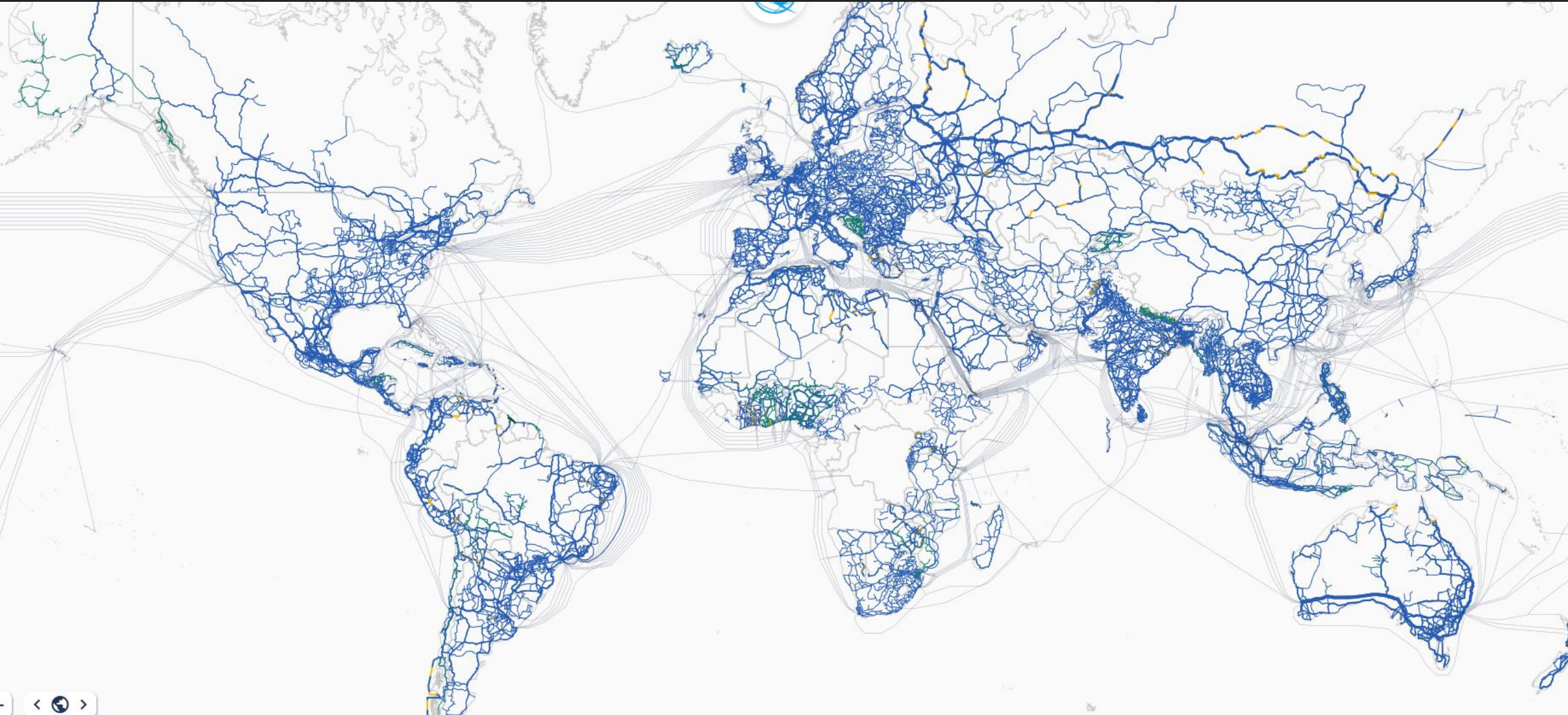


# Quelles limites géopolitiques pour l'Internet demain?

Louis Pétiniaud  
GEODE – Institut Français de Géopolitique – Paris 8

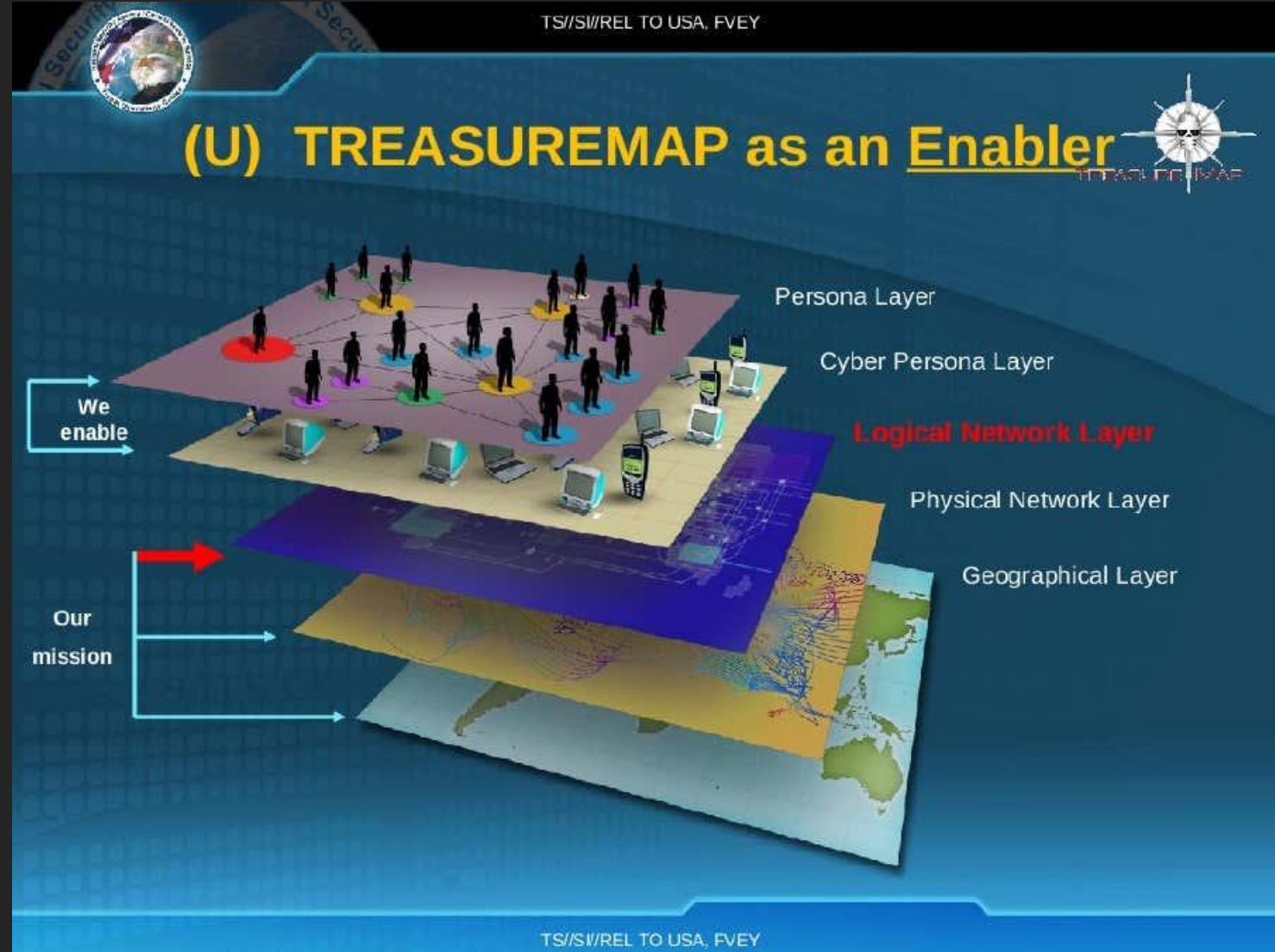
*[l.petiniaud@gmail.com](mailto:l.petiniaud@gmail.com)*

# Les routes des données : d'abord un réseau de câbles



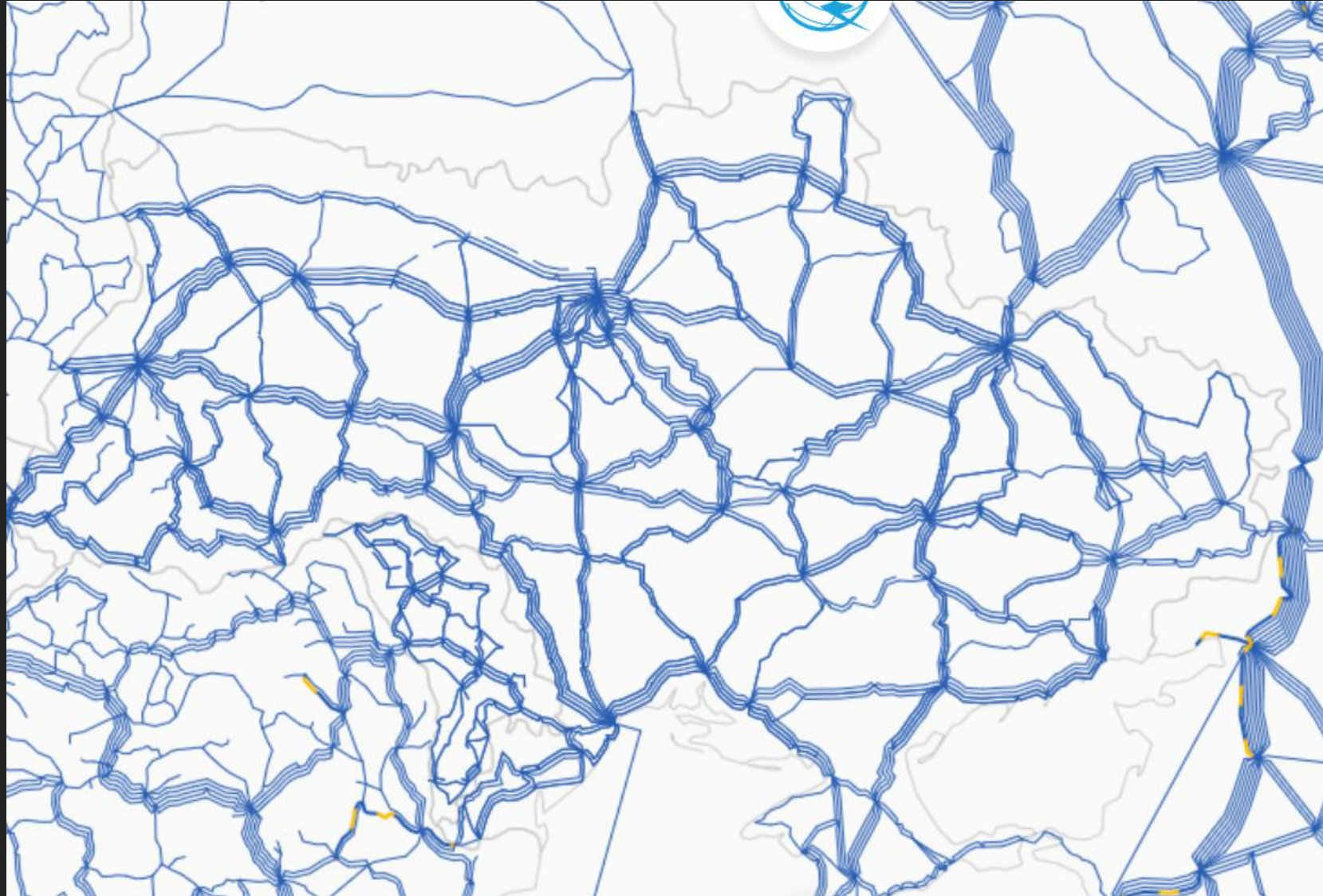
# Géopolitique de la couche logique : la maîtrise des routes

- Cyberspace = conception opérationnelle en 3 ou 4 couches
- « Infrastructures d'Internet » = couche physique + couche logique
- Couche physique = câbles, datacenters, routeurs...
- Couche logique permet aux éléments physiques de communiquer entre eux

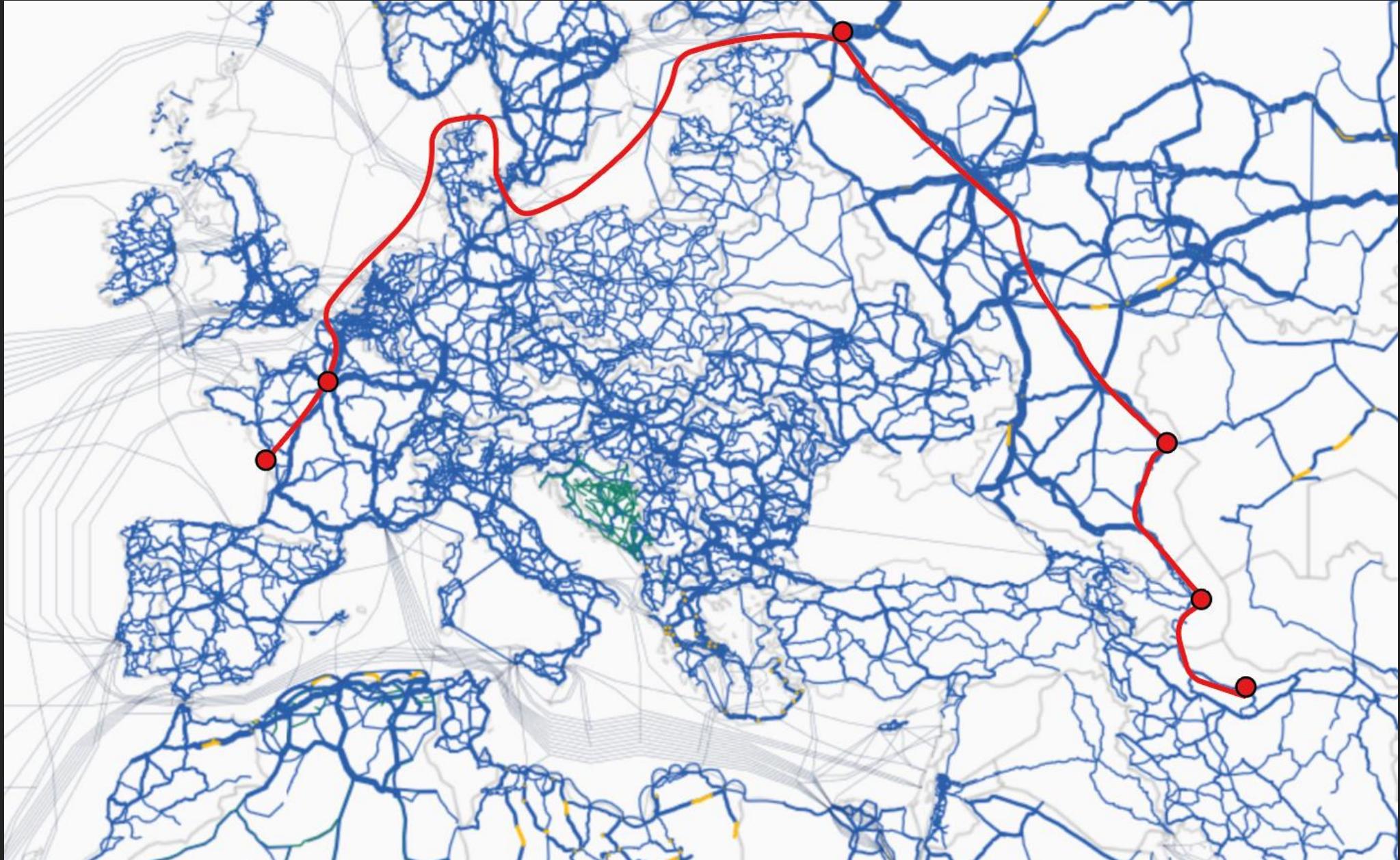


# « L'espace » des données numériques : le routage

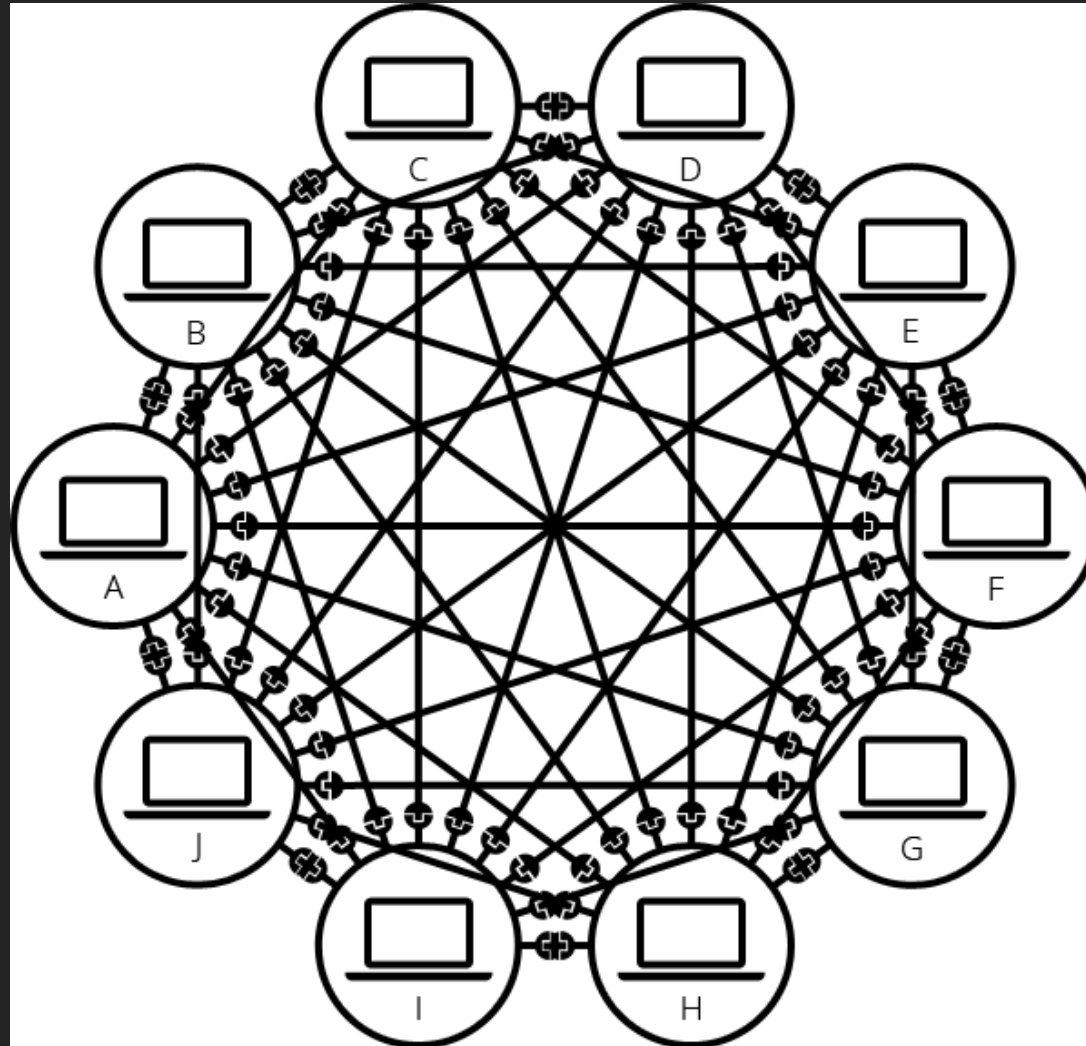
- Un câble  $\neq$  une connexion Internet
- La géographie des câbles ne donne qu'une indication parcellaire des routes des données

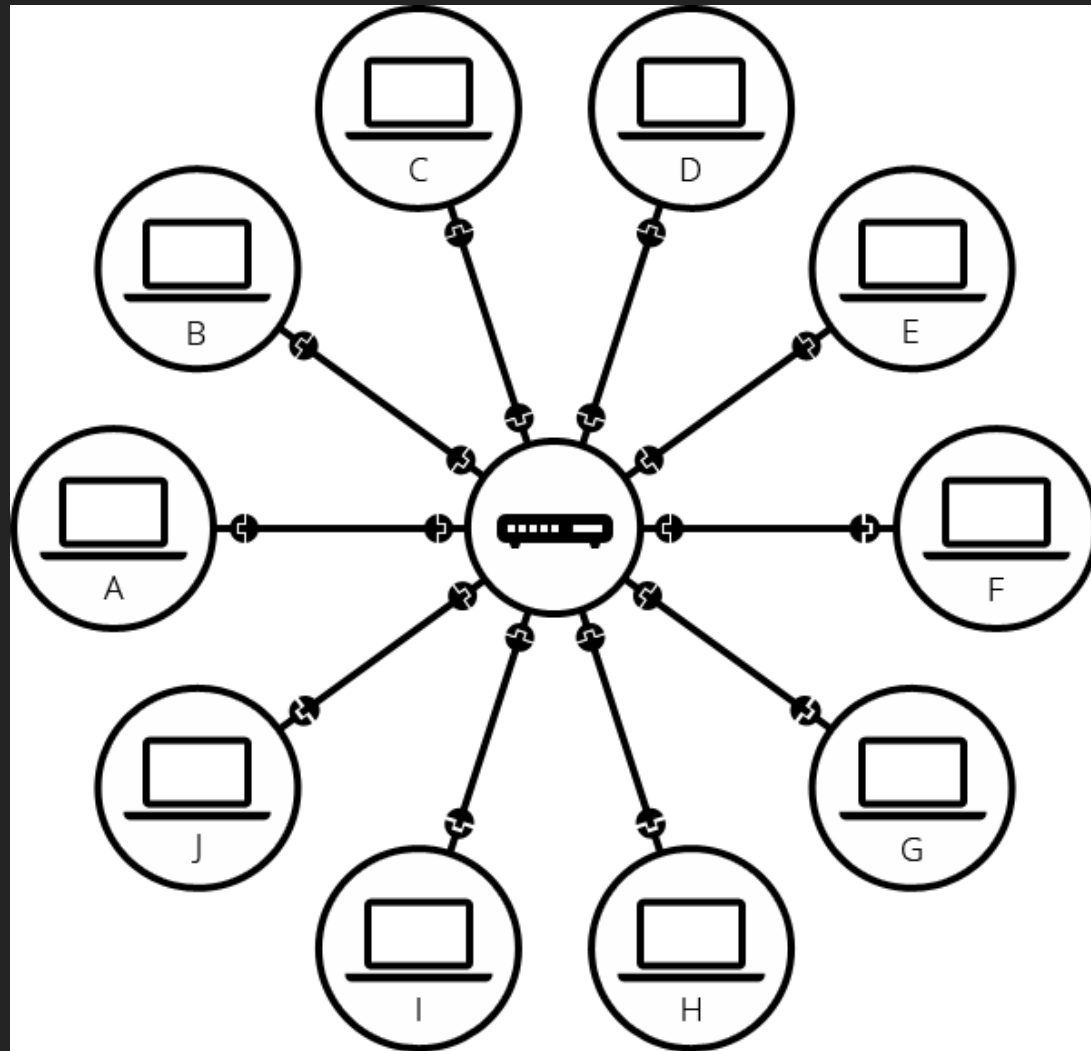


# Le routage des données numériques

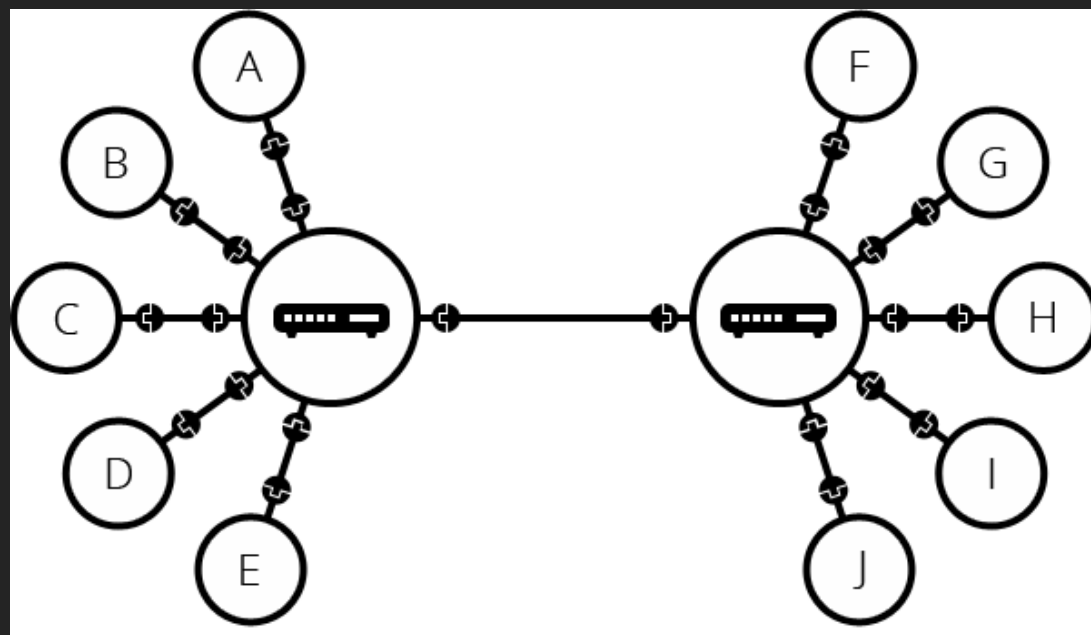


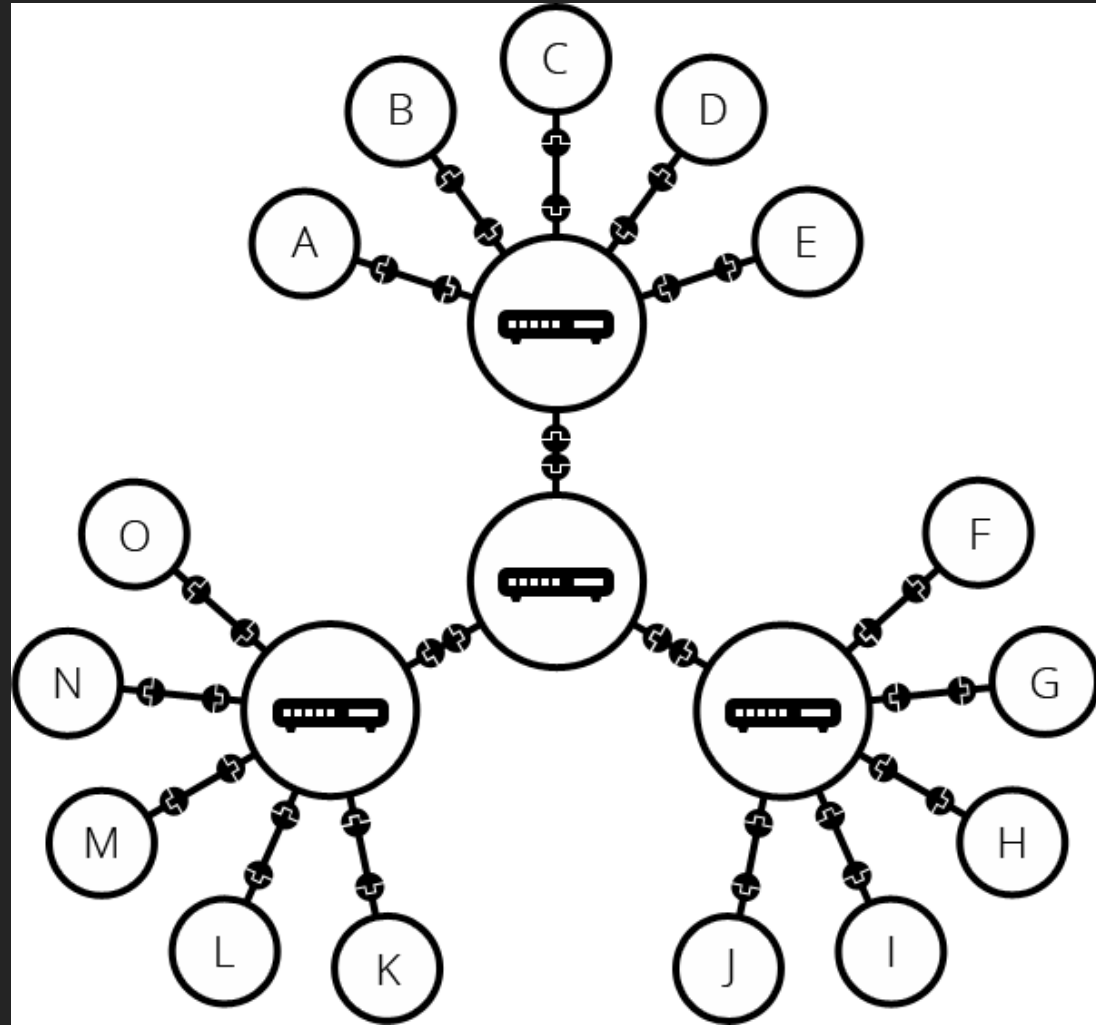






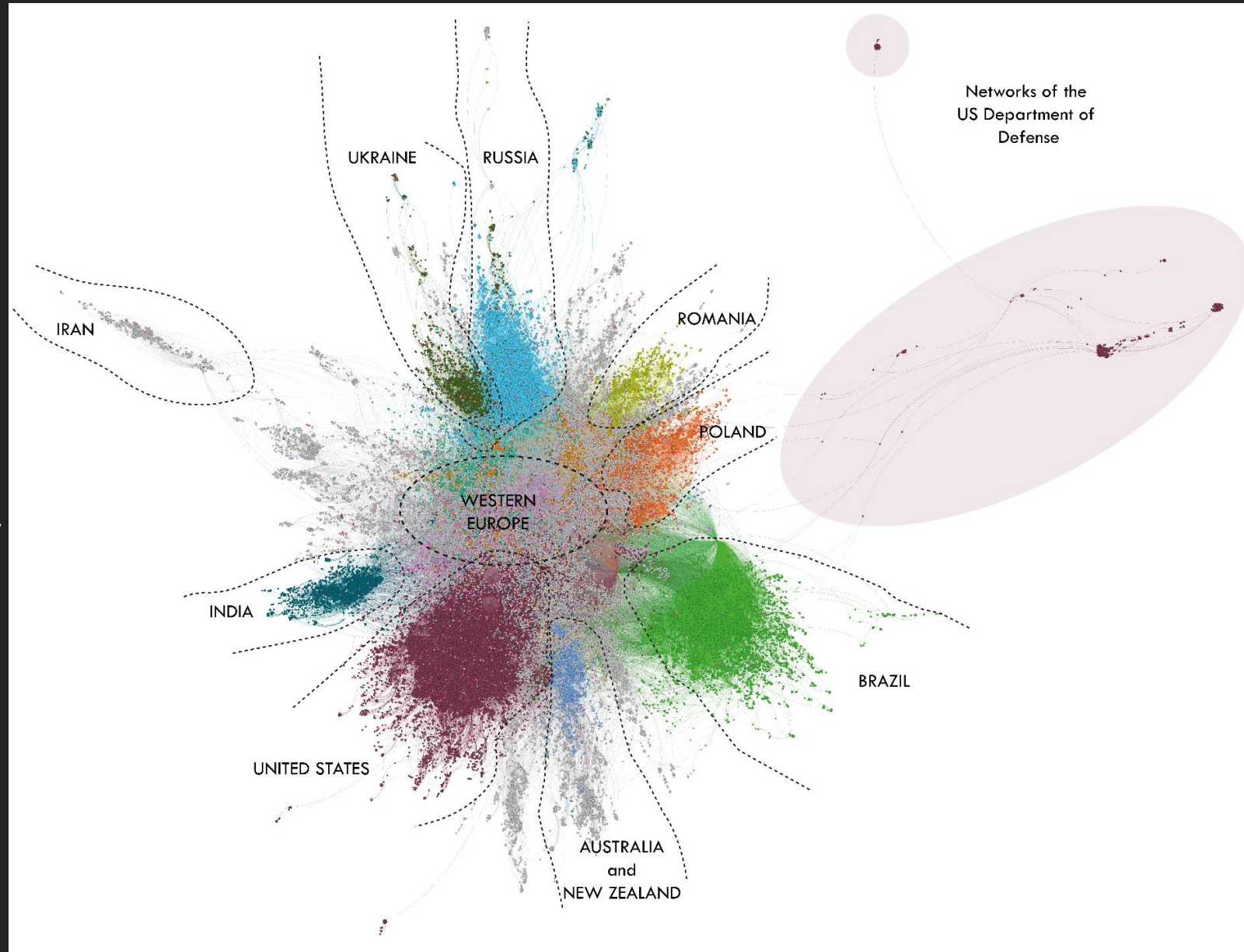




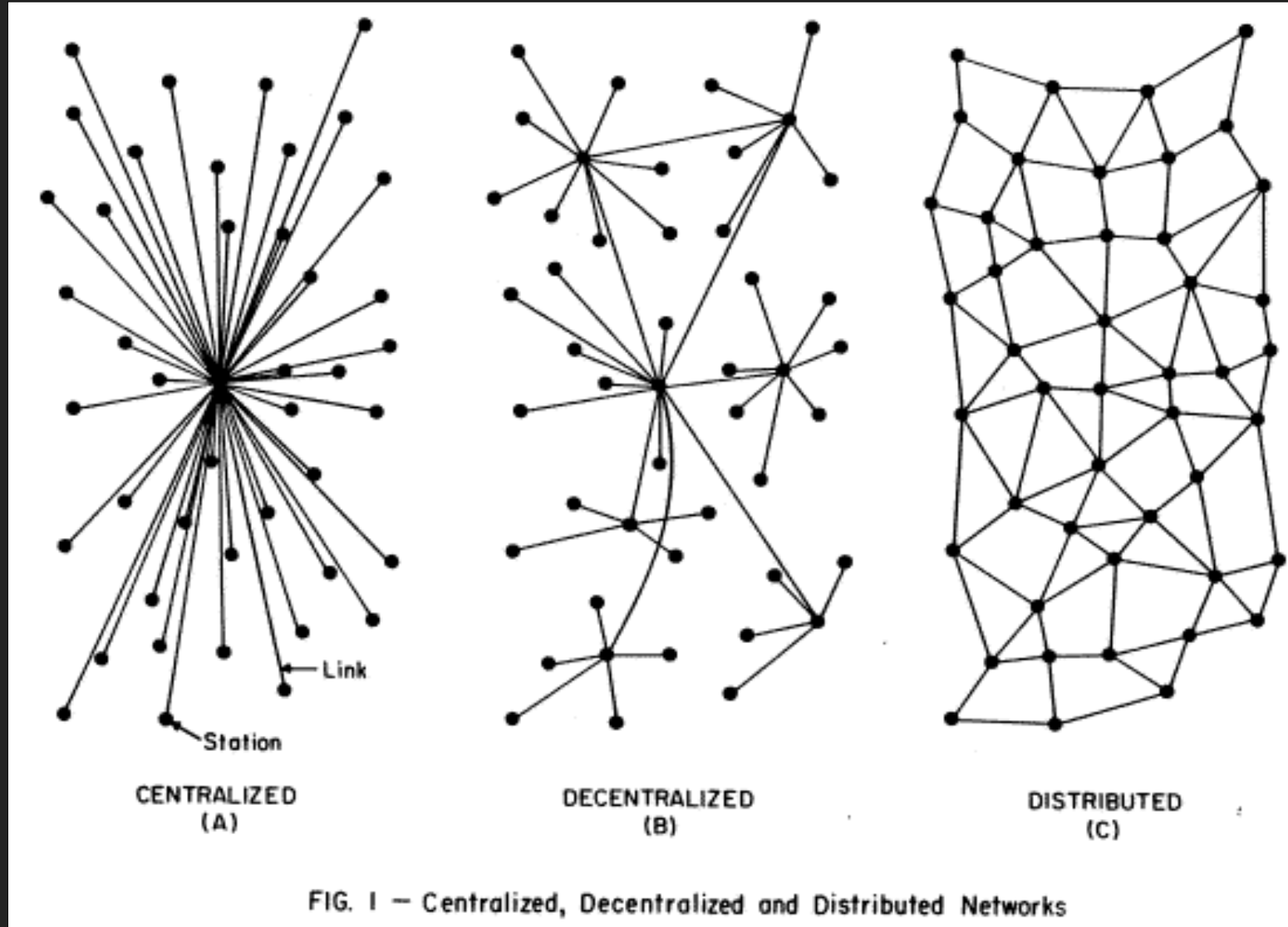


# Une observation topologique des routes des données

- Internet = un réseau mondial d'environ 120 000 « systèmes autonomes » (AS)
- AS = FAI, fournisseur de transit, de contenu...
- Leurs interconnexions créent les chemins disponibles pour les données
- **Représentation en graphe**
  - Couleur = pays
  - Taille si applicable : centralité intermédiaire (d'autres existent)



# BGP, un protocole d'interconnexion simple qui permet en théorie un réseau « distribué » et résilient





## Vers la création de barrières ou de frontières numériques ?

1. Un réseau qui vise l'interconnexion
2. Fermer et éteindre le réseau, une pratique croissante
3. Manipuler le réseau à des fins stratégiques
4. Frontiérifier le réseau dans la guerre : un précédent ?
5. Des politiques privées de fermeture du réseau?

# Un réseau international et à vocation d'ouverture

- Routage permet efficacement l'interconnexion globale des utilisateurs du réseau
  - Il existe des exceptions notables plus ou moins fortes : Corée du Nord, Chine, Iran...
- Interconnexion = produit de l'action conjointe de nombreux acteurs
  - AS / opérateurs
  - Organismes de normalisation
  - Politique

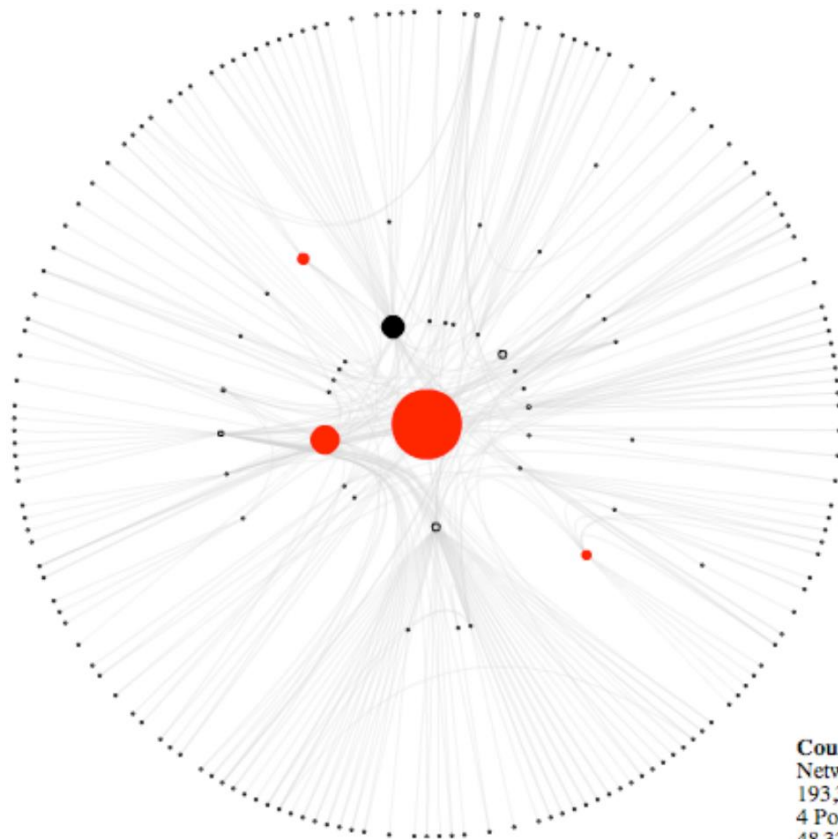
## Un réseau international et à vocation ouverte

- Depuis quand le politique se mêle-t-il de routage ? Une archéologie à faire
  - 2006 : « There is little regulation, and network operators are free to decide where, how, and with whom to connect. » IDC Report whitePaper
- Depuis les années 2010, plus encore 2020: croissance rapide de conceptions territoriales du réseau
  - Routage devient un enjeu stratégique



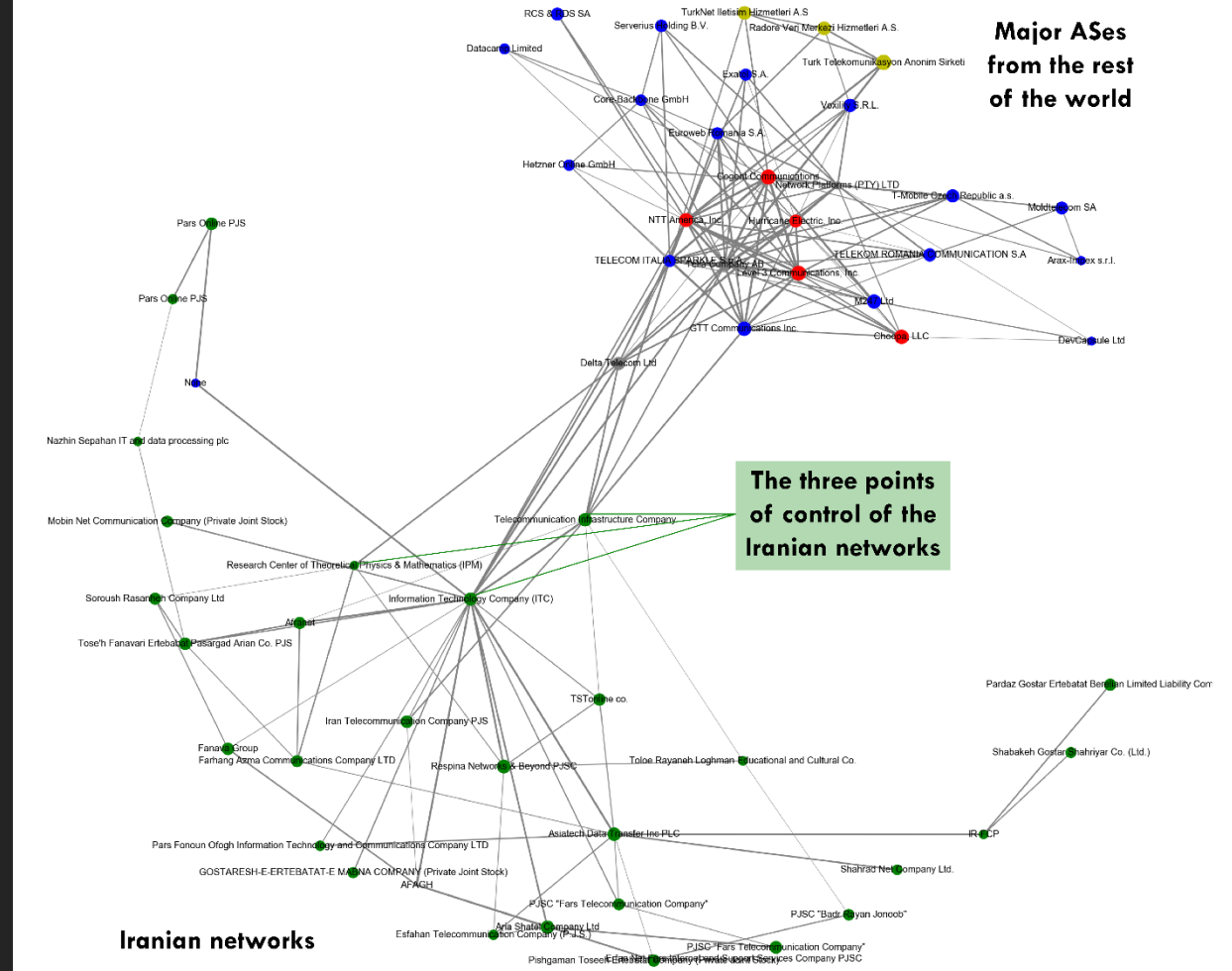
# Contrôle par dessein : Chine, Iran

## AUTONOMOUS SYSTEM DIAGRAM - China



**Country Summary:**  
 Network Complexity: 0.149  
 193,304,497 IP Addresses  
 4 Points of Control:  
 48,326,124 IPs per Point of Control

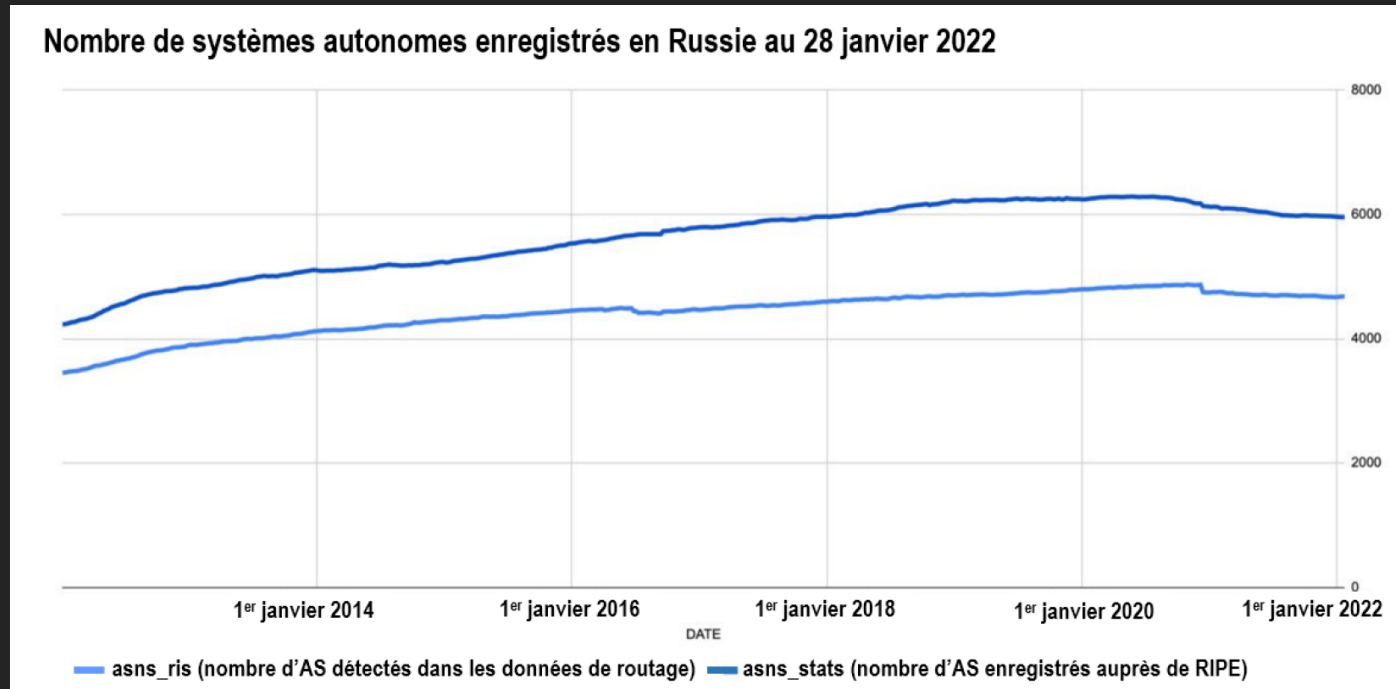
## Major ASes from the rest of the world



## Iranian networks

# Enjeux de contrôle étatique: Chine, Iran, Russie

- Ambitions russes: un ex. de contrôle décentralisé
  - Annonce de déconnexion réussie en 2019
  - Annonce 2021
  - Annonce 2023

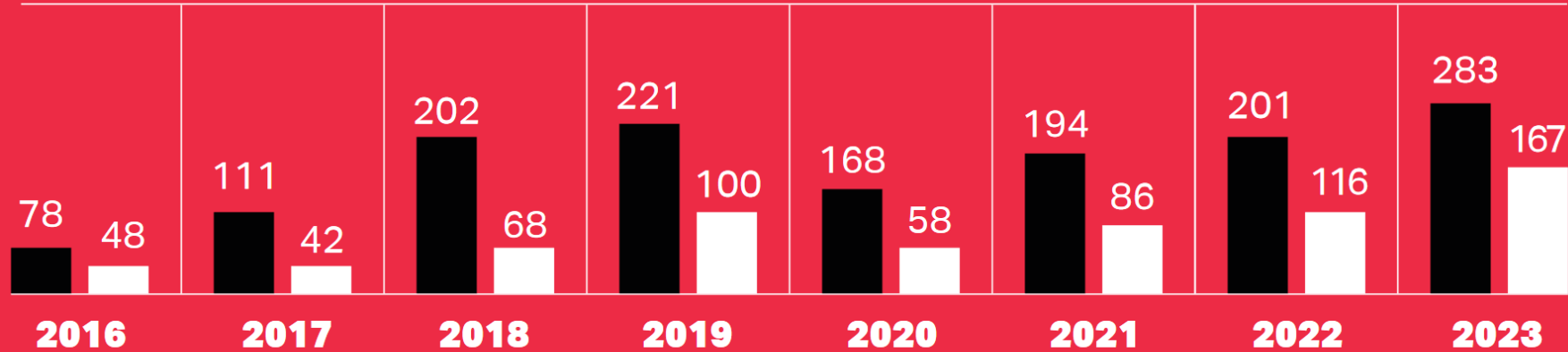


# Coupures Internet, phénomène croissant

## Overview of 2023 data

### Documented internet shutdowns by year \*

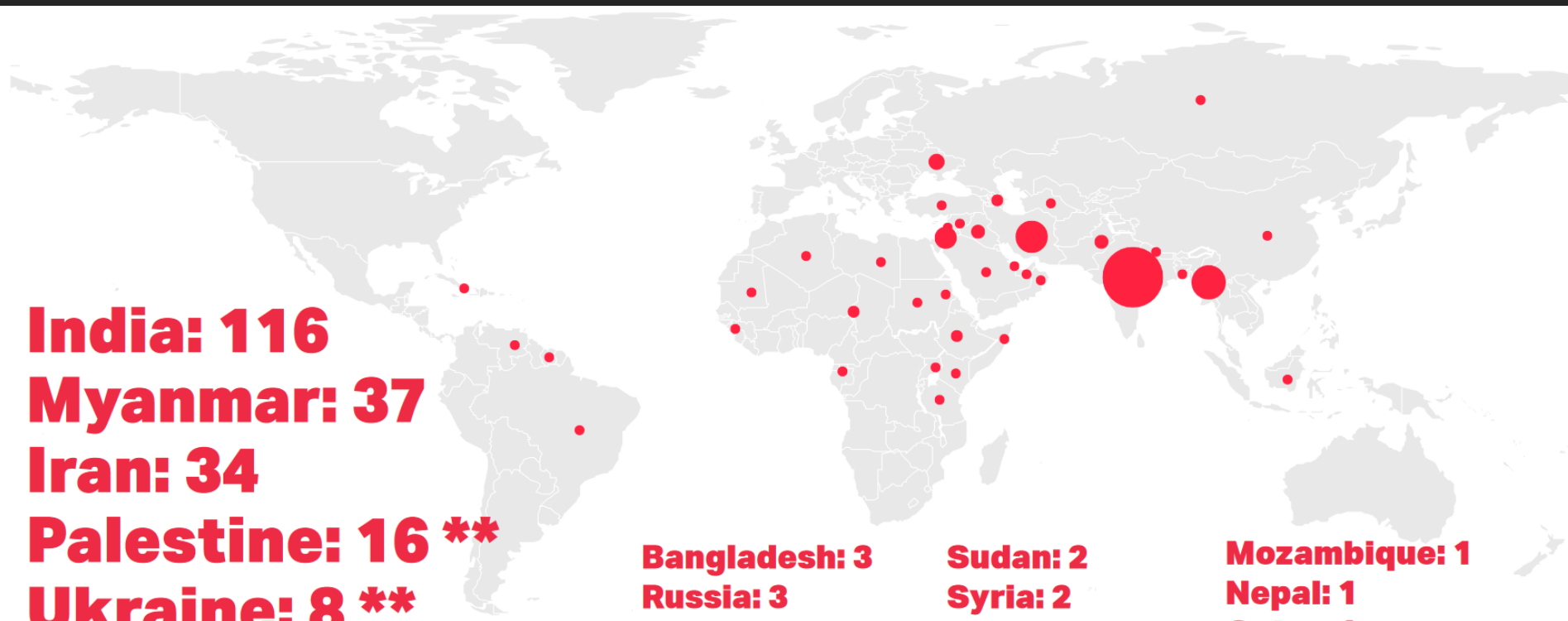
■ Total number of shutdowns  
■ Total number of shutdowns, not including India



\* These numbers reflect the latest data available as of publication of this report and include updates to previously published totals for past years.

### Number of countries where shutdowns occurred





**India: 116**  
**Myanmar: 37**  
**Iran: 34**  
**Palestine: 16 \*\***  
**Ukraine: 8 \*\***  
**Pakistan: 7**  
**Iraq: 6**  
**Azerbaijan: 5**  
**Ethiopia: 4**  
**Senegal: 4**

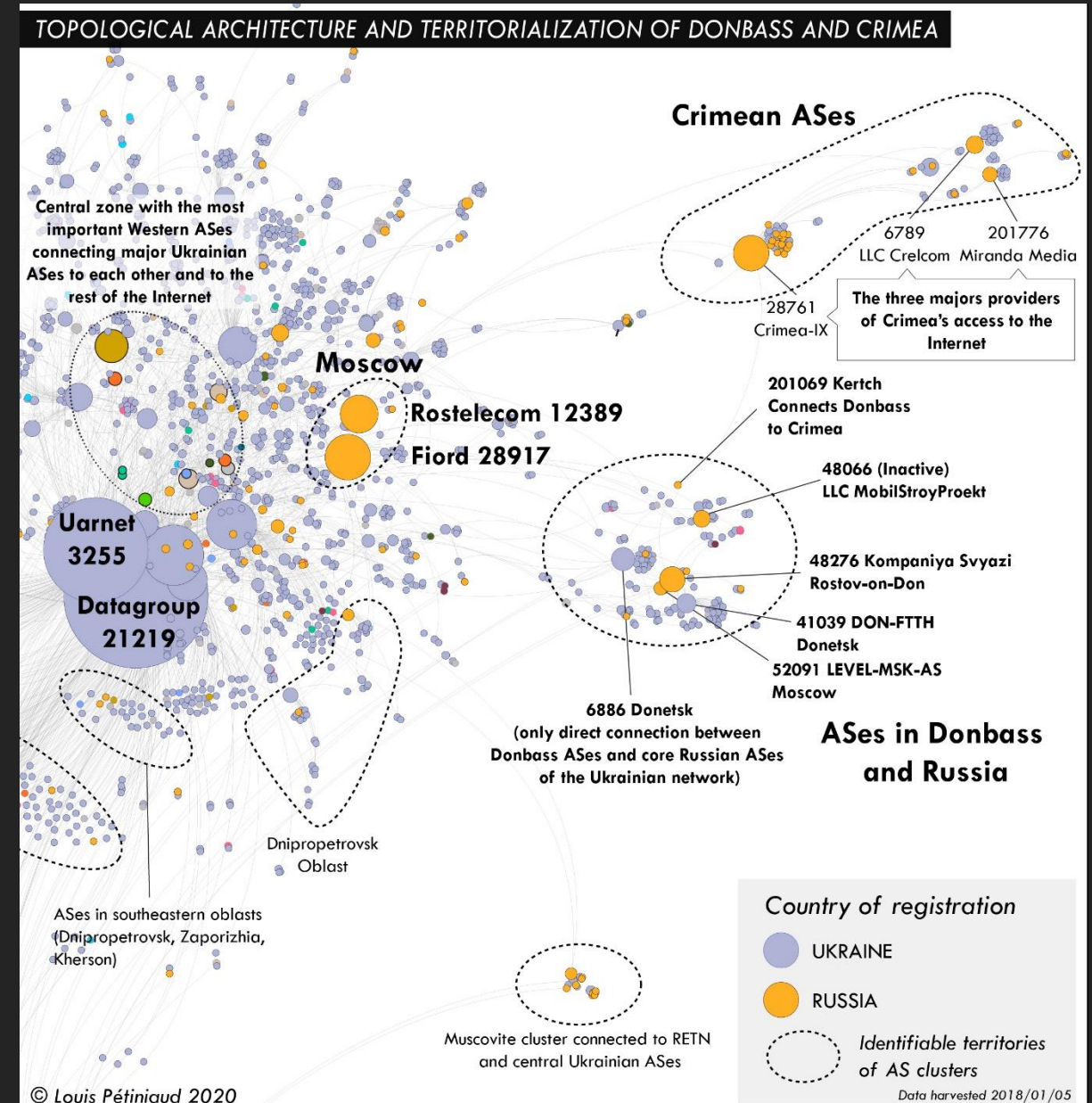
**Bangladesh: 3**  
**Russia: 3**  
**Jordan: 3**  
**Libya: 3**  
**China: 2**  
**Guinea: 2**  
**Mauritania: 2**  
**Oman: 2**  
**Tanzania: 2**  
**Turkmenistan: 2**

**Sudan: 2**  
**Syria: 2**  
**Türkiye: 2**  
**Algeria: 1**  
**Brazil: 1**  
**Cuba: 1**  
**Gabon: 1**  
**Indonesia: 1**  
**Kenya: 1**  
**Lebanon: 1**

**Mozambique: 1**  
**Nepal: 1**  
**Qatar: 1**  
**Saudi Arabia: 1**  
**Somaliland: 1**  
**Suriname: 1**  
**United Arab Emirates: 1**  
**Uganda: 1**  
**Venezuela: 1**

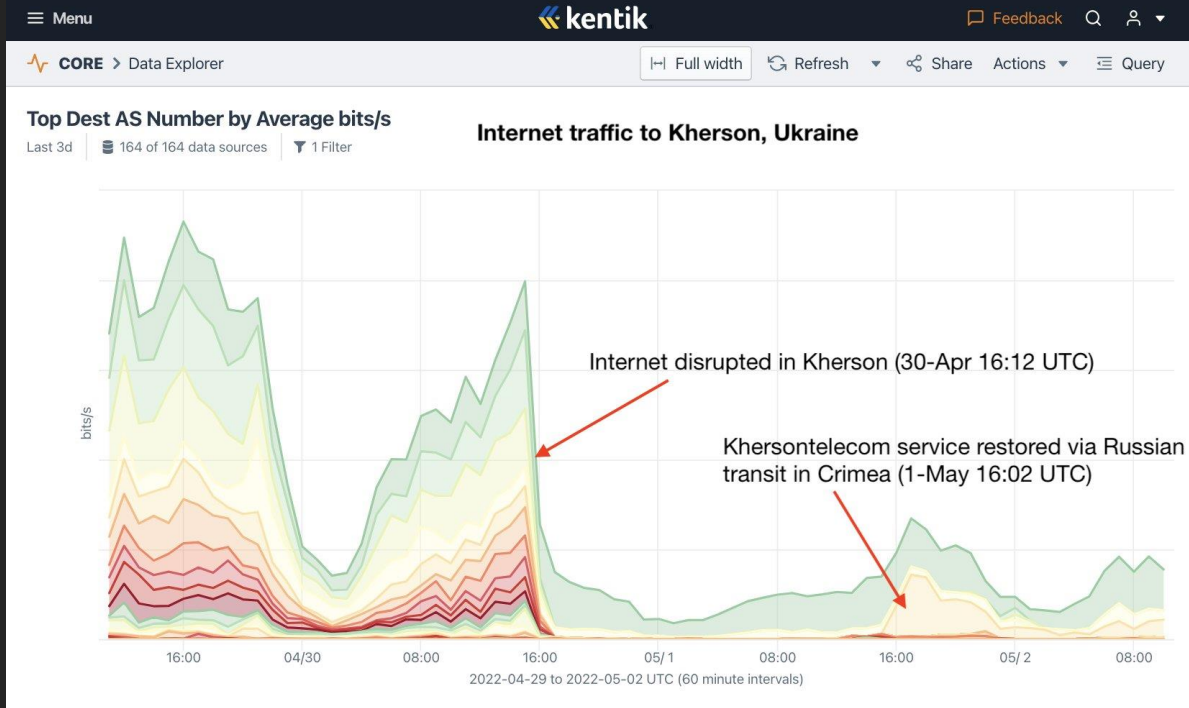
# Manipuler le réseau à des fins stratégiques

- Déconnexion progressive entre Donbass et Crimée et les fournisseurs ukrainiens
- Reconnexion simultanée à Internet à travers fournisseurs russes
- Déploiement d'une « puissance topologique » russe par l'infrastructure logique
  - Les câbles Ukraine – Donbass existent mais ne sont plus utilisés



# Appropriation territoriale par l'infrastructure : une stratégie opérationnelle russe

- Phénomène très visible en 2022: "The first thing the Russians do when they occupy Ukrainian territory is cut off the networks" Stas Prybytko, ministère des télécommunications
  - Kherson, cas principal



"TODAY THEY ARE BRINGING THEIR FIBER FROM CRIMEA TO THE CITY TO COMPLETELY BLOCK THE INTERNET. WE KNOW THAT RUSSIA IS NOT THE WORLD WIDE WEB, BUT A CUT-OFF BLOCKED INTERNET. AND THEY ARE NOW TRYING TO BLOCK INFORMATION. THE TELEPHONE AND MOBILE NETWORKS HAVE BEEN BLOCKED FOR ALMOST A WEEK, AND THERE IS NO INTERNET. THIS IS DONE TO THROW RESIDENTS INTO AN INFORMATION VACUUM"

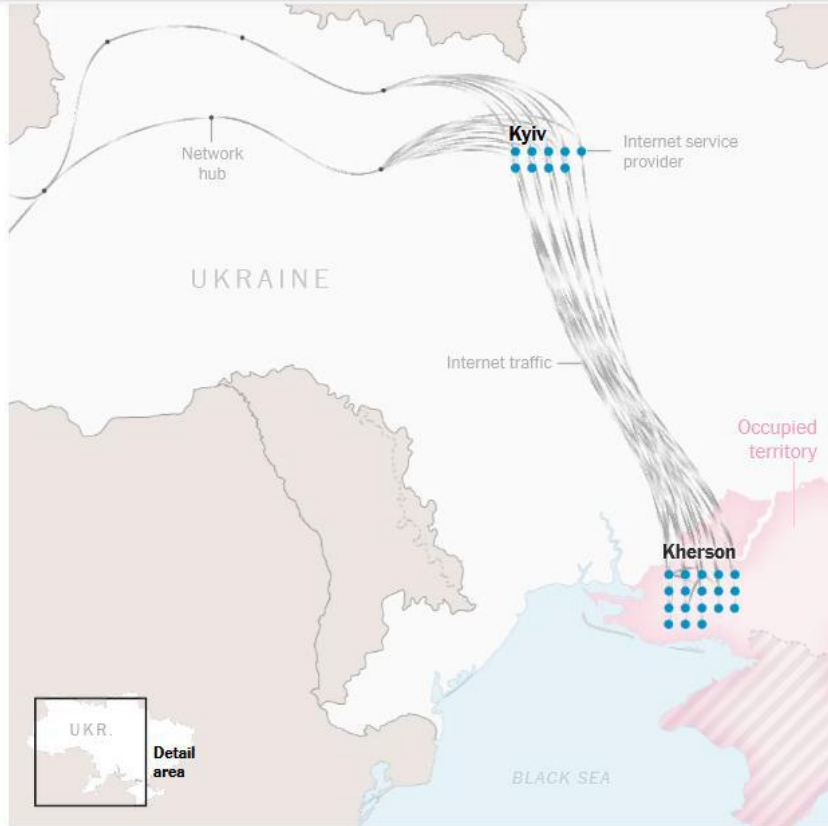
”

Mayor of Melitopol Ivan Fedorov

# Territorialiser le routage pour contrôler le territoire

The New York Times

TECHNOLOGY | How Russia Took Over Ukraine's Internet in Occupied Territories



**May 29**

Kherson stayed connected to the global internet even after Russian forces took control in March.



**June 1**

Then the connection closed. Russian authorities rerouted Kherson's internet traffic through a state-controlled network in Crimea.



**June 5**

Russia has only added to the network infrastructure, routing more traffic through Moscow to strengthen its control of Kherson's internet.

Source: Kentik (traffic data); Institute for the Study of War with American Enterprise Institute's Critical Threats Project (occupied territory) • Note: Internet service provider and traffic route locations are approximate. The service area for one provider whose traffic has been routed through Crimea could not be verified and is not shown.

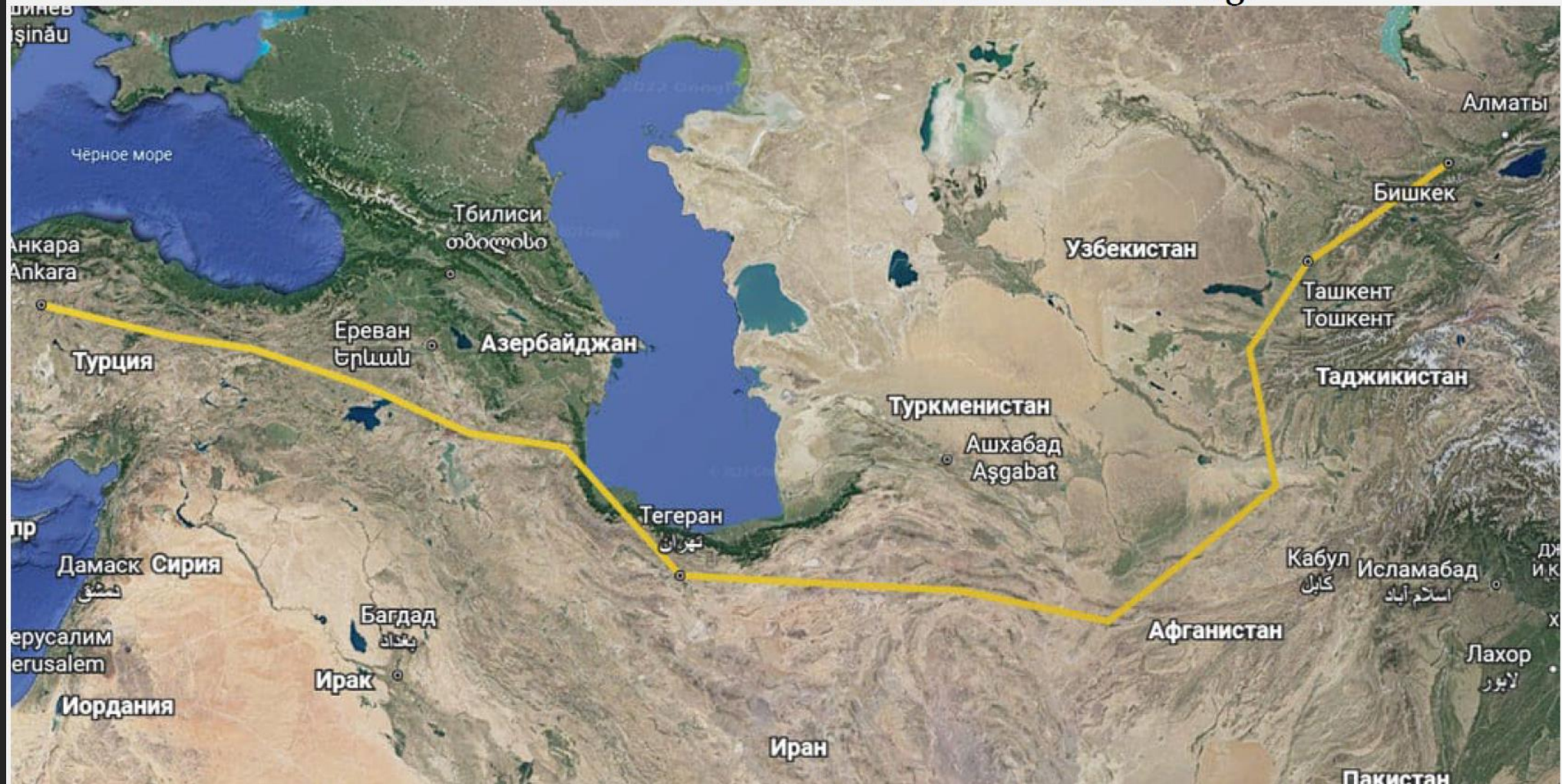
# Conséquences du contrôle du routage

- Censure territorialisée
  - Communications interpersonnelles trans-front
  - Information et diversité de l'information
  - Organisation collective (espionnage)
  - Indisponibilité (relative) des Services publics (Diia)  
/ privés (banques)
- Et contournement
  - Usages des VPNs
  - Maintien du réseau physique
  - Solutions techniques alternatives



# Contourner les dépendances infrastructurelles : l'exemple kirghize

7. Planned cable between Ankara and Bishkek (source: *Economist.kg*)



# Politisation croissante de l'infra de routage : le cas de l'Ukraine

- Cas unique dans un pays en guerre d'équilibre introuvable
  - Besoin de contrôle des routes
  - Besoin d'adhérer aux normes et valeurs occidentales en termes d'ouverture du réseau
- Complexité des interactions et débats entre acteurs
  - Acteurs de l'Etat ukrainien
  - Agences de sécurité : RNBO, SBU
  - Agences de régulation : NKRZI, NCU
  - Opérateurs Internet (FAI, registres DNS...)
  - Groupes consultatifs / acteurs de la gouvernance (UIA)
  - ONG / Associations / presse
  - Organes supranationaux : CEDH, OSCE

## Pratiques et controverses de souverainisation de l'espace info ukrainien

- ◆ 2017 : Blocage accès à différentes ressources russes, notamment domaines et sous-domaines de Yandex, Vkontakte, Odnoklassniki, Mail.ru
- ◆ Ajouts entre 2018 et 2021 : 600 domaines en tout
  
- ◆ Transformation de l'infrastructure qui dévoile une **vision sécuritaire**, une « *conception et [...] administration des infrastructures [qui] intériorisent des valeurs politiques et économiques qui finissent par influencer le champ de la liberté [...] en ligne* » (Musiani, 2018)

# Le délicat équilibre d'une politique ukrainienne de souveraineté informationnelle

- Nombreuses critiques
  - Institutionnelle : Yuriy Stets (ministre politique de l'information) « Les médias sociaux sont un monde où les gens peuvent échanger des informations. Si vous y allez pour censurer (car c'est de la censure, purement et simplement), vous ne censurez pas le réseau social, mais la personne spécifique qui y publie. Il s'agit déjà d'une atteinte à la Constitution. »
  - Acteurs privés : NetAssist conteste la décision de la NKRZI
  - Société civile : comparaisons avec le Runet souverain (SBU recommande installation boîtiers de contrôle)
  - OSCE
- SBU : « L'Ukraine adhère à toutes les normes d'une société démocratique. C'est pourquoi il est souvent difficile de rassembler rapidement des preuves et de bloquer rapidement les canaux de diffusion de fausses nouvelles »

## A partir de 2022 : une problématique renouvelée

- « Nous sommes le premier pays au monde qui, au XXIe siècle, est contraint de repousser l'ennemi dans quatre espaces à la fois » (Min. Def. Ukraine)
- Multiplication de mesures de blocage
- Blocage 600 réseaux russes : coupure de nombreuses « routes d'Internet »
  - Dimension inédite
  - Un autre niveau d'infrastructure touché
  - Equivalent d'un blocage de 48 millions d'IP russes : indiscrimination
- Controverse moindre
  - Acceptation de la loi martiale
  - Une contestation de NetAssist déboutée
  - Contrôle difficile et manque de transparence : rapport des entreprises n'est pas public

# Conclusion: un intérêt politique croissant pour le routage

- Emergence et consolidation de la vision stratégique du routage
  - Contrôle étatique : Chine, Iran, Russie, Allemagne
  - Etats (externe)
    - Stratégies territoriales (Russie)
    - Ukraine
  - « Sanctions privées » (Cogent, Lumen, LINX)

## FCC wants rules for ‘most important part of the internet you’ve probably never heard of’

U.S. agencies want to secure the Border Gateway Protocol, but experts question whether their approach could worsen security.

BY TIM STARKS • APRIL 24, 2024