COMMITTEE : ITU - Critical Digital Infrastructures
ISSUE : How can States ensure their digital sovereignty while reducing their growing dependence on digital infrastructures controlled by transnational private companies ?
CHAIRS : Mathilda REY, John-Tyler DUPEROY, Maya YANKOVSKAYA

PRESENTATION OF THE CHAIRS



Hello dear delegates.
My name is John-Tyler Duperoy and I am 16 years old. I was born in the city of Nîmes in the Gard department and I have always lived in France.
I am delighted to be your committee chair for FerMUN 2027. Passionate about public affairs and political life, I aspire to attend Sciences Po and then the INSP. With this in mind, I have already completed several internships, notably at the Senate and the National Assembly.
At this FerMUN 2027, we will address a crucial topic: the digital sovereignty of states in the face of large transnational private companies. Because this issue directly concerns us, whether it's our public services or our sensitive and personal digital data. This debate will be marked by the heavy reliance of states on digital tools, in a world where everything is connected, and I look forward to the discussions we will have.



Hello everyone, dear delegates.
My name is Maya, I am 16 years old, and I am in the IB Diploma Programme at Toronto French School in Canada. I grew up in Latvia before moving to Toronto a few years ago, and I speak English, Russian, and Latvian in addition to French.
I am particularly interested in the links between economics, technology, and international politics. This is my second year in MUN : I have already had the opportunity to travel to Morocco for a conference, as well as participate in provincial and national conferences.
Outside of school, I play volleyball and the piano. I hope you will approach these issues with curiosity and rigor; I am confident that your ideas will make this committee memorable !

KEY-WORDS

Digital sovereignty : the ability of a state to control its digital infrastructure, data, strategic technologies and the rules governing their use, so as not to depend on private actors or foreign powers.

Critical digital infrastructure: all the elements essential to the functioning of the Internet: submarine cables, data centers, clouds, satellites, DNS servers, semiconductors. Their failure can disrupt essential public services.

Hyperscaler: a company that provides cloud services on a very large scale (such as AWS, Microsoft Azure, or Google Cloud). These players dominate the global cloud market and host a large portion of public and private data.

Vendor lock-in: a situation where a customer becomes dependent on a technology provider, making switching difficult or expensive. This limits a state's ability to modify its digital infrastructure.

Sovereign cloud: a cloud designed to ensure that a state's sensitive data is hosted according to its own rules, with national control over data security, access, and location.

Digital resilience: is the ability of digital infrastructures to withstand cyberattacks, outages, disasters or crises, while maintaining essential services and enabling their rapid recovery.

Clarifying Lawful Overseas Use of Data Act (Cloud Act)[1] **:** US law that requires American companies to provide data to US authorities, even if that data is stored in another country.

General Data Protection Regulation (GDPR)[2] **:** European regulation that protects citizens' personal data by imposing strict rules on the collection, use and storage of data.

Semiconductors: essential electronic components for all digital devices (smartphones, computers, servers, AI). Their production is concentrated in a few countries, creating a global dependency.

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

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

Internet Corporation for Assigned Names and Numbers (ICANN)[3] **:** an international organization that manages domain names and IP addresses, ensuring the stability and uniqueness of the Internet addressing system.

United Nations Conference on Trade and Development (UNCTAD)[4] **:** is the principal organ of the UN General Assembly, founded in 1964 to help developing countries integrate into the global economy.

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

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

OVERVIEW

A new strategic challenge for digital sovereignty

Digital transformation has made digital infrastructure essential to the functioning of states, their economies, and their security. According to the International Telecommunication Union (ITU), nearly 5,5 billion people were using the internet in 2024[5]. However, control of these infrastructures is increasingly exercised by a small number of transnational private companies.

States are therefore seeking to strengthen their digital sovereignty while maintaining an open internet. Digital sovereignty is thus becoming a major issue of security and competitiveness.

Global infrastructures, controlled by a few private actors

The internet relies on physical and software infrastructure : submarine cables, data centers, satellites, cloud services, and semiconductors. Much of this infrastructure is controlled by a few transnational private companies, primarily American and Chinese, creating a dependency for states.

Nearly 99% of global internet traffic passes through submarine cables[6]. Several strategic cables are financed by private companies :

- Google funded: Dunant (USA–France), Grace Hopper (USA–UK–Spain) and Equiano (Portugal–South Africa)
- Meta funded: 2Africa, which tours the African continent
- Amazon is participating in the financing of the Hawaiki Nui cable (Pacific link)

These cables carry data for governments, businesses and citizens : their control is therefore strategic.

Data centers, where information is stored, are also concentrated. The United States hosts a large portion of them: nearly 45%[7], this means that many foreign public services rely on

[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

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

infrastructure located outside their territory. This data may then fall under extraterritorial laws: the US CLOUD Act[8] (2018) allows US authorities to demand access to data held by US companies, even if stored abroad.

The cloud market is dominated by three hyperscalers : AWS, Microsoft Azure, and Google Cloud[9]. Together, they represent a majority of the global market. A failure at one of them can affect thousands of public services: the AWS outage of October 20, 2025[10]. This has disrupted many online services, including administrative services.

Semiconductors, essential to all digital devices, are produced primarily in East Asia, particularly in Taiwan and South Korea. Without these components, no cloud, no server, no network can function. Taiwan, through TSMC, produces, for example, the vast majority of the world's most advanced chips[11]

These factors demonstrate that critical digital infrastructures are global, but controlled by a limited number of private actors. States are therefore dependent on decisions made abroad, sometimes outside their legal framework.

Limited global governance

This dependence directly raises the question of global digital governance. L'ITU[12], l'UN[13] and the ICANN[14] play an important, but limited, role :

- The ITU is a specialized agency of the UN. It coordinates the use of the radio spectrum and satellite orbits and develops technical standards for telecommunications. It does not control private cables or cloud services.

[8] | Cloud Act text: 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

- The UN provides a framework for dialogue, notably through the Internet Governance Forum (IGF)[15] and the Global Digital Pact[16] adopted in 2024. These texts are not legally binding.
- ICANN is a private, non-profit organization under California law. It coordinates the domain name and IP address system using a multi-stakeholder model. Its role is technical and does not extend to physical infrastructure or platforms.

States must therefore cooperate to reduce risks, while recognizing that private companies hold a large part of the technical power.

The positions of the actors

The United States and China are two countries with significant capabilities in AI, cloud computing, data, platforms, and infrastructure. UNCTAD[17] highlights the high global concentration of these capabilities : Investments, AI research and computing infrastructure are concentrated in a very small number of players, mostly American and Chinese.

- United States: their power rests on private companies. Their influence is also exerted through law, notably with the CLOUD Act
- China: the model relies on strong state control, with national champions and a legal framework for data sovereignty such as the 2021 Personal Information Protection Law[18], which notably requires data localization

The European Union (EU) appears as a major regulatory power, but has yet to translate this legal influence into genuine technological autonomy. It remains largely dependent on foreign providers for cloud computing, platforms, and AI models. It relies on four texts that contribute to digital sovereignty, but not in the same way :

- **The GDPR** protects the personal data of European citizens and limits its use by foreign companies. It applies to any company processing the data of individuals located in the EU, regardless of its place of establishment: it is an important tool for data sovereignty.

[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/

- **The Digital Services Act**[19] : It allows the EU to impose obligations on large platforms operating in Europe. It strengthens the state's ability to regulate the internet.
- **The Digital Markets Act**[20] : limits the power of very large platforms and seeks to preserve competition. It contributes to economic and digital sovereignty.
- **The AI Act**[21] **:** It regulates the use of AI according to the level of risk and imposes obligations on companies. It strengthens the EU's capacity to control AI technologies.

India, Japan, South Korea and Taiwan are countries with significant skills and industries, but their degree of self-reliance varies according to technology.

- **Taiwan, South Korea, Japan:** strong positions in semiconductors. They remain dependent on the United States for a large part of their software, cloud and AI models, as well as a global supply chain.
- **India:** strong capacity in digital services and public digital infrastructure**,** and a data protection framework since the DPDP law of 2023. However, India remains dependent on foreign technologies for cloud and hardware.

The Least Developed Countries (LDCs), located in Africa or Latin America, primarily use technologies, infrastructure and services developed by major powers. UNCTAD estimates that 80% of digital investments in developing countries are concentrated in just ten economies, mainly in Asia[22]. Other countries therefore have very little room to negotiate with large digital companies, which limits their ability to impose their rules, control their data or develop their own 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://unctad.org/fr/news/les-investissements-mondiaux-dans-leconomie-numerique-augmentent-fortement-mais-restent

CONCLUSION

Sustainable sovereignty in an interconnected environment

Critical digital infrastructures have become essential elements of the power, security and functioning of states. The increasing dependence of public authorities on transnational private actors thus raises major issues of security, data control and autonomous decision-making capacity.

But as this report points out, digital sovereignty is not defined by technological isolation or total self-sufficiency: it rests on the ability of states to strengthen their digital resilience, to diversify their technology partners, to legally protect their data and to actively participate in international digital governance.

The central challenge for the international community is therefore to reconcile the strategic autonomy of each nation with the maintenance of an open, interconnected and cooperative Internet: three objectives which, far from being opposed, must be pursued together.

TREATIES AND MAJOR EVENTS

ITU CyberDrills : international cybersecurity exercises where countries simulate cyberattacks to test their response capabilities. More than 100 countries have participated.
↳ https://www.itu.int/en/ITU-D/Cybersecurity/pages/cyberdrills.aspx

Global Digital Pact (UN, 2024) : a document that proposes principles for a safer, more inclusive, and more transparent internet. It promotes data protection, bridging the digital divide, and platform accountability.
↳ https://docs.un.org/fr/A/79/L.2

ICANN : Domain Name System. An organization that manages domain names and IP addresses. It protects country code domains from hijacking, but does not control the physical infrastructure.
↳ https://icann.org

Cloud Act (United States) : American law that allows authorities to access data stored by American companies, even abroad.
↳ https://www.justice.gov/criminal/cloud-act-resources

GDPR (European Union) : European regulation that protects the personal data of citizens.
↳ https://www.cnil.fr/fr/reglement-europeen-protection-donnees

The Digital Services Act : a regulation that imposes obligations on large platforms regarding moderation, transparency and risk management, with penalties that can reach 6% of their global revenue.
↳ https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

The Digital Markets Act : a regulation that prohibits large digital companies from favoring their own services, in order to preserve competition.
↳ https://www.consilium.europa.eu/fr/policies/digital-markets-act/

The AI Act : regulation that governs AI according to four levels of risk, from prohibited uses to free uses.
↳ https://artificialintelligenceact.eu/fr/ai-act-explorer/

POSSIBLE SOLUTIONS

States can develop local infrastructures, such as national data centers or sovereign clouds. France has created the SecNumCloud label[23], which guarantees that sensitive data is hosted in accordance with French rules.

They can regulate data transfers, requiring that certain information remain within their territory. Germany, for example, requires that health data be stored in national data centers[24]. They can diversify their suppliers to avoid vendor lock-in. India uses AWS, Azure, Google Cloud, and local clouds, reducing its dependence on a single player. They can relocate semiconductor production[25].

They can strengthen their cybersecurity through the ITU's CyberDrills, which have already helped more than 100 countries improve attack detection and critical infrastructure protection.

Finally, they can address the digital divide. A significant portion of the world's population still lacks internet access. Projects like the "PEACE" cable[26] improve connectivity, but also create new dependencies on the actors who finance these infrastructures.

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

[24] | 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/

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

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

GUIDED QUESTIONS

Strengthening the resilience of digital infrastructures

→ What types of infrastructure are most vulnerable in your country, and what recent incidents illustrate these weaknesses ?
→ Who finances the upgrading of critical infrastructure in your country: the states themselves, international donors, or the companies that operate them ?

Reduce dependence on private actors

→ Which company in the global cloud market controls your state's data, and what risks does this pose ?

Developing balanced digital sovereignty

→ Has your country already passed legislation on the mandatory localization of certain data (health, defense, administration)? If so, how have these laws been received by trading partners ?

Ensuring the security and flow of data

→ Does your delegation impose restrictions on the transfer of data outside the territory ?

Reducing digital inequalities

→ What percentage of your country's population has access to a reliable internet connection and local cloud infrastructure ?
→ Does digital development aid from other countries (example: Chinese funding for telecom infrastructure in Africa) create a new form of technological or geopolitical dependence for your delegation ?

BIBLIOGRAPHY

ITU

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

OECD

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

UNCTAD

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

---

UN

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

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