COMITÉ : UIT - Infrastructure numériques critiques
PROBLÉMATIQUE : Comment assurer la souveraineté numérique des États face à leur dépendance croissante envers des infrastructures numériques contrôlées par des entreprises privées transnationales ?
PRÉSIDENTS : Mathilda REY, John-Tyler DUPEROY, Maya YANKOVSKAYA

PRÉSENTATION DE LA PRÉSIDENCE



Bonjour à tous chers délégués.
Je m'appelle John-Tyler Duperoy et j'ai 16 ans, je suis né dans la ville de Nîmes dans le département du Gard et j'ai toujours vécu en France.
Je suis ravi d'être votre président de comité, pour ce FerMUN 2027. Passionné par les affaires publiques et la vie politique, je souhaite intégrer Sciences Po puis l'INSP. Dans cette perspective, j'ai déjà réalisé plusieurs stages, notamment au Sénat et à l'Assemblée nationale.
Lors de ce FerMUN 2027, nous traiterons d'un sujet primordial : la souveraineté numérique des États face aux grandes entreprises privées transnationales. Car ce sujet nous concerne directement, que ça soit pour nos services publiques ou encore pour nos données numériques sensibles et personnelles. Un débat qui sera marqué par les fortes dépendances aux outils numériques des États, dans un monde où tout est connecté, je me réjouis à l'idée des débats que nous aurons.



Bonjour à tous, chers délégués.
Je m'appelle Maya, j'ai 16 ans et je suis dans le programme du diplôme de l'IB à Toronto French School, au Canada. J'ai grandi en Lettonie avant de déménager à Toronto il y a quelques années, et je parle anglais, russe et letton en plus du français.

Je m'intéresse particulièrement aux liens entre l'économie, la technologie et la politique internationale. C'est ma deuxième année de MUN : j'ai déjà eu l'occasion de voyager au Maroc pour une conférence, ainsi que de participer à des conférences provinciales et nationales. En dehors de l'école, je joue au volley-ball et je fais du piano. J'espère que vous aborderez ces questions avec curiosité et rigueur, je suis convaincue que vos idées rendront ce comité mémorable !

MOTS-CLÉS

Souveraineté numérique : capacité d'un État à maîtriser ses infrastructures numériques, ses données, ses technologies stratégiques et les règles qui encadrent leur utilisation, afin de ne pas dépendre d'acteurs privés ou de puissances étrangères.

Infrastructure numérique critique : ensemble des éléments indispensables au fonctionnement d'Internet : câbles sous-marins, data centers, clouds, satellites, serveurs DNS, semi-conducteurs. Leur défaillance peut perturber des services publics essentiels.

Hyperscaler : entreprise qui fournit des services cloud à très grande échelle (comme AWS, Microsoft Azure ou Google Cloud). Ces acteurs dominent le marché mondial du cloud et hébergent une grande partie des données publiques et privées.

Vendor lock-in : situation où un client devient dépendant d'un fournisseur technologique, ce qui rend le changement difficile ou coûteux. Cela limite la capacité d'un État à modifier ses infrastructures numériques.

Cloud souverain : cloud conçu pour garantir que les données sensibles d'un État sont hébergées selon ses propres règles, avec un contrôle national sur la sécurité, l'accès et la localisation des données.

Résilience numérique : est la capacité des infrastructures numériques à résister aux cyberattaques, aux pannes, aux catastrophes ou aux crises, tout en maintenant les services essentiels et en permettant leur rétablissement rapide.

Clarifying Lawful Overseas Use of Data Act (Cloud Act)[1] : loi américaine qui oblige les entreprises américaines à fournir des données aux autorités des États-Unis, même si ces données sont stockées dans un autre pays.

Règlement Général sur la Protection des Données (RGPD)[2] : règlement européen qui protège les données personnelles des citoyens, en imposant des règles strictes sur la collecte, l'utilisation et la conservation des données.

---

[1] |Texte Cloud Act: https://www.congress.gov/bill/115th-congress/house-bill/4943/text

[2] |Texte RGPD: https://www.cnil.fr/fr/reglement-europeen-protection-donnees

Semi-conducteurs : composants électroniques indispensables à tous les appareils numériques (smartphones, ordinateurs, serveurs, IA). Leur production est concentrée dans quelques pays, ce qui crée une dépendance mondiale.

Internet Corporation for Assigned Names and Numbers (ICANN)[3] **:** organisation internationale qui gère les noms de domaine et les adresses IP, garantissant la stabilité et l'unicité du système d'adressage d'Internet.

La Conférence des Nations Unies sur le commerce et le développement (CNUCED)[4] **:** est l'organe principal de l'Assemblée générale de l'ONU fondé en 1964 pour aider les pays en développement à s'intégrer dans l'économie mondiale.

[3] | https://www.icann.org/fr

[4] | https://unctad.org/fr

APERÇU GLOBAL

Un nouvel enjeu stratégique de souveraineté numérique

La transformation numérique a rendu les infrastructures numériques essentielles au fonctionnement des États, de leurs économies et de leur sécurité. Selon l'Union Internationale des Télécommunications (UIT), près de 5,5 milliards de personnes utilisaient Internet en 2024[5]. Pourtant, le contrôle de ces infrastructures est exercé de manière croissante par un nombre restreint d'entreprises privées transnationales.

Les États cherchent donc à renforcer leur souveraineté numérique tout en maintenant un Internet ouvert. La souveraineté numérique devient ainsi un enjeu majeur de sécurité et de compétitivité.

Des infrastructure mondiales, contrôlées par peu d'acteurs privées

Internet repose sur des infrastructures physiques et logicielles : câbles sous-marins, centres de données, satellites, services cloud et semi-conducteurs. Une grande partie de ces infrastructures est contrôlée par quelques entreprises privées transnationales, principalement américaines et chinoises, ce qui crée une dépendance pour les États.

Près de 99 % du trafic mondial passe par des câbles sous-marins[6]. Plusieurs câbles stratégiques sont financés par des entreprises privées :

- Google a financé : Dunant (États-Unis–France), Grace Hopper (États-Unis–Royaume-Uni–Espagne) et Equiano (Portugal–Afrique du Sud)
- Meta a financé : 2Africa, qui fait le tour du continent africain
- Amazon participe au financement du câble Hawaiki Nui (liaison dans le paciifique)

Ces câbles transportent les données des gouvernements, des entreprises et des citoyens : leur contrôle est donc stratégique.

---

[5] https://news.un.org/fr/story/2024/11/1150951#:~:text=L%27Union%20internationale%20des%20t%C3%A9l%C3%A9communications,aux%20estimations%20r%C3%A9vis%C3%A9es%20pour%202023

[6] https://news.un.org/fr/story/2026/02/1158328

Les centres de données, où sont stockées les informations, sont eux aussi concentrés. Les États-Unis en hébergent une grande partie : près de 45%[7], ce qui signifie que de nombreux services publics étrangers dépendent d'infrastructures situées hors de leur territoire. Ces données peuvent alors relever de lois extraterritoriales : le CLOUD Act[8] américain (2018) permet aux autorités américaines d'exiger l'accès aux données détenues par des entreprises américaines, même stockées à l'étranger.

Le marché du cloud est dominé par trois hyperscalers : AWS, Microsoft Azure et Google Cloud[9]. Ensemble, ils représentent une majorité du marché mondial. Une panne chez l'un d'eux peut affecter des milliers de services publics : la panne d'AWS du 20 octobre 2025[10] a ainsi perturbé de nombreux services en ligne, dont des services administratifs.

Les semi-conducteurs, indispensables à tous les appareils numériques, sont produits en grande majorité en Asie de l'Est, notamment à Taïwan et en Corée du Sud. Sans ces composants, aucun cloud, aucun serveur, aucun réseau ne fonctionne. Taïwan, via TSMC, produit par exemple la grande majorité des puces les plus avancées au monde[11]

Ces éléments montrent que les infrastructures numériques critiques sont mondiales, mais contrôlées par un nombre limité d'acteurs privés. Les États dépendent donc de décisions prises à l'étranger, parfois en dehors de leur cadre juridique.

Une gouvernance mondiale limitée

Cette dépendance pose directement la question de la gouvernance mondiale du numérique. L'UIT[12], l'ONU[13] et l'ICANN[14] jouent un rôle important, mais limité :

- L'UIT est une agence spécialisée de l'ONU. Elle coordonne l'usage du spectre radio et des orbites satellitaires et élabore des normes techniques de télécommunication. Elle ne contrôle ni les câbles privés ni les services cloud.

---

7 | https://www.cargoson.com/fr/blog/nombre-de-centres-de-donnees-par-pays

8 | Texte Cloud Act: https://www.congress.gov/bill/115th-congress/house-bill/4943/text

9 | https://www.cargoson.com/fr/blog/parts-de-marche-infrastructure-cloud-mondiale-aws-azure-google

10 | https://navigacom.com/fr/blog/panne-aws

11 | https://www.reportprime.com/fr/Semi-conducteurs-et-appareils-connexes-r3073/company

12 | https://www.itu.int/fr/pages/default.aspx#/fr

13 | https://www.un.org/fr/

14 | https://www.icann.org/fr

- L'ONU offre un cadre de dialogue, notamment via le Forum sur la gouvernance d'Internet (IGF)[15] et le Pacte numérique mondial[16] adopté en 2024. Ces textes n'ont pas de force contraignante.
- L'ICANN est une organisation privée à but non lucratif de droit californien. Elle coordonne le système des noms de domaine et des adresses IP, selon un modèle multi-acteurs. Son rôle est technique et ne porte ni sur les infrastructures physiques ni sur les plateformes.

Les États doivent donc coopérer pour réduire les risques, tout en reconnaissant que les entreprises privées détiennent une grande partie du pouvoir technique.

La positions des acteurs

Les États-Unis et la Chine sont deux pays qui disposent de capacités importantes en IA, cloud, données, plateformes et infrastructures. La CNUCED[17] souligne la forte concentration mondiale de ces capacités : les investissements, la recherche en IA et les infrastructures de calcul sont concentrés dans un très petit nombre d'acteurs, majoritairement américains et chinois.

- États-Unis : leur puissance repose sur des entreprises privées. Leur influence s'exerce aussi par le droit, notamment avec le CLOUD Act.
- Chine : le modèle repose sur un fort contrôle de l'État, avec des champions nationaux et un cadre juridique de souveraineté sur les données comme la loi sur la protection des informations personnelles de 2021[18], qui impose notamment une localisation des données

L'Union Européenne (UE) apparaît comme une grande puissance réglementaire, mais doit encore transformer cette influence juridique en véritable autonomie technologique. Elle reste largement dépendante de fournisseurs étrangers pour le cloud, les plateformes et les modèles d'IA. Elle s'appuie sur quatre textes qui contribuent à la souveraineté numérique, mais pas de la même manière :

[15] | https://www.intgovforum.org/fr

[16] | https://www.un.org/fr/summit-of-the-future/global-digital-compact

[17] | https://unctad.org/fr

[18] | https://termly.io/fr/ressources/articles/pipl/

- **Le RGPD :** protège les données personnelles des citoyens européens et limite leur utilisation par des entreprises étrangères. Il s'applique à toute entreprise traitant des données de personnes situées dans l'UE, quel que soit son lieu d'établissement : c'est un outil important de souveraineté sur les données.
- **Le Digital Services Act[19] :** permet à l'UE d'imposer des obligations aux grandes plateformes opérant en Europe. Il renforce la capacité de l'État à réguler Internet.
- **Le Digital Markets Act[20] :** limite le pouvoir des très grandes plateformes et cherche à préserver la concurrence. Il contribue à la souveraineté économique et numérique.
- **L'AI Act[21] :** encadre l'utilisation de l'IA selon le niveau de risque et impose des obligations aux entreprises. Il renforce la capacité de l'UE à contrôler les technologies d'IA.

L'Inde, le Japon, la Corée de Sud et Taïwan sont des pays possédant des compétences et des industries importantes, mais leur degré d'autonomie varie selon les technologies.

- **Taïwan, Corée du Sud, Japon :** positions fortes dans les semi-conducteurs. Ils restent dépendants des États-Unis pour une grande partie des logiciels, du cloud et des modèles d'IA, ainsi que d'une chaîne d'approvisionnement mondiale.
- **Inde :** forte capacité en services numériques et en infrastructures publiques numériques, et un cadre de protection des données depuis la loi DPDP de 2023[22]. L'Inde reste cependant dépendante de technologies étrangères pour le cloud et le matériel.

Les Pays les Moins Avancés (PMA) qui se situent en Afrique ou encore en Amérique Latine utilisent principalement des technologies, infrastructures et services développés par les grandes puissances. La CNUCED estime que 80 % des investissements numériques dans les pays en développement se concentrent dans seulement dix économies, principalement en Asie[23]. Les autres pays ont donc très peu de marge pour négocier avec les grandes entreprises du numérique, ce qui limite leur capacité à imposer leurs règles, à contrôler leurs données ou à développer leurs propres solutions.

[19] | https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

[20] | https://www.consilium.europa.eu/fr/policies/digital-markets-act/

[21] | https://artificialintelligenceact.eu/fr/ai-act-explorer/

[22] | https://www.intelligencex.org/fr/resources/dpdp-act-2023-explained

[23] | https://unctad.org/fr/news/les-investissements-mondiaux-dans-leconomie-numerique-augmentent-fortement-mais-restent

CONCLUSION

Une souveraineté durable dans un environnement interconnecté

Les infrastructures numériques critiques sont devenues des éléments essentiels de la puissance, de la sécurité et du fonctionnement des États. La dépendance croissante des autorités publiques envers des acteurs privés transnationaux soulève ainsi des enjeux majeurs de sécurité, de contrôle des données et de capacité de décision autonome.

Mais comme ce rapport le souligne, la souveraineté numérique ne se définit pas par l'isolement technologique ou l'autosuffisance totale : elle repose sur la capacité des États à renforcer leur résilience numérique, à diversifier leurs partenaires technologiques, à protéger juridiquement leurs données et à participer activement à la gouvernance internationale du numérique.

Le défi central pour la communauté internationale consiste donc à concilier l'autonomie stratégique de chaque nation avec le maintien d'un Internet ouvert, interconnecté et coopératif: trois objectifs qui, loin de s'opposer, doivent être poursuivis ensemble.

TRAITÉS & GRANDS ÉVÉNEMENTS

CyberDrills de l'UIT : exercices internationaux de cybersécurité où les pays simulent des cyberattaques pour tester leur capacité de réponse. Plus de 100 pays y ont participé.
↳ https://www.itu.int/en/ITU-D/Cybersecurity/pages/cyberdrills.aspx

Pacte numérique mondial (ONU, 2024) : document qui propose des principes pour un Internet plus sûr, plus inclusif et plus transparent. Il encourage la protection des données, la réduction de la fracture numérique et la responsabilité des plateformes.
↳ https://docs.un.org/fr/A/79/L.2

ICANN : gestion des noms de domaine Organisation qui gère les noms de domaine et les adresses IP. Elle protège les domaines nationaux contre les détournements, mais ne contrôle pas les infrastructures physiques.
↳ https://icann.org

Cloud Act (États-Unis) : loi américaine qui permet aux autorités d'accéder aux données stockées par des entreprises américaines, même à l'étranger.
↳ https://www.justice.gov/criminal/cloud-act-resources

RGPD (Union européenne) : règlement européen qui protège les données personnelles des citoyens.
↳ https://www.cnil.fr/fr/reglement-europeen-protection-donnees

Le Digital Services Act : règlement qui impose aux grandes plateformes des obligations de modération, de transparence et de gestion des risques, avec des sanctions pouvant atteindre 6 % de leur chiffre d'affaires mondial.
↳ https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

Le Digital Markets Act : règlement qui interdit aux grandes entreprises numériques de favoriser leurs propres services, afin de préserver la concurrence.
↳ https://www.consilium.europa.eu/fr/policies/digital-markets-act/

L'AI Act : règlement qui encadre l'IA selon quatre niveaux de risque, des usages interdits aux usages libres.
↳ https://artificialintelligenceact.eu/fr/ai-act-explorer/

SOLUTIONS POSSIBLES

Les États peuvent développer des infrastructures locales, comme des centres de données nationaux ou des clouds souverains. La France a créé le label SecNumCloud[24], qui garantit que les données sensibles sont hébergées selon des règles françaises.

Ils peuvent encadrer les transferts de données, en imposant que certaines informations restent sur leur territoire. L'Allemagne exige par exemple que les données de santé soient stockées dans des data centers nationaux.[25] Ils peuvent diversifier leurs fournisseurs pour éviter le vendor lock-in. L'Inde utilise AWS, Azure, Google Cloud et des clouds locaux, ce qui réduit sa dépendance à un seul acteur. Ils peuvent relocaliser la production de semi-conducteurs[26]

Ils peuvent renforcer leur cybersécurité grâce aux CyberDrills de l'UIT, qui ont déjà aidé plus de 100 pays à améliorer la détection des attaques et la protection des infrastructures critiques.

Enfin, ils peuvent agir sur la fracture numérique. Une partie importante de la population mondiale n'a toujours pas accès à Internet. Des projets comme le câble "PEACE"[27] améliorent la connectivité, mais créent aussi de nouvelles dépendances vis-à-vis des acteurs qui financent ces infrastructures.

---

[24] | https://cyber.gouv.fr/enjeux-technologiques/cloud/

[25] | https://www.insideprivacy.com/digital-health/germany-enacts-stricter-requirements-for-the-processing-of-health-data-using-cloud-computing-with-potential-side-effects-for-medical-research-with-pharmaceuticals-and-medical-devices/

[26] | https://next.ink/166117/semi-conducteurs-la-course-folle-de-leurope-pour-reduire-ses-dependances/

[27] | https://hommesetsciences.fr/nouvelles-routes-de-la-soie-numeriques-ou-va-la-chine/

QUESTIONS GUIDÉES

Renforcer la résilience des infrastructures numériques

→ Quels types d'infrastructures sont les plus vulnérables dans votre pays, et quels incidents récents illustrent ces failles ?
→ Qui finance la mise à niveau des infrastructures critiques dans votre pays : les États eux-mêmes, les bailleurs internationaux, ou les entreprises qui les exploitent ?

Réduire la dépendance envers les acteurs privés

→ Quelle entreprise du marché du cloud mondial contrôle les données de votre État, et quels risques cela pose-t-il ?

Développer une souveraineté numérique équilibrée

→ Votre pays a-t-il déjà légiféré sur la localisation obligatoire de certaines données (santé, défense, administration) ? Si oui, comment ces lois ont-elles été reçues par les partenaires commerciaux ?

Garantir la sécurité et la circulation des données

→ Votre délégation impose-t-elle des restrictions sur le transfert de données hors du territoire ?

Réduire les inégalités numériques

→ Quel pourcentage de la population de votre pays a accès à une connexion Internet fiable et à des infrastructures cloud locales ?
→ L'aide au développement numérique venant d'autres pays (exemple: financements chinois, d'infrastructures télécoms en Afrique) crée-t-elle une nouvelle forme de dépendance technologique ou géopolitique pour votre délégation ?

SITOGRAPHIE

UIT

https://www.itu.int/fr/mediacentre/Pages/PR-2024-11-27-facts-and-figures.aspx#:~:text=Selon%20de%20nouvelles%20donn%C3%A9es%20de,r%C3%A9vis%C3%A9es%20pour%20l'ann%C3%A9e%202023

https://www.itu.int/itu-d/sites/priorities/fr/digital-transformation/

https://www.itu.int/fr/ITU-D/Regulatory-Market/Pages/digital-transformation-wheel.aspx

https://www.itu.int/fr/ITU-D/Innovation/Pages/Digital-Transformation-Accelerators.aspx

https://news.un.org/fr/story/2024/11/1150951#:~:text=L'Union%20internationale%20des%20t%C3%A9l%C3%A9communications,aux%20estimations%20r%C3%A9vis%C3%A9es%20pour%202023

OCDE

https://www.oecd.org/content/dam/oecd/fr/publications/reports/2025/05/competition-in-the-provision-of-cloud-computing-services_f42582ad/27798cae-fr.pdf

https://www.oecd.org/fr/publications/securite-economique-dans-un-monde-en-mutation_3f5404db-fr/full-report/special-focus-semiconductor-value-chains_dc772986.html?utm_source

https://www.oecd.org/content/dam/oecd/fr/publications/reports/2025/05/competition-in-the-provision-of-cloud-computing-services_f42582ad/27798cae-fr.pdf

https://www.oecd.org/fr/topics/sub-issues/digital-security-risk-management.html

https://www.oecd.org/en/publications/2026/06/digital-government-outlook_4585678e/full-report.html

https://www.oecd.org/fr/topics/sub-issues/semiconductors.html

---

CNUCED

https://unctad.org/fr/news/la-forte-concentration-des-marches-numeriques-met-les-consommateurs-en-danger-voici-comment

---

MISSION OPEN DATA

https://www.mission-open-data.fr/nombre-de-data-center/#:~:text=Les%20%C3%89tats%2DUnis%20dominent%20largement,environ%2045%20%25%20du%20total%20mondial

---

ONU

https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2025/index/

https://www.un.org/digital-emerging-technologies/global-digital-compact?