La sénatrice démocrate de New York Kirsten Gillibrand a déposé fin mai un amendement au projet de loi d'autorisation budgétaire de la défense (*National Defense Authorization Act*, ou NDAA) pour l'exercice 2027, qui prévoit la création d'une « *Cyber Force* ». Selon son bureau, cette nouvelle armée serait rattachée à l'*Army*, l'armée de terre américaine, sur le modèle existant qui place la Space Force sous la tutelle de l'*Air Force* et le Corps des *Marines* sous celle de la *Navy*. Si elle aboutissait, cette réforme porterait à sept le nombre de branches des forces armées américaines.

L'élue justifie sa démarche par l'inadéquation, selon elle, de l'organisation actuelle face à des menaces numériques en expansion. Elle estime que des années d'ajustements progressifs n'ont pas permis de répondre au niveau de la menace et qu'une force dédiée serait nécessaire pour préparer le pays au combat sur le champ de bataille moderne. De source parlementaire, des dispositions comparables circuleraient également à la Chambre des représentants, où le républicain texan Pat Fallon a affirmé en début d'année devant le *Center for Strategic and International Studies* (CSIS) qu'une telle force était selon lui « *inévitable* ».

L'idée n'est pas nouvelle. Gillibrand la défend depuis plusieurs années : dès le NDAA pour l'exercice 2024, elle avait fait adopter en commission une disposition chargeant le ministère de la Défense de commander une étude sur l'opportunité d'établir une branche dédiée au cyberespace, assortie d'une clause interdisant toute interférence du Pentagone dans les conclusions. Cette mention n'avait toutefois pas survécu aux négociations avec la Chambre, dont le texte ne comportait pas de provision équivalente.

Le NDAA pour l'exercice 2025 a relancé la démarche en confiant aux *National Academies of Sciences, Engineering, and Medicine* une évaluation des « *modèles organisationnels alternatifs* » pour les forces cyber des armées, incluant l'examen de la faisabilité d'une armée distincte consacrée au domaine numérique. Les résultats de cette étude n'ont pas encore été publiés. Les détails précis de l'amendement de 2026 ne sont pas non plus connus, mais plusieurs centres de réflexion ont déjà élaboré leurs propres maquettes de force.

Quelle physionomie pour une telle force ?

Les contours possibles d'une *Cyber Force* restent au stade des hypothèses. Un rapport publié en 2024 par la *Foundation for Defense of Democracies* (FDD), organisation favorable au projet, avançait qu'une telle branche pourrait rassembler environ 10 000 personnels pour un budget de l'ordre de 16,5 milliards de dollars, et être effectivement adossée à l'armée de terre.

En août 2025, la FDD et le CSIS ont lancé une commission conjointe sur la « *génération de forces cyber* », chargée de doter la Maison-Blanche et le Pentagone d'un cadre directeur dans l'hypothèse d'une décision favorable. Cette commission doit rendre ses conclusions au plus tard en juin 2026. Le débat s'inspire largement du précédent du *Special Operations Command* (SOCOM), dont le statut hybride (doté de prérogatives proches de celles d'une armée tout en restant un commandement interarmées) est régulièrement cité comme modèle de référence.

Le rattachement à l'*Army* ne fait pas consensus. Un ancien responsable militaire a estimé que cette option reléguerait la mission cyber au rang de priorité secondaire, l'armée de terre étant

déjà la plus vaste des branches (environ la moitié des effectifs du département) et la plus difficile à administrer. Selon lui, l'argument de la facilité d'intégration masquerait un risque de dilution de la fonction numérique.

À l'inverse, Mark Montgomery, contre-amiral en retraite et chercheur à la FDD, défend l'urgence d'agir. Il soutient qu'une telle réforme structurelle doit être engagée en début ou en milieu de mandat présidentiel, et non à son terme, pour disposer du temps politique nécessaire. L'amendement devra de toute manière franchir les multiples étapes de réécriture au Sénat puis à la Chambre avant de figurer, le cas échéant, dans la version de compromis du NDAA.

CYBERCOM 2.0, la voie concurrente

L'initiative parlementaire s'inscrit dans la rivalité entre deux approches. La première, dite CYBERCOM 2.0, consiste à renforcer l'actuel *U.S. Cyber Command* en améliorant le recrutement, la formation, la fidélisation des opérateurs et son contrôle budgétaire, sans créer de nouvelle armée. Esquissé sous l'administration Biden fin 2024 autour de quatre piliers, dont un nouveau modèle de génération de forces, ce plan a été remanié puis déployé fin 2025. Ses détracteurs le qualifient de « *statu quo amélioré* » et estiment qu'il diffère le vrai débat sur la création d'une branche autonome. Ses partisans, dont l'ancien commandant de *Cyber Command* Timothy Haugh, y voient au contraire une option plus rapide et moins coûteuse, privilégiant les capacités opérationnelles plutôt que la création d'une nouvelle bureaucratie.

La seconde voie est précisément celle d'une *Cyber Force* indépendante. Ses promoteurs avancent que c'est le seul moyen de résorber durablement les difficultés de recrutement et d'encadrement du commandement : Pat Fallon a ainsi relevé que, sur la quinzaine d'officiers généraux affectés à *Cyber Command*, un seul disposerait d'un parcours spécialisé dans le domaine.

Le soutien de l'administration Trump à cette démarche bipartisane reste incertain. Katie Sutton, secrétaire adjointe à la Défense chargée de la politique cyber et principale conseillère en la matière du secrétaire Pete Hegseth, a défendu en janvier devant la commission des forces armées du Sénat les réformes de *Cyber Command*, tout en jugeant qu'un commandement modernisé et une nouvelle armée n'étaient pas incompatibles. Elle a présenté les deux questions comme des débats distincts méritant chacun un examen de leurs avantages et inconvénients.

Les partisans d'une force dédiée mettent par ailleurs en avant la convergence avec les orientations de l'exécutif, notamment les appels à des « *opérations cyber offensives* » figurant dans la stratégie antiterroriste publiée par la Maison Blanche. Cet argumentaire intervient alors que la dimension numérique a pris une place croissante dans des opérations militaires récentes, en Iran comme au Venezuela. Montgomery résume ainsi la position des promoteurs : une posture plus offensive supposerait de générer davantage de forces, un volume que le dispositif actuel ne permettrait pas d'atteindre pour couvrir simultanément les missions offensives et défensives.