celle du dispositif technique.

Il est désormais acquis qu'un modèle n'a pas seulement une architecture. Il a une nationalité stratégique. Le lieu de son siège social, l'implantation de ses centres de données, le droit qui s'applique à l'entreprise qui l'édite, jusqu'à la nationalité des personnes qui le servent et le développent, deviennent des variables de souveraineté. Imaginons un grand groupe industriel européen qui aurait repéré dans un tel modèle des propriétés précieuses pour la simulation et la conception. Soucieux de bien faire, il ne branche pas son activité sur l'interface publique. Il passe par un hébergeur en région européenne, chiffre ses données, cloisonne son environnement et gère ses propres clés. Il bâtit sa chaîne par-dessus et commence à démanteler la filière interne devenue redondante. L'inférence tourne à Stockholm, ce qui paraît rassurant. Le modèle, lui, demeure une technologie d'origine américaine, sous licence, contrôlée depuis les États-Unis. Au matin du 13 juin, la documentation de l'hébergeur indiquait que l'éditeur avait demandé la révocation de l'accès pour l'ensemble des utilisateurs. Sans préavis, le socle technique d'une entreprise entière pouvait disparaître.

L'arme de l'interdépendance

Le geste de Washington s'inscrit dans une pratique américaine ancienne, qui transforme les liens d'interdépendance en moyens de pression¹¹. La position centrale des États-Unis dans les réseaux mondiaux leur donne la capacité d'en fermer les points de passage. Le système de compensation en dollars est un exemple significatif. Presque toute transaction internationale transite à un moment par une banque américaine et Washington peut sanctionner un établissement étranger qui commerce avec un pays sous embargo, comme l'a éprouvé une grande banque française, la BNP Paribas, condamnée en 2014 à une amende de près de neuf milliards de dollars¹². La règle du produit direct étranger procède du même esprit appliqué à la technologie. Un seul point de passage suffit, pourvu qu'on le tienne.

Le modèle d'intelligence artificielle de pointe vient d'être désigné comme un nouveau point de passage. Celui qui l'édite et l'héberge tient un robinet que les autres avaient appris à utiliser.

¹¹ Sur la transformation des points de passage des réseaux mondiaux en moyens de coercition, voir H. Farrell et A. Newman, « Weaponized Interdependence: How Global Economic Networks Shape State Coercion » (International Security, 2019).

¹² Amende de l'ordre de 8,9 milliards de dollars infligée en 2014 à la BNP Paribas pour violation de régimes de sanctions américains, illustration de la portée extraterritoriale du dollar.

La nouveauté réside dans sa démonstration grandeur nature sur une technologie présentée comme un bien de consommation universel. Le robinet existait. On vient de le voir se fermer.

L'épisode souligne une asymétrie troublante entre les deux rives de l'Atlantique. L'Union européenne a construit une régulation de l'intelligence artificielle parmi les plus abouties au monde, centrée sur la maîtrise du risque et la protection des droits. Les États-Unis, eux, organisent l'intelligence artificielle comme un attribut de puissance. Les deux démarches ne jouent pas dans la même catégorie. Encadrer la manière dont on emploie l'outil d'un autre ne donne aucune prise sur la décision de couper l'accès à cet outil. Une réglementation, aussi exigeante soit-elle, suppose que la chose réglementée demeure disponible. Le 13 juin a montré que cette disponibilité ne va pas de soi. La conformité n'est pas la souveraineté.

Diffuser ou refuser, la contradiction américaine

Washington poursuit deux objectifs difficilement compatibles. D'un côté, faire de la technologie américaine le standard mondial, équiper la planète de ses modèles, lier les économies alliées et les États du Golfe à sa pile logicielle pour asseoir une domination durable. De l'autre, rationner l'accès à cette même technologie dès qu'un risque de sécurité apparaît. Diffuser pour régner exige la confiance des clients. Or rien n'entame la confiance comme la menace d'être coupé du jour au lendemain. On ne peut pas être à la fois la plateforme du monde et le douanier qui ferme le guichet au gré de ses alarmes.

La guerre froide avait trouvé une parade à ce dilemme. Le contrôle des exportations vers l'Est s'exerçait collectivement, à travers une instance multilatérale qui répartissait l'effort entre alliés et préservait, à l'intérieur du camp occidental, une circulation relativement libre. Rien de tel n'existe pour l'intelligence artificielle. Il n'y a pas de CoCom de l'IA, pas d'enceinte où les démocraties s'accorderaient sur ce qui se partage et ce qui se retient. Faute d'un tel cadre, l'action américaine est unilatérale, soudaine et frappe les partenaires au passage. L'Union européenne et le Canada ont découvert la coupure comme des dommages collatéraux¹³.

La cause invoquée aggrave le malaise. Si Mythos a été visé parce qu'il sait débusquer dans presque tout logiciel des failles inconnues et fournir le code pour les exploiter, alors la capacité qui en fait un produit de grande valeur est aussi ce qui en fait une arme. Anthropic avait bâti son positionnement commercial sur la sûreté de ses modèles. Cette sûreté revendiquée est précisément ce qui a attiré l'attention de l'État, jusqu'à transformer une fierté d'ingénierie en problème de sécurité nationale. La frontière entre l'assistant de codage le plus avancé du marché et un instrument de cyberattaque tient à quelques garde-fous.

¹³ Réactions européenne et canadienne rapportées par Reuters et Euronews, 14 juin 2026 : propos du porte-parole de la Commission Thomas Regnier sur le caractère non discriminatoire que devraient revêtir les mesures et sur la nécessité d'une souveraineté technologique, et mise en garde du Premier ministre canadien Mark Carney contre la dépendance à un nombre restreint de fournisseurs.

L'effet de démonstration

Tout gouvernement, toute administration, toute entreprise hors des États-Unis sait désormais que l'interrupteur existe, qu'il est à portée de main d'un seul État et qu'il a fonctionné. L'effet de démonstration compte davantage que la durée réelle de la coupure. La dépendance est devenue tangible.

Le premier effet se mesurera dans les contrats et dans les bilans. Le risque souverain entre dans l'équation de tout projet d'intelligence artificielle d'ampleur, au même rang que le coût et la performance. La promesse d'un fournisseur, fût-il le plus avancé, ne vaut que ce que vaut la stabilité du régime juridique qui l'encadre. Le deuxième effet touche à la manière de concevoir les projets. Brûler des dizaines de milliards dans des cas d'usage sans en mesurer d'abord les dépendances cachées relève désormais de l'imprudence caractérisée. La réversibilité d'un choix technique, la continuité de l'activité en cas de rupture d'accès et l'existence d'une solution de repli doivent s'évaluer avant l'engagement et non après la coupure. La résilience se pense dès l'origine. Le troisième effet est structurel car le monde s'achemine vers une fragmentation des piles technologiques - une américaine, une chinoise - et un vaste reste sommé de choisir son camp ou de tenter, à grands frais, une troisième voie. La coupure du 13 juin pousse dans ce sens. La neutralité technologique est une illusion et le code porte un drapeau capable de décider des accès.

Reste la question du rythme. Le déploiement des modèles de frontière va plus vite que la capacité collective à les éprouver et à les encadrer. D'aucuns rêvent parfois d'une coordination internationale qui les testerait avant leur mise sur le marché, soit une sorte d'agence mondiale calquée sur celle qui surveille le nucléaire. La comparaison, aussi intéressante soit-elle, reste trompeuse. La matière fissile est physique et traçable. Son contrôle repose sur un grand marché politique entre puissances qui n'a pas d'équivalent dans l'intelligence artificielle. Un modèle n'est qu'une longue suite de nombres que l'on peut copier et distiller à volonté. Surtout, l'objet à surveiller est en même temps un produit grand public et une arme potentielle.

L'Union européenne au pied du mur

L'erreur serait de tirer de tout cela un slogan. Appeler à l'autonomie européenne ne coûte rien et n'engage à rien. Le sujet mérite mieux que cette incantation répétée à chaque secousse. La véritable leçon commence par un constat de statut. L'intelligence artificielle de pointe est devenue une infrastructure critique, au même titre que l'énergie ou les paiements. On ne traite pas une infrastructure critique comme un logiciel que l'on remplace au gré des offres. On lui applique des exigences de continuité et de réversibilité que l'achat européen ignore encore trop

souvent. Tant que l'Union européenne pensera l'IA comme un service à consommer plutôt que comme un réseau vital à sécuriser, elle restera exposée à la décision d'un tiers.

Elle se poursuit par une lucidité sur les outils dont l'Union s'est dotée. Le règlement européen sur l'intelligence artificielle est un cadre de conformité. Il dit comment employer la technologie sans dire qui en garde la clé. Tel quel, il protège l'utilisateur sans rien garantir sur l'accès. Pour devenir un levier de souveraineté, il devrait s'accompagner d'exigences sur la localisation du contrôle effectif des modèles et sur la continuité d'accès en cas d'injonction d'un État tiers, jusqu'à la possibilité vérifiable de basculer vers une solution de repli. Réguler l'usage est utile mais cela ne remplace pas la maîtrise de l'accès. Hasard du calendrier, la Commission a présenté début juin 2026 un paquet sur la souveraineté technologique, neuf jours avant la coupure¹⁴.

Une distinction technique, qui commande la nature de la dépendance, mérite toute l'attention des décideurs : un modèle dont les poids restent fermés et servis depuis l'infrastructure de son éditeur peut être coupé à distance. Un modèle dont les poids sont ouverts et téléchargés échappe, lui, à toute révocation une fois installé, puisque personne ne peut reprendre ce qui a déjà été copié. Le débat sur la sûreté redoutait l'incontrôlabilité des modèles ouverts. Vu sous l'angle de la souveraineté, cette même incontrôlabilité devient une garantie de continuité. Pour un État ou une entreprise qui refuse de remettre son interrupteur à un tiers, la maîtrise des poids est désormais la condition de l'autonomie réelle.

Elle suppose enfin de regarder la capacité en face. Disposer de modèles de frontière conçus et contrôlés sous juridiction européenne est la seule garantie qu'aucune injonction étrangère ne puisse vider une chaîne entière de sa substance. L'ambition est immense et le retard considérable. La coupure du 13 juin a au moins le mérite de la clarté. Elle expose aux Européens le prix exact de la dépendance. Ce prix se règle d'avance, sous la forme d'investissements patients et de coordination, ou il se paie au comptant, le jour où l'interrupteur change de position.

¹⁴ Commission européenne, paquet sur la souveraineté technologique incluant un projet de *Cloud and AI Development Act*, présenté le 3 juin 2026, soit neuf jours avant la coupure.



Institut EGA

ISSN : 2739-3283

© Tous droits réservés, Paris, Institut d'études de géopolitique appliquée, 2026.

Institut d'études de géopolitique appliquée
66 avenue des Champs-Élysées, 75008 Paris

Courriel : secretariat@institut-ega.org

Site internet : www.institut-ega.org