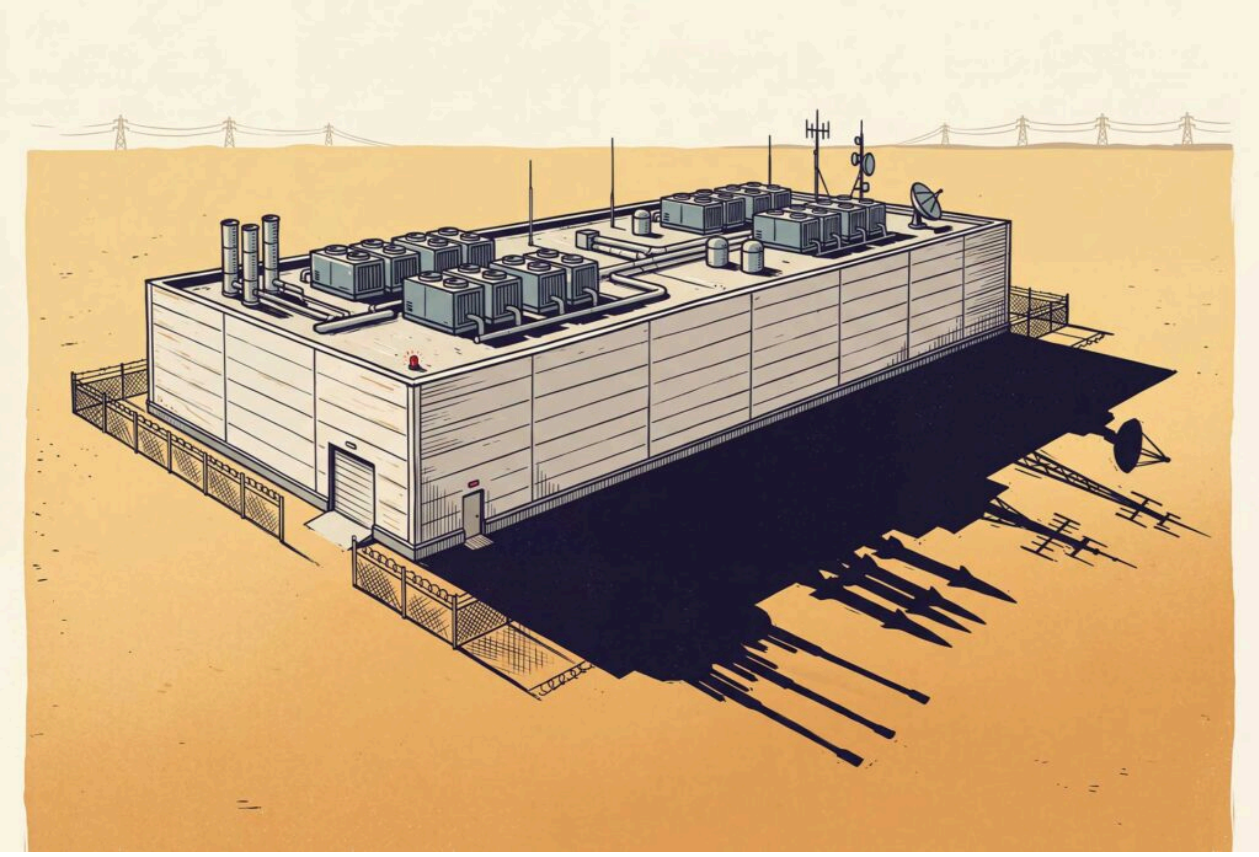
contre temps

16 novembre 2026

# IA et data centers : piliers de l'industrie militaire et de l'impérialisme

Dans ce texte, Antoine Devillet, membre du collectif Le nuage était sous nos pieds (https://lenuageetaitsousnospieds.org/), éclaire les rapports étroits entre l'industrie militaire et le secteur de l'IA et des data centers. Il analyse finement les usages de l'IA dans la surveillance de masse et les guerres hybrides conduites par les États-Unis et Israël notamment. En outre, il montre qu'en se rendant nécessaire au secteur militaro-sécuritaire, l'économie de l'IA aujourd'hui se dérisque, c'est-à-dire qu'elle supprime une partie des risques liés à ses investissements. Enfin, l'auteur souligne l'importance de lutter contre l'expansion des data centers dans une perspective anti-impérialiste et anti-militariste.

Antoine Devillet (https://www.contretemps.eu/author/antoine-devillet/)

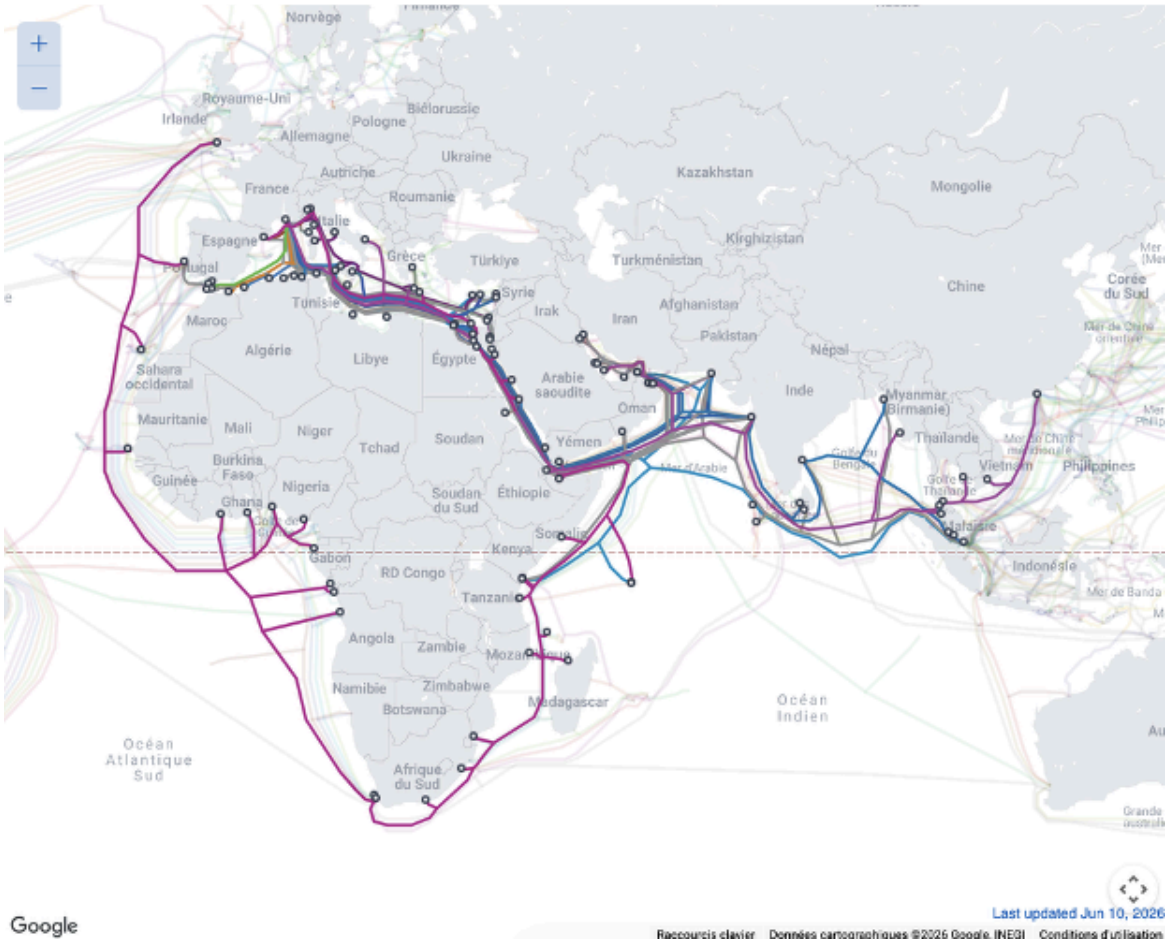


Notre collectif s'appelle Le Nuage était sous nos pieds (https://lenuageetaitsousnospieds.org/), donc le « *cloud* » était sous nos pieds. Ce nom s'inscrit dans le geste consistant à rematérialiser et à re-territorialiser le *cloud*, et donc à prendre acte qu'il passe en plein d'endroits sous nos pieds. Que le *cloud* soit sous nos pieds implique que ce qu'on appelle la « *kill chain* » militaire, qu'on traduit parfois par « la chaîne de mise à mort », passe, elle aussi, sous nos pieds. Cela sera l'objet de ce texte.

## Marseille, comptoir d'infrastructures numériques de la Big Tech

À Marseille, où est basé notre collectif, nous nous trouvons dans un point un peu particulier de l'infrastructure mondialisée du numérique, qui comporte des data centers, mais aussi des câbles sous-marins, des satellites, des antennes, de la fibre optique qui longent les chemins de fer ou les autoroutes. Marseille a été élue par différentes multinationales étatsuniennes, dont Digital Realty[1], comme « comptoir numérique » dans leur stratégie d'expansion méditerranéenne. Le champ lexical convoqué par l'expression « comptoir numérique » fait douloureusement écho au passé colonial de la ville, comme porte maritime vers les colonies et leurs comptoirs et rend très explicite l'intérêt géostratégique de Marseille.

La « porte » actuelle se traduit par la présence de 19 câbles sous-marins intercontinentaux parmi les plus puissants et importants du monde (https://www.submarinecablemap.com/landing-point/marseille-france)[2] qui viennent relier l'Europe de l'ouest et ses grands centres capitalistes (le FLAP pour Francfort, Londres, Amsterdam, Paris) aux marchés de la donnée à conquérir sur tout le pourtour méditerranéen, les pays côtiers de tout le continent africain, et via le canal de Suez, jusqu'en Océanie. Ces câbles de fibre optique, dont on voit les tracés actuels ci-dessous, suivent les anciennes routes coloniales qui elles-mêmes donnèrent lieu aux tracés des premières routes de câbles télégraphiques méditerranéens, reliant Paris à son empire colonial, et pour qui Marseille était le chemin le plus court vers ses colonies.




*Carte des 19 câbles sous-marins de fibre optique atterrés à Marseille*
*Source : Telegeography*

Ces câbles avaient plusieurs fonctions, dont celles de relier le monde à la Bourse de Londres et d'assurer la puissance de la livre sterling. L'Empire britannique, grande puissance câblière de la deuxième moitié du XXème siècle est pionnière dans le télégraphe mais aussi dans le contrôle des fonctions régaliennes assurées par les élites coloniales sur place[3]. Le premier câble sous-marin entre la France et l'Algérie est ainsi posé en 1870 entre Marseille et Annaba, suivi par un 2ème entre Marseille et Alger en 1871, dont la pose est orchestrée par Adolphe Thiers. Dans les années 1880-1890, une « *politique de câbles sous-marins en lien avec les ambitions coloniales de la France* » est élaborée, visant à raccorder les colonies d'Afrique du Nord et de l'Ouest[4]. Les câbles en cuivre isolés à la gutta-percha du télégraphe ont laissé place aux câbles coaxiaux en cuivre et polyéthylène du téléphone, eux même

remplacés par des câbles analogiques puis numériques de fibre optique du réseau internet. Cette mémoire infrastructurelle révèle la continuité des fonctions impériales de ces fibres optiques dans les fonds marins.

Cette arrivée de câbles constitue une opportunité stratégique pour la construction des data centers. Les data centers sont des usines spécialisées où l'on stocke des serveurs, qu'on pourrait comparer à de gros ordinateurs, beaucoup plus denses, et souvent beaucoup plus performants. Ces serveurs ont des capacités de stockage, de calcul, de transmission, pour l'essentiel plus importantes et spécialisées que nos ordinateurs individuels. Chaque data center va électrifier, maintenir, rafraîchir, plusieurs dizaines de milliers, voire plusieurs centaines de milliers de serveurs, en fonction de la taille du data center. Ce qui est très important, c'est que ces data centers sont interconnectés avec d'autres data centers via les réseaux câbliers et satellitaires[5].

Pour aller plus loin

**Conçu pour dominer. Palantir Technologies, bras armé numérique de la répression mondiale (https://www.contretemps.eu/palantir-technologies-bras-arme-numerique-repression-mondiale/)**

Ce sont ces data centers, interconnectés, qui constituent la base matérielle du numérique dominant dans lequel nous nous trouvons aujourd'hui. Ces data centers, à travers la « manufacture » des données[6], sont le lieu de production de valeur des mastodontes du numérique. Prenons l'exemple d'Amazon : plus de 58% du résultat d'exploitation de l'entreprise (c'est-à-dire les bénéfices opérationnels) et 17% de ses revenus totaux viennent de la vente de ses services cloud (AWS - Amazon Web Services) qui sont logés dans les data centers. Ce qui signifie que c'est de loin l'activité la plus rentable du groupe et sur laquelle il a les marges les plus élevées. Google, Oracle et Microsoft sont dans une dynamique relativement similaire[7].

Pour conclure concernant Marseille, ajoutons que Fabrice Coquio, PDG de Digital Realty en France et Europe du Sud, lors d'une audition parlementaire, révélait que 70% des clients des data centers marseillais de Digital Realty sont extra-européens et que 20% des flux traités à Marseille viennent de l'Inde, confirmant donc le rôle extractif de leur connexion au réseau câblé. L'accès au continent africain est aujourd'hui un enjeu majeur des infrastructures mondiales, car il est considéré comme un marché très prometteur, puisque peu exploité, mais aussi perçu comme sujet à une concurrence massive de la part de la Chine.[8]

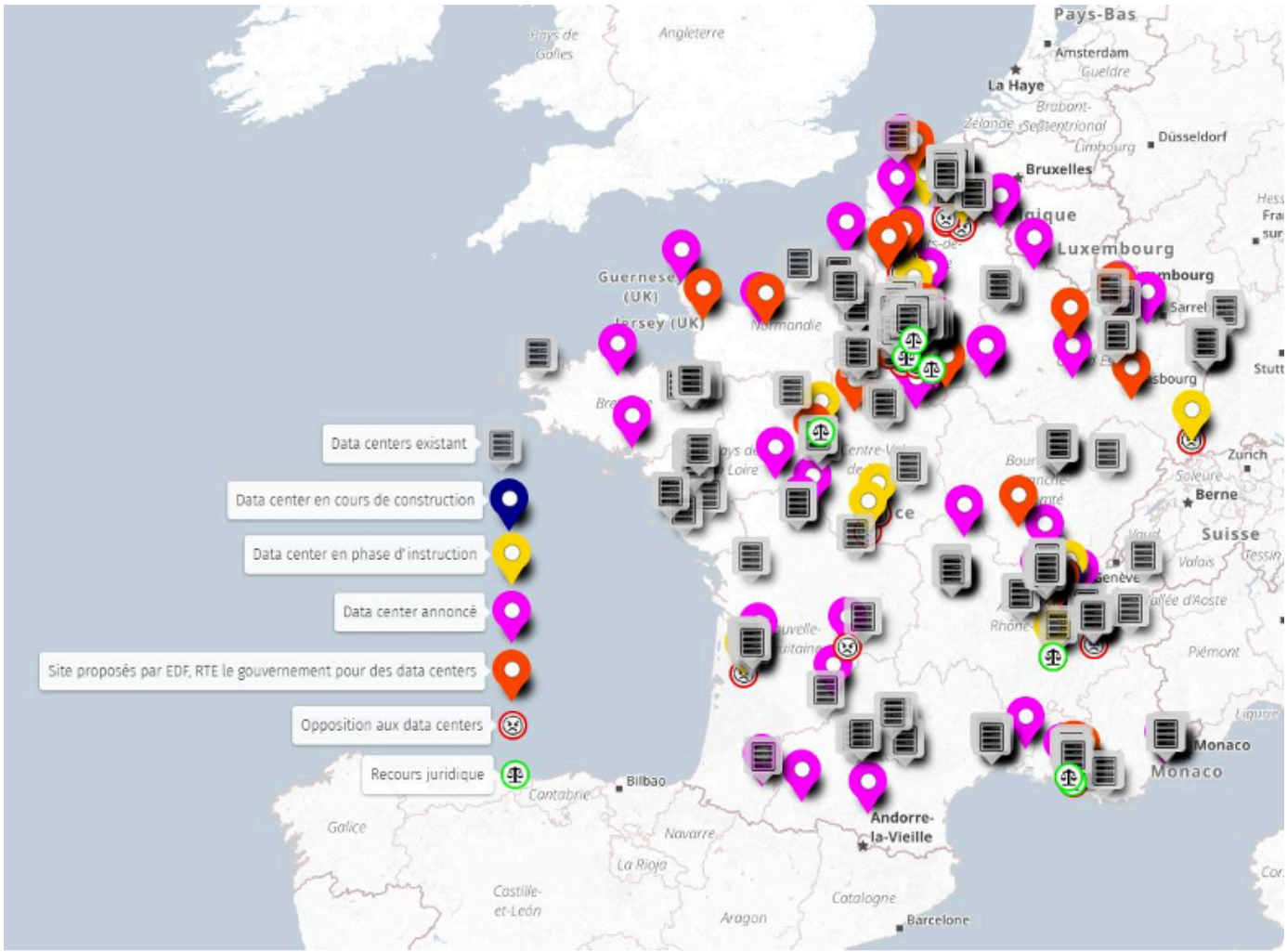
### Explosion des projets de data center

Au-delà de Marseille, on peut observer aujourd'hui un mouvement délirant de construction de data centers dans de très nombreux endroits du monde. La France de Macron cherche à tout prix à ne pas rater le coche. En 2025, elle a été le pays qui a attiré le plus d'investissements étrangers (https://unctad.org/system/files/official-document/diaeiainf2026d1_en.pdf) dans la construction de data centers (69 milliards de dollars). Ces investissements viennent en grande majorité de fonds émiratis ou US, comme le fonds MGX (https://multinationales.org/fr/enquetes/profits-et-pertes-derriere-le-boom-des-datacenters-en-france/mgx-le-tres-peu-rassurant-fonds-emirati-derriere-l-immense-centre-de-donnees), fonds d'investissement émirati lié au pétrodollar et dont les fondateurs sont proches de la branche cryptomonnaie de la famille Trump.

Si l'argument de la souveraineté est souvent présenté comme central dans la course à la construction de data centers, la provenance des financements semble plutôt l'inscrire dans une prolongation de la vassalisation de l'Europe vis-à-vis des Etats-Unis. Ces nouveaux data centers localisés en France – si l'on croit les annonces de la ministre déléguée chargée de l'Intelligence Artificielle et du numérique, Anne

Le Hénanff – consommeront la moitié du parc nucléaire français (https://www.entreprises.gouv.fr/espace-presse/rencontres-des-centres-de-donnees-pres-dun-apres-le-sommet-pour-laction-sur-lia-de)[9], en toute démesure. Ce mouvement de construction fait suite au sommet de l'IA réalisé sous l'égide de Macron en février 2025. Il y opposait au « drill, baby, drill (https://lenuageetaitsousnospieds.org/articles/2025-03-21-loi-simplification-imposer-les-data-centers.html) » de son « bon ami de l'autre côté de l'Atlantique » Donald Trump, le « plug, baby plug », signifiant « nous avons en France un super réseau nucléaire, venez plugger vos data centers chez nous ». C'est donc ce que les industriels ont fait.

Google a un projet estimé à 1,3 GW à Châteauroux (https://multinationales.org/fr/enquetes/profits-et-pertes-derriere-le-boom-des-datacenters-en-france/a-chateauroux-google-avance-masque-les-dessous-d-un-projet-de-data-center-xxl), c'est-à-dire, l'équivalent d'une grosse centrale nucléaire. À Fouju, en Seine-et-Marne, le fonds MGX, avec quelques capitaux français qui permettent un peu de « souveraineté washing » (70 % de capitaux venant de MGX), développe le projet Campus IA, avec 1,4 GW de puissance réservée annoncée. Plus récemment, lors du lancement du sommet Choose France – le dernier de Macron avant la fin de son mandat, et qui comme son nom l'indique appelle les investisseurs à choisir la France – Softbank, société à action très impliquée dans le numérique japonais, avec à sa tête Masayoshi Son, sorte d'émissaire de la Silicon Valley au Japon, vient d'annoncer l'investissement de 75 milliards d'euros en France. 45 milliards doivent être consacrés à la construction de data centers dans les Hauts de France, notamment à Dunkerque, pour une puissance cumulée de 5 GW, soit près de 5 réacteurs nucléaires de consommation électrique. Ces quelques projets permettent de percevoir l'ampleur de l'emballement délirant auquel nous faisons face.




*Carte des data centers (https://umap.openstreetmap.fr/fr/map/carte-des-data-centers-des-projets-et-des-contesta_1289485#6/47.077604/1.669922) / Site du collectif Le nuage était sous nos pieds*

Bien entendu, d'un point de vue territorial, cela représente une consommation foncière hors proportions. Il s'agit d'une consommation énergétique monstrueuse, qui impliquent toutes les problématiques en cascade liés à la production d'énergie (relance du nucléaire, réouvertures de centrale à gaz, conflits d'usage, développement industriel de renouvelable, etc). En outre, selon les technologies de refroidissement utilisées, nous aurons une grande consommation en eau

(http://./Points%20de%20rep%C3%A8re%20sur%20l'empreinte%20eau%20des%20data%20centers%20-%20de%20quoi%20parle%20t'on%20%3F%20quand%20%3F%20comment%20%3F%20combien%20%3F) [10]. Si les industriels porteurs de projet craignent le manque d'acceptabilité sociale lié à l'usage important de l'eau, il s'agira d'une consommation de fluides frigorigènes qui, en se détériorant, produiront des PFAS (https://reporterre.net/Fuite-de-tonnes-de-PFAS-terres-englouties-encore-un-enorme-data-center-polluant). À ces quelques éléments, il faut ajouter les stockages importants de fioul ou autres carburants pour les générateurs de secours, et surtout une production très importante de chaleur (https://arxiv.org/pdf/2603.20897) [11] dans ce monde qui surchauffe de plus en plus.

**Recompositions géopolitiques**

À tous ces impacts territoriaux, dans la vie du data center une fois construit, s'ajoute la chaîne amont du data center, notamment la production des composantes électroniques. Tous ces data centers, et d'autant plus les data centers dédiés à l'entraînement des IA avec leurs nombreux GPU Nvidia et de serveurs toujours plus nombreux et performants, nécessitent une intensification massive des chaînes extractivistes. Il peut y avoir plus de 70 métaux impliqués (https://journal-labreche.fr/terre-pillee-et-intoxiquee-comment-lia-change-le-monde/) en fonction du type de puces utilisées, cela impliquant autant de chaînes d'approvisionnement au Soudan, en Kanaky, en République Démocratique du Congo, au Chili, dans les Balkans, autant de chaînes de raffinages, d'usines d'assemblages, de gravures, etc.[12]

Ce boom de consommation en métaux participe à la réorganisation de toutes les chaînes d'approvisionnements mondiales et devient aujourd'hui un enjeu géopolitique majeur. À titre d'exemple, la sécurisation des chaînes d'approvisionnement de l'Intelligence Artificielle, notamment face à la menace chinoise, fut l'un des principaux sujets discuté en juin 2026 lors du G7 à Évian. Autre exemple : Donald Trump a lancé en décembre 2025 une « alliance » appelée « Pax Silica » (https://www.state.gov/pax-silica/#what), paix du Silicium, où il s'allie avec l'Australie, qui détient des métaux critiques, le Japon et la Corée du Sud, qui ont une expertise dans les filières de semi-conducteurs, Israël, qui a d'importants centres de recherche et de développement logiciel, le Qatar ou les Émirats Arabes Unis, qui ont une énergie bon marché et de très grosses capacités d'investissements liés au pétrodollar, le Royaume-Uni comme puissance diplomatique ou encore la Malaisie comme terrain d'extraction.

Le but de cette « paix » est de réorganiser les chaînes d'approvisionnement mondiales pour assurer le « leadership » étatsunien dans le secteur de l'Intelligence Artificielle. Au sein de cette alliance, les plus grandes puissances, et au premier chef les USA, gardent la main sur les processus d'innovation, le design, ce qui assure le plus de production de valeur, tout en cherchant à garder ouvert les marchés pour écouler leurs produits. L'Union Européenne rejoint l'alliance tardivement, (https://legrandcontinent.eu/fr/2026/06/29/pax-silica-leurope-saligne-t-elle-sur-washington-dans-la-guerre-technologique-avec-pekin/) en juin 2026, prise entre l'envie de diminuer ses dépendances numériques aux USA et sa dépendance économique et politique structurelle[13].

Cette sécurité se fait au prix du sang, et prolonge les hiérarchies impérialistes entre centre et périphérie. La violence armée reste *in fine* la manière la plus sûre de garder un accès à bas coût aux métaux indispensables pour l'essor mondial de l'IA, et on constate que la plupart des guerres, conflits armés ou tensions géopolitiques contemporaines, ont cet objectif d'assurer les chaînes extractivistes minières (quand il ne s'agit pas de pétrole), que ce soit les milices armées au Kivu, la fausse guerre civile au Soudan, la doctrine « Donroe » en Amérique du Sud, les menaces d'annexion du Groenland, ou encore les tensions autour de Taiwan.

On peut dès lors se demander : « *c'est quoi le délire ?* » Pourquoi autant de pays se jettent à corps perdus dans la construction de data centers ? Pourquoi veulent-ils éviter de « louper le train » de l'IA ?

Bien entendu, il y a plusieurs raisons : on peut regarder du côté du fonctionnement du capital (https://www.contretemps.eu/destruction-capital-fictif-bulle-intelligence-artificielle-mystere-rentabilite/) [14], du côté de la guerre commerciale entre puissances industrielles, mais aussi, et c'est tout aussi central, du côté de l'importance de l'IA dans le complexe militaro-sécuritaire, sur lequel nous insistons dans ce texte.

Dès sa création, le technopôle de la Silicon Valley, les premières grandes entreprises d'Internet et les acteurs qui composent cet univers, sont étroitement entremêlés au secteur militaire (ARPAnet par exemple, ancêtre d'Internet, émerge du programme américain de défense en contexte de Guerre froide). Ensuite, durant une certaine fenêtre temporelle, les leaders du secteur de la Tech ont prétendu prendre leurs distances avec l'effort de guerre et les politiques impérialistes des États-Unis, cherchant à partager une image progressiste, compatible avec leurs besoins d'attirer de jeunes cadres, ce qui nous a peut-être fait un peu perdre de vue ce lien organique[15]. Aujourd'hui, ces interactions complexes et permanentes entre secteurs militaires et numériques reviennent sur le devant de la scène. Toutes les armées ont des cellules de recherche en *disruptive innovation*, donc investissent massivement dans la recherche, et tendent à réorganiser la recherche publique pour faire advenir des innovations militaires qui permettront de donner un avantage comparatif, une disruption dans la manière de faire la guerre qui assurera une domination (ou une capacité de résistance à une puissance militaire jugée supérieure technologiquement).

C'est ce qui fabrique une « obligation d'y aller ». La lectrice ou le lecteur aura peut-être vu passer la petite passe d'arme médiatique entre le Pape et Arthur Mensch (https://www.clubic.com/actualite-614614-le-patron-de-mistral-repond-au-pape-sur-la-guerre-de-l-europe-face-a-la-tech-americaine.html), le PDG de Mistral AI, lors de laquelle le Pape appelait à désarmer l'IA. Arthur Mensch a répondu en substance : « nous ne pouvons pas désarmer l'IA, parce que les Chinois, ou nos ennemis, eux, vont l'armer ». Mensch, comme d'autres (dont Alex Karp, CEO de Palantir), va même jusqu'à dire des capacités IA militaires qu'elles sont la nouvelle dissuasion à l'heure où l'arme nucléaire ne suffit plus.

Ainsi, de la même manière que l'avantage militaire que conférait l'adoption du pétrole au XXe siècle ou du charbon (https://lundi.am/Pour-la-Palestine-comme-pour-la-Terre-d-Andreas-Malm) au XIXe avait entraîné toutes les armées dans les énergies fossiles, de même ce que permet militairement l'IA au XXIe siècle est un des principaux leviers d'entraînements qui obligent tous les pays à investir dans l'IA. La question militaire est donc centrale pour comprendre cet emballement, et toute lutte conséquente contre les data centers se doit d'être antimilitariste, sinon elle n'aboutira à rien.

## Comment les data centers sont utilisés par le militaire

Les IA militaires sont très liées aux renseignements, à « l'intelligence », à la planification, à la génération de cibles pour l'armée, et aux systèmes d'armements autonomes (qualifiés parfois de « robots tueurs ») ; toutes nécessitent de très grandes bases de données (et les petites mains des travailleur·euses du clic) pour leur entraînement et leur fonctionnement, et n'ont de sens qu'avec l'existence de très grandes bases de *cheap data*. Les infrastructures du numérique servent ainsi d'infrastructure de production et de circulation de la donnée nécessaire pour le secteur militaire contemporain.

Par exemple, on peut évoquer le « Maven Smart System », contrat porté par le département de Défense US, pour un contrat à 1,3 milliards de dollars qui allie les sociétés Palantir, fondée par Peter Thiel et Alex Karp, avec, jusqu'à très récemment, Anthropic, qui produit le chatbot *Claude*, remplacée par OpenAI, qui produit le chatbot *ChatGPT* puis finalement par un mix un peu opaque de Grands Modèles de Langages (https://www.nytimes.com/2026/05/01/us/politics/pentagon-ai-companies-deals.html), ainsi que Amazon Web Services, la branche cloud de Amazon[16]. Le « Maven Smart System » est un système intégré de commandement, dont le cœur est le *targeting,* le fait d'établir des cibles. Le système agrège entre elles toutes une série de données (satellites, data center, bases de données, radars, informations en lignes, etc.) pour fabriquer des cibles. Le système les identifie, les localise et ensuite propose différents plans d'actions pour les atteindre. Enfin, si les systèmes d'armement de ces plans d'action sont également automatisés, ces systèmes d'armement peuvent exécuter le plan d'action et déclencher une opération. C'est notamment avec le « Maven Smart System » que les USA ont déclenché l'opération « Epic Fury », cette agression militaire abominable coordonnée avec Israël contre l'Iran.

On dit que ce système a pu générer plus de 1000 cibles, avec plans d'actions, durant les douze premières heures de l'opération, parmi lesquelles 900 opérations sur les 1000 ont été déclenchées. En outre, on estime qu'il y avait à peu près 1 minute 20 entre chaque opération, informées en direct par Starshield, le système satellitaire d'Elon Musk. Il a été question dans certains médias du fait que Dario Amodei, PDG de Anthropic refusait d'avoir un process sans aucune décision humaine[17], et de nombreux commentateurs commentent les enjeux de dilution des « responsabilités » légales. Mais la question principale derrière l'intégration de l'IA générative dans le militaire est bien l'intensification des

capacités meurtrières, et surtout de leurs cadences. On estime qu'une équipe d'analystes humains mettait en moyenne 8 heures à établir une cible et un plan d'attaque, avec une précision de 80 %. Le « Maven Smart System » s'il accélère les cadences, fait tomber le niveau de précisions à 60 %. Le cas du bombardement par l'armée étatsunienne, le 28 février 2026, de l'école pour fille de Minab, Shajareh Tayyebeh, pourrait constituer une telle « erreur du système », touchant 175 personnes, majoritairement des élèves, à l'heure où les parents emmènent leurs enfants à l'école.

La phase opérationnelle des attaques militaires est un autre exemple de la manière dont les IA peuvent intégrer les guerres contemporaines. L'autonomisation des drones, des machines au sol, etc., requièrent que les machines puissent se déplacer sur les champs de batailles ou dans les airs. Elles nécessitent des capacités de « *computer vision* », c'est-à-dire des logiciels de traitement en direct des données captées par les caméras intégrées pour s'orienter ou éventuellement de reconnaissance faciale pour confirmer les cibles. À l'origine en 2017, le projet Maven était un contrat entre le Pentagone et Google pour développer des IA à partir des caméras équipées sur les drones. Ajoutons que le système d'armement Maven Smart System est un produit qui s'exporte : il a été acheté par l'OTAN, pour qui Palantir a développé une version spéciale, en partenariat avec le vendeur d'armes français Safran.

De plus en plus, ces systèmes d'armement deviennent des interfaces de commandement où un clic donne des ordres à des armes présentes sur le terrain. Les vidéos commerciales d'Anduril, (https://www.youtube.com/@Anduril/videos) mastodonte de la *defense tech* étatsunienne, permettent de bien se rendre compte, dans un marketing digne d'Apple ou de Coca-Cola, du fonctionnement de ces systèmes d'armes létales autonomes.

Les guerres récentes ont servi de rampe de lancement de ces technologies, aujourd'hui perçue comme centrale dans les nouveaux complexes militaro-industriels. Gaza, mais aussi la Cisjordanie et toute la Palestine, ou encore le Liban, ont servi de laboratoire à ciel ouvert. L'Etat sioniste est un des fers de lance de la recherche et du développement de logiciels de contrôle, de répression et de ciblage. Les noms de ces logiciels sont souvent d'un cynisme et d'une violence inqualifiable – l'un d'entre eux se nomme « *Where's Daddy ?* ». C'est un logiciel qui, suite à l'identification de la cible et l'identification de son domicile, capte les données des familles et proches de la cible afin de localiser la personne à abattre et déclencher l'attaque. L'un des logiciels qui permet l'identification des individus s'appelle Lavender (https://www.972mag.com/lavender-ai-israeli-army-gaza/) : le logiciel produit un « score » de dangerosité par individu étudié, et en fonction du score établi, le logiciel définit un nombre de victimes collatérales acceptables. Si ces personnes sont jugées importantes dans la résistance palestinienne, on estime que ce chiffre peut monter jusqu'à 300 victimes collatérales acceptables. Il est toujours utile de rappeler que l'expérimentation de ces technologies de contrôles (https://www.aljazeera.com/video/featured-documentaries/2025/1/30/the-palestine-laboratory-ep-1) sur le peuple palestinien précède largement le 7 octobre 2023.

La guerre en Ukraine a aussi été un terrain de jeu macabre des armateurs numériques. Il n'est pas toujours facile à analyser, notamment parce que la résistance du peuple ukrainien est importante et légitime. Mais en même temps, toute une partie du complexe militaro-industriel numérique s'est servi de ce contexte pour normaliser ces technologies, et les inscrire dans le « camp du bien », masquant la dimension inter-impérialiste du conflit. Par exemple, Elon Musk, à travers sa compagnie Space X, a pu démontrer l'utilité stratégique de sa constellation de satellites Starlink dans les conflits (https://www.lemonde.fr/international/article/2026/05/10/avec-starlink-elon-musk-a-gagne-la-bataille-des-satellites_6687693_3210.html), que ce soit dès le début en fournissant gratuitement[18] des milliers de satellites à l'armée ukrainienne, ou plus récemment, en coupant des accès au Kremlin. L'entrée en bourse de Starlink a été la plus importante entrée en bourse de l'histoire avec 75 milliards de dollars. La guerre en Ukraine a servi de pipeline à la normalisation de ces technologies, se faisant sur le dos de la résistance ukrainienne. Drones, bombes planantes, actions entièrement automatisées qui ont permis de reprendre des positions russes, (https://www.lexpress.fr/monde/europe/robots-tueurs-lukraine-experimente-la-guerre-sans-soldats-et-redessine-lart-de-la-guerre-)toutes les victoires ukrainiennes se traduisent en arguments de ventes grâce au logo « *combat proven* » qu'on voit estampillé dans les salons d'armements, « éprouvées au combat ». C'est d'autant plus cynique lorsque l'on sait qu'une bonne partie des armateurs numériques ou vendeurs de matériels *dual use*, à double usage, c'est-à-dire tant civil que militaire se sont arrangés pour contourner les sanctions et ont continué de vendre massivement à l'agresseur Russe.

Pour finir, l'agression contre l'Iran peut être perçue comme une occasion d'industrialisation de ces technologies, notamment à travers l'usage débridé du Maven Smart System. Il s'agit de la première utilisation à grande échelle de ce système pour des bombardements par l'armée étatsunienne. Mais c'est également la riposte qui a été intéressante : l'armée iranienne à très explicitement visé les

datacenters d'Amazon Web Services (https://fr.euronews.com/2026/07/21/iran-les-gardiens-revendiquent-lattaque-du-data-center-damazon-a-bahrein) au Bahreïn et aux Émirats Arabes Unis, elle a également menacé de frapper les positions du projet Stargate, projet phare de data center dédié IA dans le désert d'Abou Dhabi. Les data centers changent alors de nature, ils sont moins perçus comme « autoroute de l'information » que comme des bases militaires extérieure (https://ajuntament.barcelona.cat/digital/en/news/news/qui-mana-en-lera-digital-una-conversa-amb-cecilia-rikap-1615997)s.

Les data centers sont donc intégrés à la *kill chain*, ils sont une des pièces maîtresses de la possibilité des guerres contemporaines, et ils sont tous virtuellement mobilisables. Mais certains sont spécifiquement dédiés à devenir la boîte noire de ces opérations où la majeure partie des calculs et des puissances logicielles. De nombreux pays, comme la Belgique (https://www.rtbf.be/article/pourquoi-la-belgique-veut-elle-investir-un-milliard-dans-des-data-centers-militaires-pour-renforcer-sa-souverainete-numerique-11587457), annoncent des sommes toujours plus importantes pour la construction de data centers militaires. Leurs statuts juridiques bénéficient des mêmes statuts que les infrastructures militaires. Il est aujourd'hui urgent et nécessaire d'identifier ces data centers militaires et les projets porté dans le cadre des projets d'armements impériaux, mais il est aussi nécessaire de rappeler que virtuellement, tout data center peut être embrigadé dans la *kill chain*.

## Capitalisme de surveillance

Une grande partie de ces logiciels s'appuie sur des données dites « civiles », croisées avec d'autres données, issues de services de renseignement. Cela s'inscrit en continuité avec ce que l'universitaire étatsunienne Shoshana Zuboff appelle le capitalisme de la surveillance (https://www.zulma.fr/livre/lage-du-capitalisme-de-surveillance/). (https://www.zulma.fr/livre/lage-du-capitalisme-de-surveillance/)Suite à l'éclatement de la bulle spéculative autour d'Internet au tournant des années 2000, Google, entre autres, a initié un nouveau modèle économique qui a ensuite servi à structurer le fonctionnement global d'Internet. Tous les usages d'Internet (recherche, réseaux sociaux, application de rencontre ou de sport, etc.) et après des objets connectés (GPS, montre connectées, thermostats) produisent un surplus de données comportementales sur lesquelles d'autres entreprises vont pouvoir capitaliser. C'est là qu'une trajectoire technologique d'internet se déclenche avec l'objectif de stocker des quantités massives de données, qu'on va traiter, analyser, recomposer, interpréter avec divers objectifs commerciaux. Le premier c'est évidemment la publicité ciblée, qu'on connaît bien, mais ces ensembles de données ont aussi été au centre de l'attention des assureurs, des banquiers, et surtout des services de renseignements policiers et militaires (https://www.monde-diplomatique.fr/2019/01/ZUBOFF/59443). C'est la possibilité de recomposer et d'intégrer ces données à travers une interface facilement utilisable qui a fait le succès de Palantir.

Le jeu Pokemon Go est un exemple concret de ces logiques du capitalisme de surveillance qui ne se contentent plus de collecter le surplus de données comportementales, mais commence à conduire les comportements à produire des données. Cette appli a été lancée par John Hanke, responsable de Google Street View, qui a fondé Google Earth. Il a ensuite fait fortune grâce à cette application qui envoyait le monde entier filmer tous les coins de la planète connectée au service localisation de Google Maps, pour attraper un Pikachu, un Dracaufeu ou Mewtwo. Tout de suite, l'objectif est de faire faire à des millions de personnes ce qui coûterait trop cher à faire soi-même : une cartographie photographique participative sans que les participant·es ne soient au courant de ce qu'iels font. Ensuite, de nombreuses enseignes ont payé pour que des Pokémons apparaissent dans leurs établissements. Il y a un Rondoudou chez le glacier, on prendrait bien une boule ou deux, liant l'application au publicitaire. Mais surtout, toutes les données collectées pouvaient être utilisées pour de nombreuses fins commerciales. Une des fonctionnalités de Pokémon Go impliquait de scanner de manière précise des zones contre des récompenses. Ces scans 3D aujourd'hui ont été rachetés et servent désormais à entraîner des IA utilisées pour assister des drones militaires et orienter des militaires pour éviter l'usage du GPS, facilement brouillé sur le champ de bataille, notamment en Ukraine (https://www.leparisien.fr/international/ukraine/guerre-en-ukraine-comment-30-milliards-dimages-de-pokemon-go-sont-exploitees-pour-entrainer-une-ia-militaire-14-06-2026-V5LAPL3LCZFIRDEJJJW6POIM5I.php). La ligne de séparation entre le civil et le militaire est complètement brouillée.

C'est pour tous ces usages qu'il faut donc construire ces immenses capacités de stockage, de traitement, de connexions réseaux, contenus dans les data centers. C'est là qu'interviennent les services cloud : pour pouvoir extraire toujours plus de « surplus informationnels », il faut tout déplacer « en ligne », donc toute une série d'usages, comme les logiciels de bureautique, les jeux vidéos qu'on installait depuis un CD-Rom, le stockage de documents sur clé USB ou disque dur sont amenés à passer « en ligne » – c'est-à-dire dans le cloud. Le streaming de jeux vidéos, les services publics, et même toute une série de pratiques en dehors d'internet sont amenées à produire des données : Uber, e-shopping, France Travail, Airbnb, agriculture de précision, *smart homes*, doubles numériques, etc.

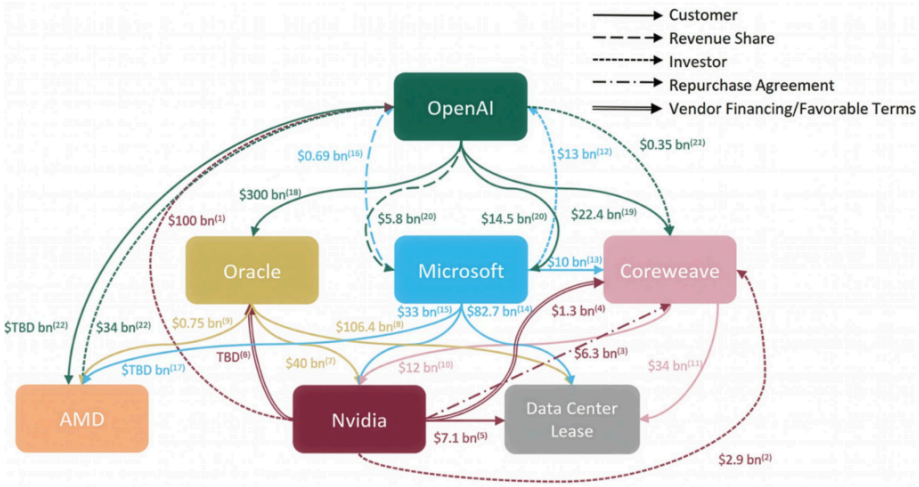
Toute cette plateformisation de l'économie produit une circulation intense d'informations en tout genre, potentiellement réquisitionnables. Ces choix économico-politiques ont fait d'Internet un ogre énergétique et métallier, mêlant intrinsèquement l'économie du numérique à celle de la surveillance commerciale, policière et militaire indistinctement. Rappeler la spécificité de cette trajectoire permet de rappeler que ce monde numérique-là est le fruit de sa trajectoire dans un mode d'organisation capitaliste, mais surtout, qu'il existe plein de réalité de ce monde numérique qui y résiste, et qu'il aurait pu en être autrement. Wikipédia, par exemple, grande encyclopédie contributive, le *peer-to-peer* (architecture de transfert de données sans système central), ou encore des sites comme celui de Low-Tech Magazine, qui indique en fond d'écran la météo à Barcelone où se situe le panneau solaire qui alimente le serveur hébergeant le site afin que l'utilisateur puisse anticiper ses usages, sont des exemples d'autres paradigmes technologiques, supports d'autres projets économico-politiques. Nous ne savons pas ce que ces paradigmes pourraient faire émerger s'ils étaient soutenus beaucoup plus massivement, notamment par les administrations publiques.

Il est central de savoir que cette trajectoire technique du numérique comme enjeux politique de première importance est pleinement théorisé par le *venture capitalist* comme Peter Thiel : sa stratégie assumée est d'investir dans toutes les start-ups qui permettent d'assurer la « suprématie occidentale », allant des start-ups militaires aux plateformes dérégulant le droit du travail, voir permettant de se passer des travailleurs eux-mêmes, fonctionnaires d'état compris. Cette stratégie d'orientation du développement technologique doit permettre à l'Occident de faire émerger une élite à même d'assurer une domination mondiale[19].

## Économie en circuit fermé, bulle spéculative et coussin militaire[20]

Ce que cette analyse permet également de visibiliser, c'est la place singulière du secteur numérique dans l'économie contemporaine : la trajectoire technique spécifique du numérique dominant est à la fois cause et effet des contradictions internes du capitalisme mondial. C'est ce qui pousse le chercheur en sciences de l'information et de la communisation Nikos Smyrnaios (https://www.contretemps.eu/au-dela-du-techno-feodalisme-pour-une-critique-de-limperialisme-numerique/) à développer une analyse de l'« impérialisme numérique », qui serait la réponse à la situation actuelle qu'on peut analyser comme tension entre stagnation économique, période intense d'innovation numérique, déstabilisation des démocraties libérales et remilitarisation des relations internationales.

Cette tension se matérialise, entre autres, à travers la bulle spéculative de l'IA. Pour le moment, les leaders de l'IA, Open AI, Anthropic ne génèrent pas de revenus, et perdent même plusieurs milliards de dollars par an. On peut se référer au schéma de Morgan Stanley « AI Ecosystem Flow », sur lequel on voit les flux financiers délirants ; on y observe Nvidia, fabricant des puces dédiées à l'IA, qui finance Open AI, qui construit des modèles d'IA, qui promet d'acheter des espaces de stockage cloud à Oracle, qui promet d'acheter des puces à Nvidia. L'économie circulaire de l'IA brasse des montants financiers délirants, (https://www.lemonde.fr/economie/article/2025/10/26/intelligence-artificielle-la-folle-circulation-des-milliards-qui-nourrit-le-secteur-et-fait-craindre-une-bulle_6649648_3234.html?srsltid=AfmBOoqqCpqOvwI8WwfIMpKDu84Odd3-pxxNxofBCyX_qvGchjWPQdlP) comme l'illustre le schéma présenté ci-dessous, qui permettent *in fine* le lancement de tous ces projets de data center. Elle fonctionne sur des investissements qui comptent sur des promesses de profits et de gains de productivité futurs. Le capital se valorise dans des revenus espérés pour une fiction de croissance et de rentabilité mystérieuse (https://www.contretemps.eu/destruction-capital-fictif-bulle-intelligence-artificielle-mystere-rentabilite/). C'est pourquoi de nombreuses personnes avancent que la bulle va éclater.




Ce schéma de Morgan Stanley (https://www.morganstanley.com/im/en-us/individual-investor/insights/articles/bull-and-bear-investment-cases.html) illustre les mécanismes d'autofinancement de la bulle de l'IA, ses flux financiers circulaires et interdépendances.

Mais, les Palantir, Google, Microsoft, etc., ont un filet de sécurité : les États sont devenus trop dépendants de ces entreprises pour leurs fonctions régaliennes, et ont rendu leurs industries trop dépendantes.Ainsi, si la bulle éclate, elles seront considérées comme « *too big to fail* » (comme les banques systémiques en 2007-2008) et les États viendront à leur rescousse. Lors d'une présentation publique, la directrice commerciale d'OpenAI, en réponse à une question sur les risques économiques, a répondu que l'entreprise avait des « garanties fédérales », avant de se rétractée suite à un tollé. Mais cela révèle bien que ces grandes entreprises sont tellement intégrées au fonctionnement des puissances gouvernementales, qu'elles savent que l'État leur servira de coussin de sécurité, notamment lors de la crise économique qui pourrait survenir suite à l'éclatement de la bulle spéculative. À l'instar de la crise financière de 2008, celles et ceux qui paieront les conséquences de la crise seront ceux qui ne sont pas nécessaires à la puissance de l'État.

**Le nuage nous intégrait à l'empire**

Pour finir, il paraît important de préciser le rôle tout à fait singulier des opérateurs *cloud* dans l'écosystème numérique contemporain, à la fois du point de vue militaire mais aussi en tant qu'acteurs clé du développement de l'empire numérique. Les « *clouders* », les fournisseurs de services et d'infrastructures *cloud,* sont bien connus, mais pas toujours en tant que tels. Dans l'ordre d'importance en termes de part de marché, on trouve : Amazon Web Services, Google Cloud et Microsoft Azure, puis, dans une moindre mesure, Ali Baba (surtout grâce au marché Chinois). Dans une stratégie d'intégration verticale, ces acteurs investissent en propre dans la construction de data center et de câbles sous-marins, même s'ils louent également des espaces dans des data centers de colocation (comme ceux de Equinix ou Digital Realty) et qu'ils utilisent les câbles construits par de grands consortium.

Comme nous l'avons vu plus haut, les capacités des *clouds* sont aujourd'hui vitales pour le fonctionnement des armées : que ce soit les suites logicielles de bureautique ou le stockage et traitement de données, les opérateurs cloud sont aujourd'hui en lien avec les pires armées du monde, dont évidemment l'armée israélienne. De nombreux contrats de *cloud* sont aujourd'hui au cœur de mouvements sociaux importants comme le mouvement « No tech for apartheid », qui visent à l'annulation d'un contrat reliant Google et Amazon à l'armée et au gouvernement israélien. Ces contrats sont nécessaires, non seulement aux nouveaux systèmes d'armements comme évoqué, mais aussi au fonctionnement même des armées : logiciels de bureautique, organisation, communication. Si l'on prend le temps d'écouter les conférences « IT for IDF », différents responsables israéliens insistent régulièrement sur la nécessité des capacités clouds, sans lesquelles ils n'auraient jamais pu tenir la cadence de leurs opérations, ne serait qu'en termes d'organisation du travail. Leurs contrats avec les *clouders* est central dans les outils et le management du projet génocidaire à l'encontre du peuple palestinien. La rapporteuse spéciale des nations unies sur les territoires palestiniens occupés Francesca Albanese, a ainsi rendu un rapport (https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session59/advance-version/a-hrc-59-23-aev.pdf) le 30 juin 2025 nommant explicitement la complicité des opérateurs cloud dans le génocide en cours à Gaza.

Précisons ici que cette complicité n'est pas accidentelle : les opérateurs cloud n'ont pas décidé de se mettre par opportunisme dans le champ militaire, mais, pour le dire avec les mots de l'économiste Claude Serfati, la relation entre numérique et militaire est devenue *organique* (https://www.contretemps.eu/systemes-militaro-industriels-noyau-totalitaire-capitalisme/). Les quelques traits de la logique du capitalisme de surveillance présentés plus haut permettent de saisir cette relation. Cette co-évolution entre les deux secteurs est constitutive : si le militaire a besoin de technologies de guerre disruptives pour garder un avantage comparatif (ou le rattraper), il a besoin des capacités technologiques des big tech, et notamment de son infrastructure permettant la recherche et le développement. Les opérateurs cloud, eux, ont besoin de ces investissements, et surtout du marché captif que constituent les armées[21]. Le secteur militaire oriente le secteur recherche et développement, et en contrepartie les opérateurs cloud bénéficient de la puissance militaire pour la sécurisation de sa chaîne de production et de ses marchés.

Ce pouvoir de capture technique des *clouders* ne s'arrête pas au champ militaire. Tout utilisateur de services cloud externalise ses capacités de stockage, calcul et transmission de données. Lors de l'émergence des premiers data centers, et donc de la possibilité d'externalisation de services numériques, ces services étaient souvent envisagés comme de simples technologies d'information et de communication, plutôt périphérique à l'activité centrale des entreprises. L'externalisation semblait donc être une simple sous-traitance. Aujourd'hui, les capacités de calculs rentrent au cœur des process industriels et finissent par prendre un rôle toujours plus central dans la gestion publique, domestique et privée. À travers la rente intellectuelle sur les capacités logicielles ou l'accès à de larges bases de données (https://www.econstor.eu/bitstream/10419/280831/1/1850871124.pdf), la mise en dépendance infrastructurelle par la dépendance aux serveurs nécessaires pour faire tourner les services numériques, à travers les places de marché qu'ils détiennent, le *cloud* devient un outil de mise en dépendance. La stratégie de Google, Amazon et Microsoft est la migration intégrale des activités informatiques vers leur cloud (45% des activités numériques sont estimées avoir lieu sur le *cloud* en 2025).

Parmi ces activités à faire migrer sur le *cloud*, celles des services des États sont particulièrement prisées. Il constitue à la fois une manne financière très importante et un levier de mise en dépendance immense[22], et la signature de contrats de cloud entre les gouvernements et les *clouders* occupe une bonne partie des lobbyistes. Plus les États, les entreprises et les usagers rejoignent le *cloud*, plus le *cloud* devient un haut lieu de production de valeur, mais aussi de capacités d'innovation, recherche et développement, et par la suite de mise en dépendance envers ces technologies émergentes qui s'imposent comme nécessaire. C'est aussi à ce titre-là que le numérique semble particulièrement central dans la stratégie impérialiste US actuelle. L'exportation de capitaux pour la construction de ces infrastructures *cloud* à travers l'Europe relève, en profondeur, de cette stratégie, même si elle se pare de l'imaginaire fallacieux de la souveraineté numérique.[23]

Les opérateurs *clouds* deviennent une des forces constitutives de l'impérialisme étatsunien actuel, à la fois en tant que parfaitement intégrée à la puissance coercitive militaire, et à la fois, en tant que puissance économique de vassalisation de différentes fractions de classe à travers le monde. Cette vassalisation transparaît dans différentes législations (https://synthmedia.fr/international/ia-act-regulations-internationales/cloud-souverain-bruxelles-sovereignty-washing/), étatsuniennes comme européennes. Il paraît intéressant de reprendre ici les quelques analyses proposées par Marlène Rosato (https://www.contretemps.eu/sortir-lanti-imperialisme-moral-desoccidentaliser-france/) sur la façon dont les investissements étatsuniens directs à l'étranger (IDE) servent à la production d'une bourgeoisie intérieure en Europe, dont les intérêts sont alignés sur les intérêts de la bourgeoisie étatsuniennes.

Les capacités actuelles de projection internationale de la bourgeoisie européenne dépendent de la réussite des entreprises étatsuniennes. Cela s'observe particulièrement dans le secteur numérique qui représente une part croissante des IDE étatsuniens en Europe, et en grande partie, pour la création de data center (https://www.somo.nl/eus-data-centre-expansion-will-fast-track-profits-and-power-for-us-big-tech-and-investors/). Les projets de Google à Châteauroux, ou à Farciennes en Belgique, de Digital Realty en Île-de-France et à Marseille, ou le projet Campus IA à Fouju, tout autant que les nombreux projets Microsoft ou Google au Nord des Pays-Bas (https://thehmm.nl/event/the-hmms-data-centre-tour-2/), ou encore les projets de Meta en Espagne (https://tunubesecamirio.com/2025/03/24/macrogranjas-de-datos-meta-en-talavera-de-la-reina/), apparaissent donc comme l'une des matérialisations contemporaines, particulièrement saillantes, du renouvellement et des mutations de l'intégration de l'Europe à la chaîne impérialiste étasuniennes.

## Conclusion

Aujourd'hui, les data centers sont construits massivement, et sont toujours plus grands. Si la bulle spéculative éclate, il est possible que ces grands hangars en béton ne se remplissent pas. Nous aurions peut-être alors de drôles de ruines dans des campagnes dépeuplées à qui on avait promis monts et merveilles – quelques emplois de sécurité et quelques taxes permettant la construction d'une nouvelle piscine ou d'une nouvelle piste cyclable[24]. Mais il est certain que seront sauvées les parties de l'infrastructure nécessaire à la reproduction du capitalisme de surveillance et au maintien de la puissance militaire impériale.

Le mouvement contre les data centers prend en ampleur aux États-Unis et en Amérique du Sud ; il se forme en Europe et dans de nombreuses régions d'Asie. L'imbrication de ces infrastructures avec le complexe militaro-industriel rend la lutte ardue, mais elle demande aussi des alliances rigoureuses et exigeantes.

Il existe aujourd'hui en France un nombre croissant de collectifs qui abordent le travail de la lutte contre l'expansion des data centers depuis une perspective territoriale[25], reprenant tout le répertoire d'actions développés dans les luttes locales : contestations juridiques, manifestations, pressions sur les élus locaux, etc. Les arguments les plus perceptibles qui percent médiatiquement sont souvent ceux qui permettent la contestation juridique et locale : consommation électrique, foncière, nuisance sonore, pollutions, le peu d'emploi. À côté de ces collectifs, d'autres luttes émergent issues de divers mondes professionnels impactés par l'arrivée de l'IA générative (artistes, traducteurs, graphistes, développeurs, etc.) ou par les IA agentiques (travail social, fonction publique, enseignement, etc.)[26], probablement rejoints prochainement par les travailleurs de l'industrie (de plus en plus de développeurs de systèmes IA travaillent à des systèmes permettant d'optimiser les processus industriels)[27]. Certaines composantes syndicales entrent dans la bataille et ce sont d'autres répertoires de luttes qui peuvent dès lors être convoqués, en prenant appui sur l'histoire longue des stratégies pour défendre le travail contre le capital.

D'autres collectifs, déjà engagés dans des campagnes de long cours autour des libertés fondamentales sur le net[28], partisans du logiciel libres, ou communauté de *permacomputing*[29] ou industriels de la « *fairtech* »[30], travaillent déjà à faire exister des alternatives possibles, matérielles, culturelles, législatives pour un Internet plus désirable. Si souvent ces alternatives sont aujourd'hui insuffisantes pour créer un numérique réellement éthique, hors de toutes logiques impérialistes, il n'en reste pas moins qu'elles indiquent des voies technologiques possibles[31]. Pour une bonne partie de ces organisations, il semble impératif de penser les liens avec les nombreux collectifs organisés contre l'extractivisme, sur le territoire français, et surtout ceux qui cherchent à construire politiquement les responsabilités des entreprises et dirigeants du Nord Global concernant l'extractivisme minier rendu nécessaire par le déploiement massif d'infrastructures numériques.[32]

Pour penser des points de ralliements de ces multiples mouvements, divers élus, ONG ou collectifs cherchent à construire l'hypothèse d'un moratoire sur la construction de data centers (à échelle communale, nationale ou européenne), ou de formes type « convention citoyenne » pour le numérique pour contrer la dérégulation rapide en œuvre autour de l'implantation de data centers. D'autres encore cherchent à tenir ensemble les organisations de la chaîne de production de l'IA en soutenant l'action des collectifs dans les zones du monde concernées[33]. L'initiative portée par une coalition de mouvements politiques allemands « Cables of resistances » (https://cableresist.de/) proposait un week-end de mobilisations et de discussions autour de neuf « pistes » de résistance à la Big Tech – politique urbaine, eau et matière première, travail, climat et énergie, militarisation, fascisme, féminismes, futurs et arts. Le week-end avait rassemblé près d'un milliers de personnes afin de donner une opportunité à l'articulation stratégique entre ces différents pistes.

Nous ne pouvons citer ici tout ce qui se met en mouvement autour des enjeux que posent les data centers en tant que matérialisation concrète des diverses problématiques que peuvent soulever l'expansion actuelle rapide des infrastructures du numérique dominant[34]. Nous souhaitons ici, en lien avec le travail que nous menons avec d'autres, comme les collectifs Equinox (https://equinox.shiftx.space/)[35] ou Lignes Anti-impérialistes (https://lecturesantiimperialistes.org/)[36], suggérer aux collectifs engagés dans des luttes anti-militaristes et anti-impérialistes que leur participation dans la construction de ce mouvement est de première importance. Nous invitons également le mouvement contre l'expansion des data centers à penser son action à partir de la richesse théorique et stratégique des luttes anti-guerre et anti-impérialistes.

*

*Ce texte reprend pour partie une intervention d'Antoine Devillet dans le cadre de la table ronde intitulée « L'écologie sociale à l'épreuve de la guerre » (aux côtés de Soraya El Kahlaoui, Alexis Cukier et Vincent Rissier) lors du Festival du Livre Indépendant et politique le 7 juin 2026 à Marseille.*

# Notes

[1] Surnommé le gestionnaire foncier d'internet, Digital Realty est un fonds d'investissement immobilier étasunien (REIT) spécialisé dans la construction et la gestion de data centers. Tel un promoteur immobilier le fond construit l'enveloppe du data center et loue des salles informatiques dans lesquelles ses « locataires » qui vont des gouvernements aux big tech, en passant par les géants du e-commerce et du streaming viennent poser leurs serveurs. La multinationale fait partie des leader mondiaux du secteur et possède 18 data centers en France, dont 5 à Marseille où sont notamment hébergés les clouds de Amazon, Microsoft, Google et Oracle.

[2] Le nombre de 19 peut sembler minime au regard des 600 câbles de fibre optique sous-marins existants ou en cours de pose actuellement dans le monde. En réalité ces 600 câbles, qui supportent 99% du trafic internet, sont de tailles et capacités très diverses. Certains font quelques centaines de kilomètres et ont un faible débit, quand d'autres en font des millions et peuvent transporter des milliards de données à la seconde. A titre de comparaison, il y avait, en 2023, 11 câbles internet entre les Etats-Unis et l'Europe. La spécificité de Marseille est que la plupart des 19 câbles font partie des plus stratégiques du monde. Quelques exemples : le câble 2AFRICA, « le câble le plus long du monde », copropriété de Meta, dont les 45 000 km et les 16 paires de fibre optique relient 33 pays, l'ensemble des pays côtiers du continent Africain avec l'Asie et l'Europe et la région SWANA ; ou encore le câble PEACE, long de 25 000 km initié par China Mobile qui relie l'Europe, Afrique et Asie du Sud Est ; enfin le câble BLUE - RAMAN, initié par Google et qui relie l'Inde, la région SWANA et l'Europe en passant par Israël.

[3] Voir le travail de la chercheuse Camille Morel, *Les câbles sous-marins*, Paris, CNRS Editions, 2023

[4] Gérard Fouchard, « Les télécommunications sous-marines en Méditerranée occidentale entre 1850 et 2002 », *Actes des congrès nationaux des sociétés historiques et scientifiques*, n°*128*, 2009.

[5] Le réseau satellitaire est historiquement très marginal, même si les acteurs comme Starlinks cherchent à changer la donne.

[6] C'est le terme employé par les industriels, notamment Digital Realty pour parler de la chaîne de fabrication d'une donnée. En effet, une donnée, à l'image d'un produit manufacturé, est composée d'une multitude de services fabriqués par différents prestataires (trackers publicitaires, IA, cybersécurité, interconnection telecom ...) qui sont assemblées dans l'usine qu'est le data center, et c'est cette agrégation qui crée de la valeur.

[7] Google Cloud représente 15 % du chiffre d'affaires d'Alphabet, le Search et AdWords restant de loin les moteurs des profits du groupe. Les services « intelligent cloud », incluant le cloud Azure de Microsoft représentent 37 % de son chiffre d'affaires en 2025.

Les enjeux de la permanence coloniale des infrastructures du numérique en Afrique sont gigantesques et dépassent largement le cadre de cet article, mais nous pouvons a minima mentionner le concept d'« *infrastructure-as-debt* » avancé par Admire Mare, professeur associé au département de la communication et des médias de l'université de Johannesburg, en Afrique du Sud. Ce concept permet de contester l'idée d'« *infrastructure-as-service* » et de visibiliser le pouvoir que les gestionnaires d'infrastructures ont sur la politique africaine, notamment les élections.

[9] La puissance installée du parc nucléaire en France par EDF représente 61,4 GW. En janvier 2026, la ministre a annoncé que la puissance électrique recherchée par les projets de data center était de 28,6 GW.

[10] Pour une étude précise autour des enjeux de consommation en eau des data center voir https://hubblo.org/fr/articles/data-center-water-consumption-assessment/ (https://hubblo.org/fr/articles/data-center-water-consumption-assessment/)

[11] Une étude de Cambridge menée entre 2004 et 2024 sur 8 400 data centers dans le monde révèle que la chaleur qu'ils génèrent fait augmenter la température alentour de 2 degrés en moyenne, jusqu'à 9 degrés dans certains cas. Ces îlots de chaleur peuvent modifier la température sur une dizaine de kilomètres autour du data center.

[12] Pour une compréhension générale des enjeux miniers, en lien avec le numérique et leurs chaînes d'approvisionnement voir le texte de Célia Izoard qui sert d'introduction à l'ouvrage coordonné par le collectif Stop Micro, Anatomie d'une puce : https://www.terrestres.org/2026/06/01/peut-on-relocaliser-lempire/ (https://www.terrestres.org/2026/06/01/peut-on-relocaliser-lempire/) ou l'article de Gauthier Roussilhe, *Les GPU et IA génératives : une nouvelle phase de l'histoire environnementale de la numérisation* : https://gauthierroussilhe.com/articles/la-phase-g-les-gpu-et-les-ia-generatives-comme-nouvelle-phase-de-l-histoire-environnementale-de-la-numerisation-partie-1 (https://gauthierroussilhe.com/articles/la-phase-g-les-gpu-et-les-ia-generatives-comme-nouvelle-phase-de-l-histoire-environnementale-de-la-numerisation-partie-1)

[13] Notons tout de même les réserves de la France, peu documentées. (https://www.globaltimes.cn/page/202606/1364438.shtml)

[14] Selon Marko Mann, dans son article du 23 janvier 2026, *La destruction créancière du capital fictif. Bulle de l'intelligence artificielle et mystère de la rentabilité,* (https://www.contretemps.eu/destruction-capital-fictif-bulle-intelligence-artificielle-mystere-rentabilite/) « Le capital se tourne vers l'IA parce qu'il ne trouve plus d'opportunités suffisantes ailleurs. La machine d'accumulation rencontre ses limites. Les taux de profit réels stagnent, les gains de productivité plafonnent et la planète n'offre plus de nouvelles zones de pillage. Alors il investit dans la promesse d'une valeur à venir. L'IA sert de terrain d'atterrissage pour des masses de capital qui ne peuvent plus se valoriser dans la production *réelle*. »

[15] Voir Sylvie Laurent, *La Contre Révolution Californienne*, Le Seuil, 2025, ou extraits choisis publié sur https://www.contretemps.eu/contre-revolution-californienne-sylvie-laurent/ (https://www.contretemps.eu/contre-revolution-californienne-sylvie-laurent/)

[16] Les péripéties récentes autour du Maven Smart System ont montré l'ambiguïté des relations entre fournisseurs de Grands Modèles de Langages et le gouvernement Américain, entre bonne conscience et co-dépendance, voir l'article de Félix Tréguer, « La bonne conscience de la Silicon Valley (https://www.monde-diplomatique.fr/2026/05/TREGUER/69543) ».

[17] Félix Tréguer, « La bonne conscience de la Silicon Valley », *Le Monde Diplomatique*, mai 2026 https://www.monde-diplomatique.fr/2026/05/TREGUER/69543

[18] Le Pentagone puis la Pologne ont ensuite pris le relai et financé les satellites Starlink, devenus payants.

[19] Leur stratégie est souvent qualifiée de « technofascisme » pour décrire un autoritarisme qui passerait directement par l'imposition de nouvelles technologies, en contournant l'espace politique classique, voir Technofascisme, le nouveau rêve de la suprématie blanche de Norman Ajari. Il est important de noter que si certains acteurs, notamment les étatsuniens, sont très explicites concernant le projet idéologique qui sous-tend les technologies qu'ils mettent sur le marché, d'autres, comme certaines figures de la tech européenne ou française, produisent exactement le même type de technologies en les drapant d'un discours qui cherchent à la rendre plus acceptable, notamment à travers la notion de souveraineté.

[20] Cette partie doit beaucoup aux discussions avec Marko Mann, économiste.

[21] Voir par exemple le Joint Warfighting Cloud Capability (https://en.wikipedia.org/wiki/Joint_Enterprise_Defense_Infrastructure) ou le Wild and Stormy entre la NSA et Amazon (https://federalnewsnetwork.com/reporters-notebook-jason-miller/2022/04/nsa-quietly-reawarded-its-wild-and-stormy-cloud-contract/)

[22] En mars 2026, les ministères français de l'enseignement supérieur et de la recherche, de l'éducation nationale et des sports, de la jeunesse et de la vie associative ont confirmé prolonger jusqu'en 2029 un accord-cadre les liant avec Microsoft. Ce marché public, plafonné à 152 millions d'euros, permet à la Big Tech étasunienne d'installer ses logiciels et services associés, dont Windows et Office sur plus d'un million d'ordinateurs de travail et serveurs du personnel de l'Education Nationale.

[23] Selon le rapport EuroStack, entre 80 et 90 % des services de cloud computing utilisés par les clients européens sont hébergés par des entreprises basées aux États-Unis. La Commission européenne a qualifié cette situation de dépendance stratégique.

[24] C'est en tous cas l'hypothèse que la chercheuse canadienne Anne Pasek mets au travail dans diverses conférences, voir son intervention à la discussion : Reclaiming the Cloud ! Au Weizenbaum Institute de Berlin. (https://www.youtube.com/watch?v=UzkhnVHtAbc)

[25] Voir la carte réalisée par notre collectif des collectifs opposés au data center : https://lenuageetaitsousnospieds.org/articles/2025-12-11-carte-des-data-centers-des-projets-et-des-contestations-en-france.html (https://lenuageetaitsousnospieds.org/articles/2025-12-11-carte-des-data-centers-des-projets-et-des-contestations-en-france.html) Ici, plus d'une trentaine de luttes locales sont répertoriées, chacune développant des stratégies qui leurs sont propres, tout en cherchant à se coordonner. En Belgique, en Espagne (https://tunubesecamirio.com/), en Allemagne (https://heisseluft.org/), des cartes similaires sont produites ou en cours de production.

[26] Voir par exemple, le contre-sommet de l'IA organisé par le collectif en chair et en os, qui alliait questions écologiques, au questions de productions de savoirs et aux questions de travail : https://enchairetenos.org/anti-sommet-de-lia-a-lille-recit-dune-journee-de-discussions/ (https://enchairetenos.org/anti-sommet-de-lia-a-lille-recit-dune-journee-de-discussions/)

[27] Voir Juan Sebastian Carbonell, *Un taylorisme augmenté, une critique de l'intelligence artificielle,* Amsterdam, 2025. où l'auteur conclue en appelant à un renouveau du luddisme, en référence aux « briseurs de machines » textiles de l'Angleterre du début du 19eme siècle.

[28] En France, nous avons par exemple la Quadrature du Net (https://www.laquadrature.net/), en lien avec le réseau européen EDRi (https://edri.org/).

[29] Le terme Permacomputing renvoie à la fois à une communauté spécifique, et à un champ de pratiques assez diversifiés, qui ne se revendiquent pas spécialement du « permacomputing » mais qui à le mérite de faire sentir assez rapidement qu'il s'agit de penser des alternatives à l'internet dominant, structurellement et localement plus compatible avec les écosystèmes, en reprenant des principes de dé-centralisation, de circularité, de complémentarité, de diversité, etc. D'autres terminologies utilisées sont « low tech », technologie régénérative, etc.

[30] L'une des plus connues est sans doute Fairphone, nous vous suggérons de lire l'entretien réalisé par le collectif Stop Micro avec Agnès Crépet, ingénieure à Fairphone, dans leur livre *Anatomie d'une puce, semi-conducteurs, l'impossible relocalisation, Monde à l'envers, 2026*, permettant de mieux saisir la réflexion stratégique qui sous-tend l'entreprise Fairphone.

[31] Le rapport *Reclaiming Digital Sovereinty, a road map to build a digital stack for people and the planet*, coordonné par Cecilia Rikap, Cédric Durand, Edemilson Paraná, Paolo Gerbaudo et Paris Marx, constitue une feuille de route intéressante pour penser la possibilité politique de développer ces alternatives.

[32] L'association Survie, par exemple suggère de faire appliquer le devoir de vigilance concernant les conditions d'extractions minières desquelles dépendent les entreprises de la Tech. L'association *Génération Lumière* a porté une campagne contre le protocole d'accord entre l'Union Européenne et le Rwanda sur les métaux critiques, importés illégalement depuis les zones minières sous occupation du M23.

[33] Par exemple, la coalition CHIPS communities united (https://chipscommunitiesunited.org/) met en place des campagnes transnationales, en lien avec les communautés travaillant ou étant impactée par la production des semi-conducteurs, notamment à Taiwan et en Corée du Sud ou le DiPLab research Group, acronyme pour Digital Platform Labour, qui étudie et politise à échelle internationale les conditions de vie des travailleurs du clic, nécessaire au fonctionnements de IA, et à de nombreux services numériques, notons également le travail remarquable du collectif STopMicro, dans son tissage avec les collectifs anti-extractivistes.

[34] Nous avons publié l'article « construire des luttes contre les infrastructures du numérique » qui reprenait une intervention aux AMFIS 2025 : https://lenuageetaitsousnospieds.org/articles/2025-08-26-construire-des-luttes-contre-les-infrastructures-du-numerique.html (https://lenuageetaitsousnospieds.org/articles/2025-08-26-construire-des-luttes-contre-les-infrastructures-du-numerique.html) où nous tentions déjà de renvoyer vers une multiplicité de manière de lutter. Nous pouvons encore renvoyer au travail de Commission d'enquête parlementaire sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France (https://www.assemblee-nationale.fr/dyn/17/organes/autres-commissions/commissions-enquete/ce-vulnerabilites-numeriques), portée notamment par la Députée Cyrielle Chatelain, au travail de production de données précises et utiles de l'équipe d'experts Hubblo (https://hubblo.org/fr/), le travail de journalisme d'investigation mené par l'Observatoire des multinationales (https://multinationales.org/fr/), ou encore l'important travail de coordination réalisé par Data For Good (https://dataforgood.fr/).

Direction de la publication : Fanny Gallot & Hugo Palheta. ISSN : 2496-5146

[35] Organisation queer et féministe pour une justice raciale, pour une société du « care » et non du contrôle, très impliquée dans la création de liens entre mouvements de résistances à la Big Tech et mouvements antiracistes et décoloniaux.

[36] Collectif d'éducation populaire et groupe de lecture autour de l'économie politique et les théories marxistes de l'impérialisme.