Routage et infrastructures dans le conflit en Ukraine
Attaques, détournement, résilience

Louis Pétiniaud

Que nous apprend l'architecture des réseaux ukrainiens sur la situation géopolitique aux échelles nationale et locale?

- Internet et routage = objets sociotechniques
  - Routage influence dynamiques géopolitiques / géopolitique influence routage
- Trois étapes :
  - Etat initial du réseau ukrainien
  - L'appropriation territoriale par la Russie à travers le réseau 2014 - 2021
  - 2022 : nouveaux détournements, attaques et résilience du réseau

La connectivité comme phénomène géopolitique

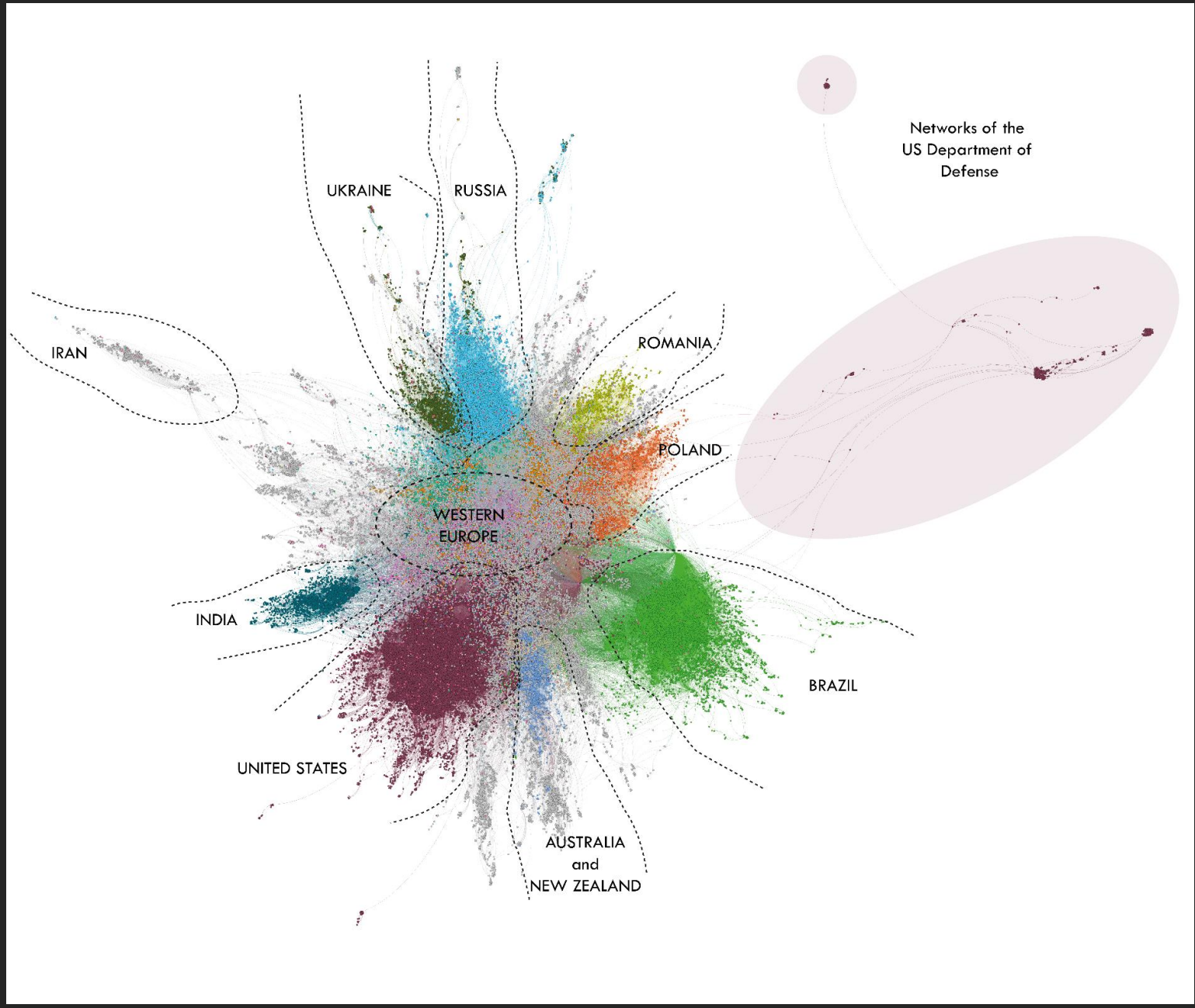
- **Fonctionnement et interconnexion des AS sont stratégiques et géopolitiquement significatifs**
  - **Administration interne de l'AS**
    - Mécanismes et algorithmes de routage => inconnus
  - **Choix du voisinage**
    - Le choix pour un AS de ses voisins est géopolitiquement significatif.

- **Un AS est partiellement « territorialisé »**
  - Différentes échelles à prendre en compte
  - international / national / régional / local

Méthode = inférence de topologie par updates BGP

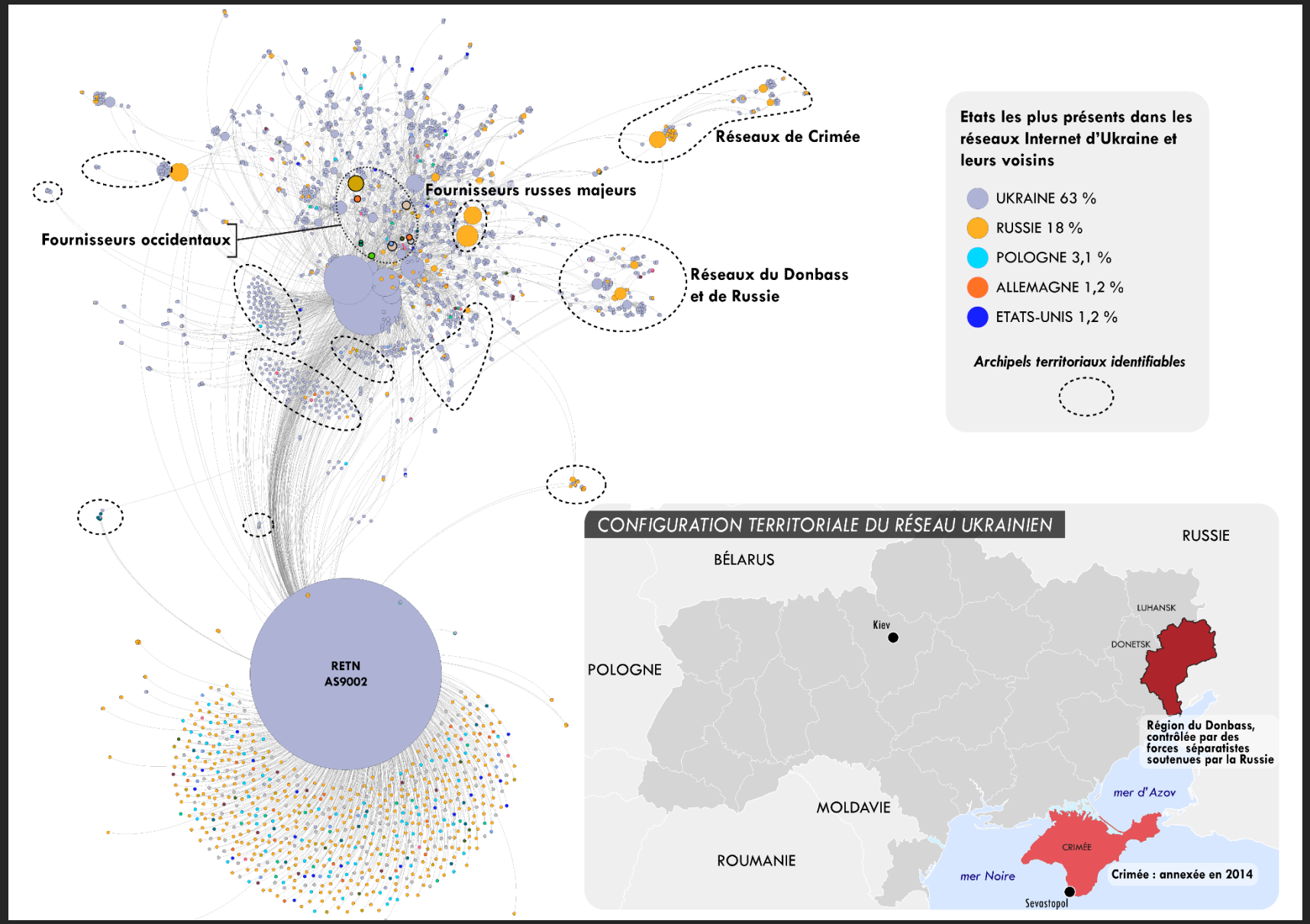
- BGPstream : inférence de liens à travers annonces de chemins
- Données issues de plusieurs feeds BGP issus de différents points d'observation
- Une capture des annonces par minute
- Au bout d'une heure environ : graphe mondial de plus de 70 000 AS
- **Représentation en graphe**

- Limites = Architecture incomplète



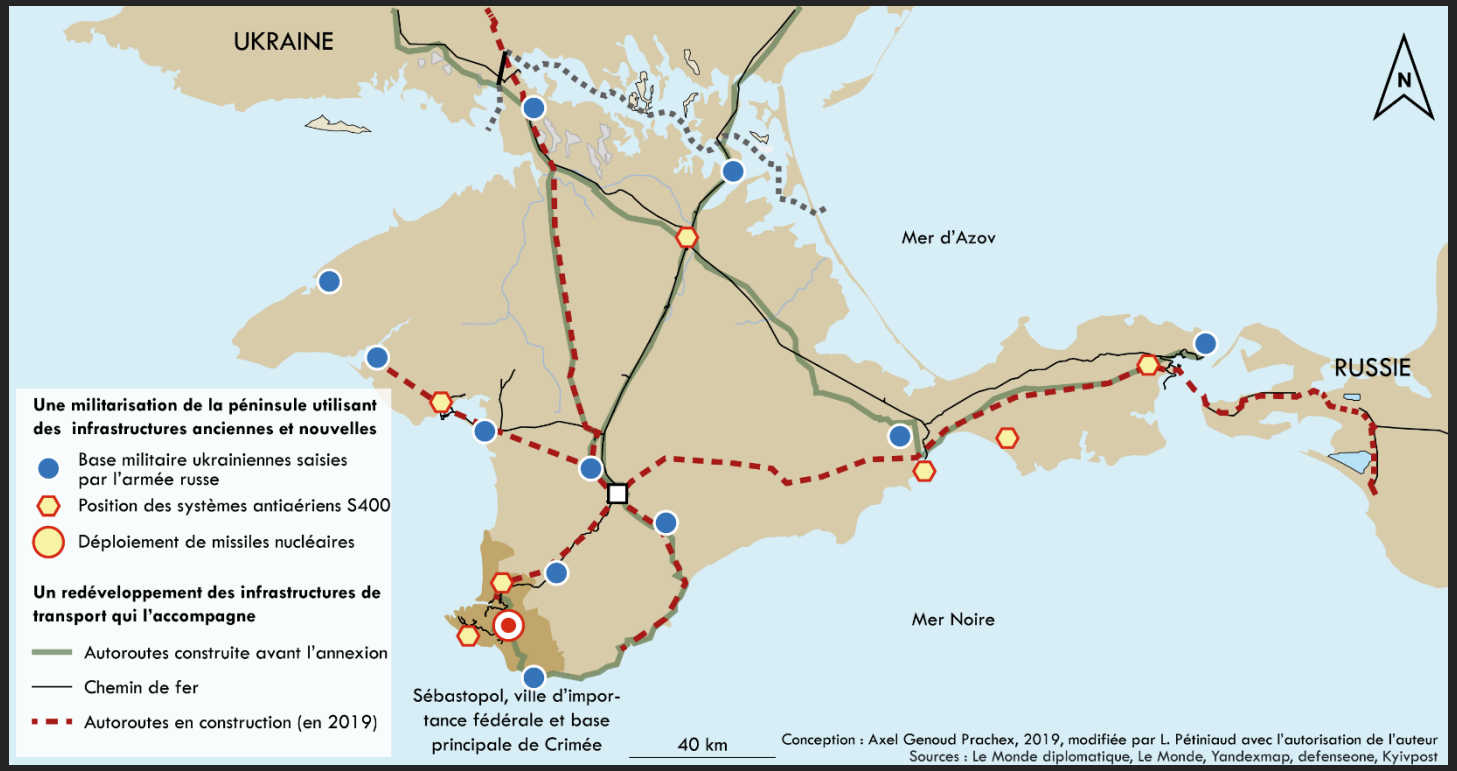
Ukraine t=0 : réseau décentralisé et résilient

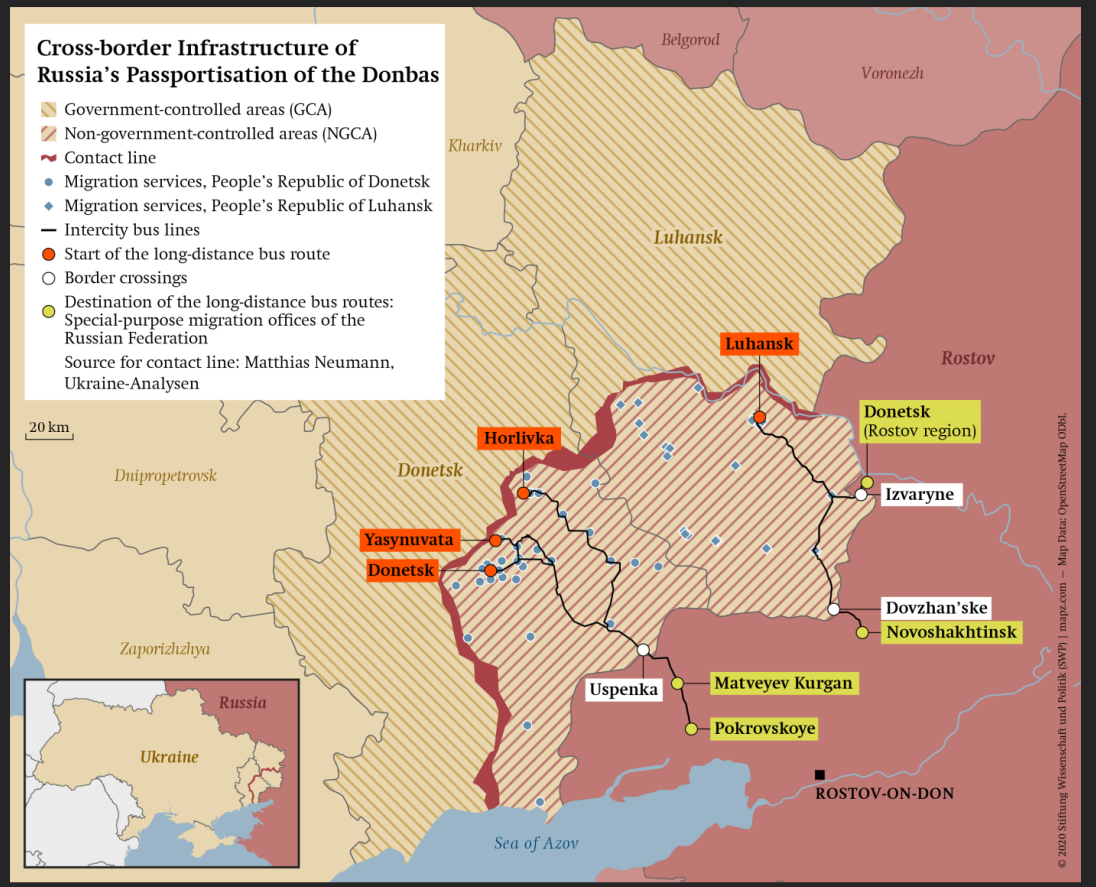
- Nombreux points de contrôle
- Un des marchés les moins concentrés du monde



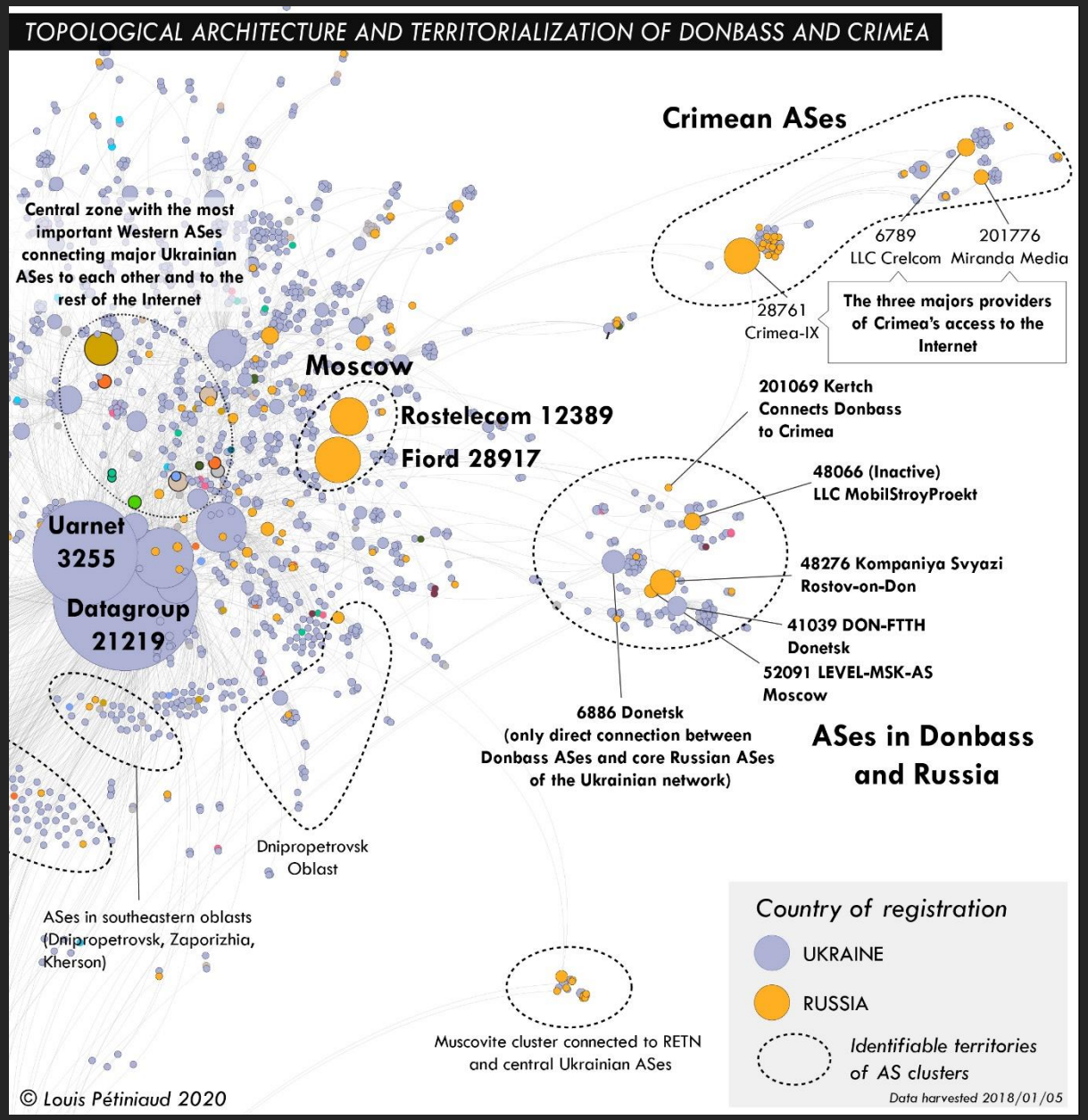
2014 – 2021 : deux situations différentes d'appropriation territoriale

- Crimée : annexion, coupure frontalière physique, rattachement infrastructurel, mainmise politique russe
- Donbass : « zone grise », rôle croissant de Moscou, coupures infrastructurelles progressives, « passeportisation »

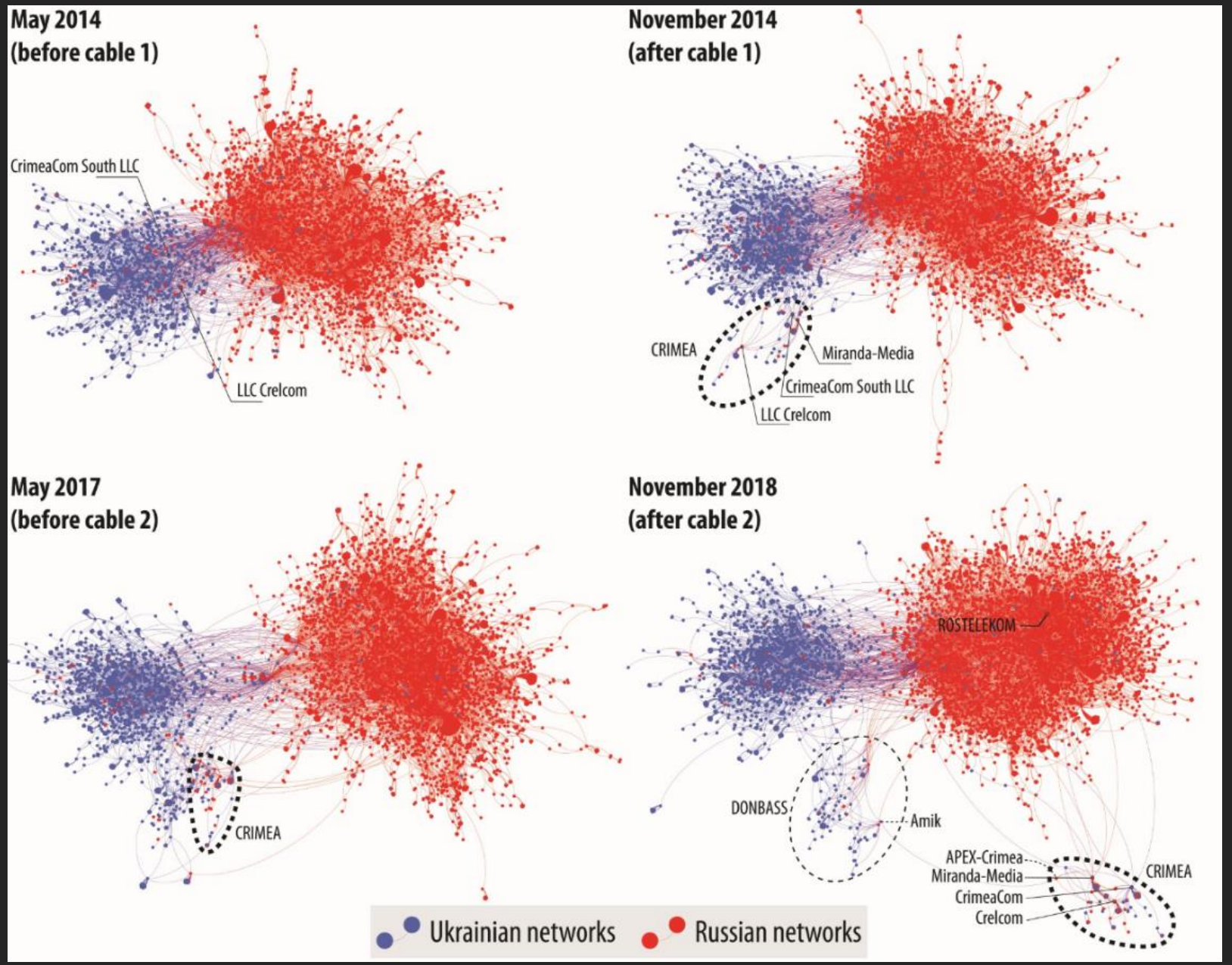




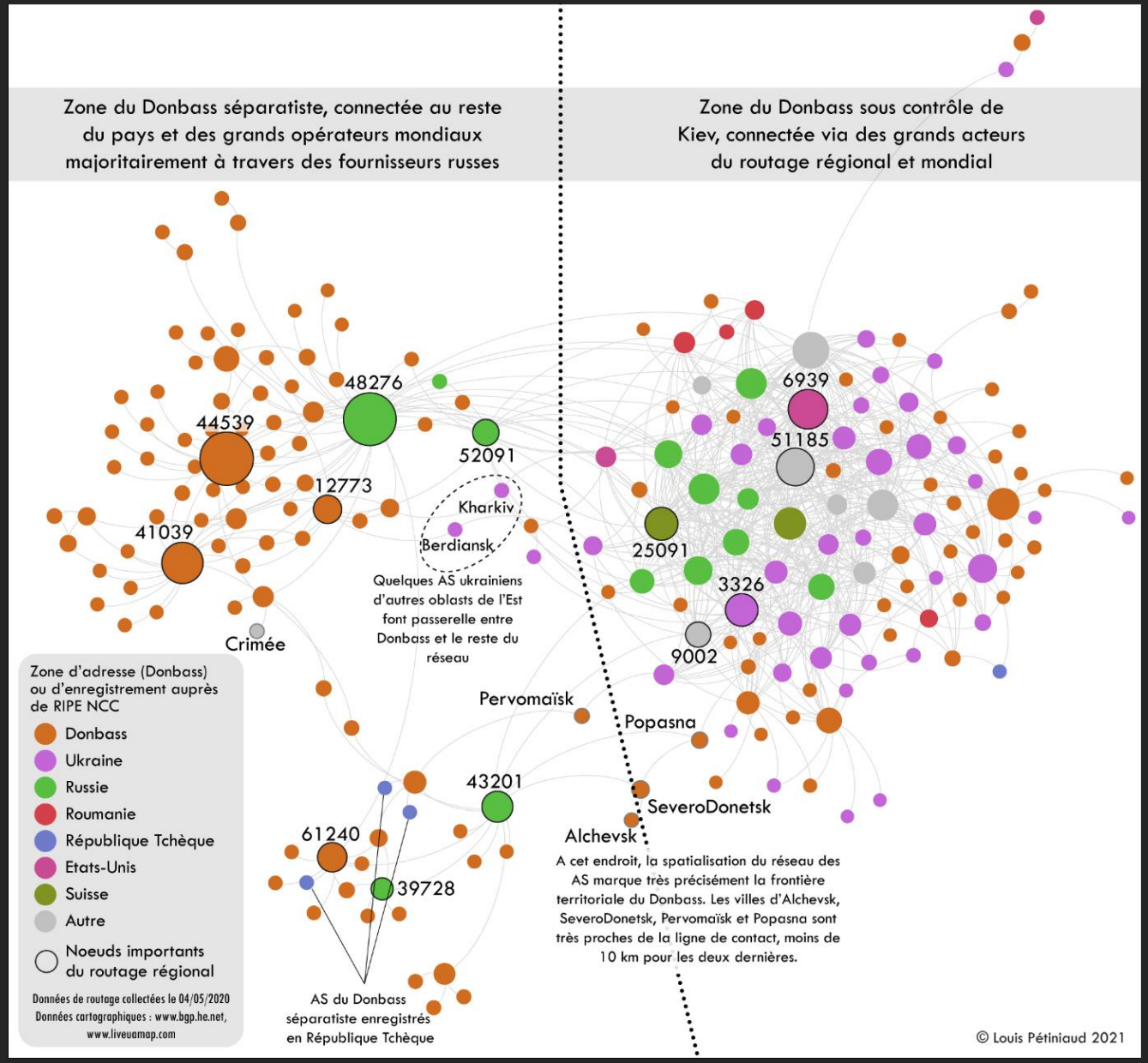
Une appropriation « par » l'architecture logique



En Crimée, une appropriation totale des réseaux

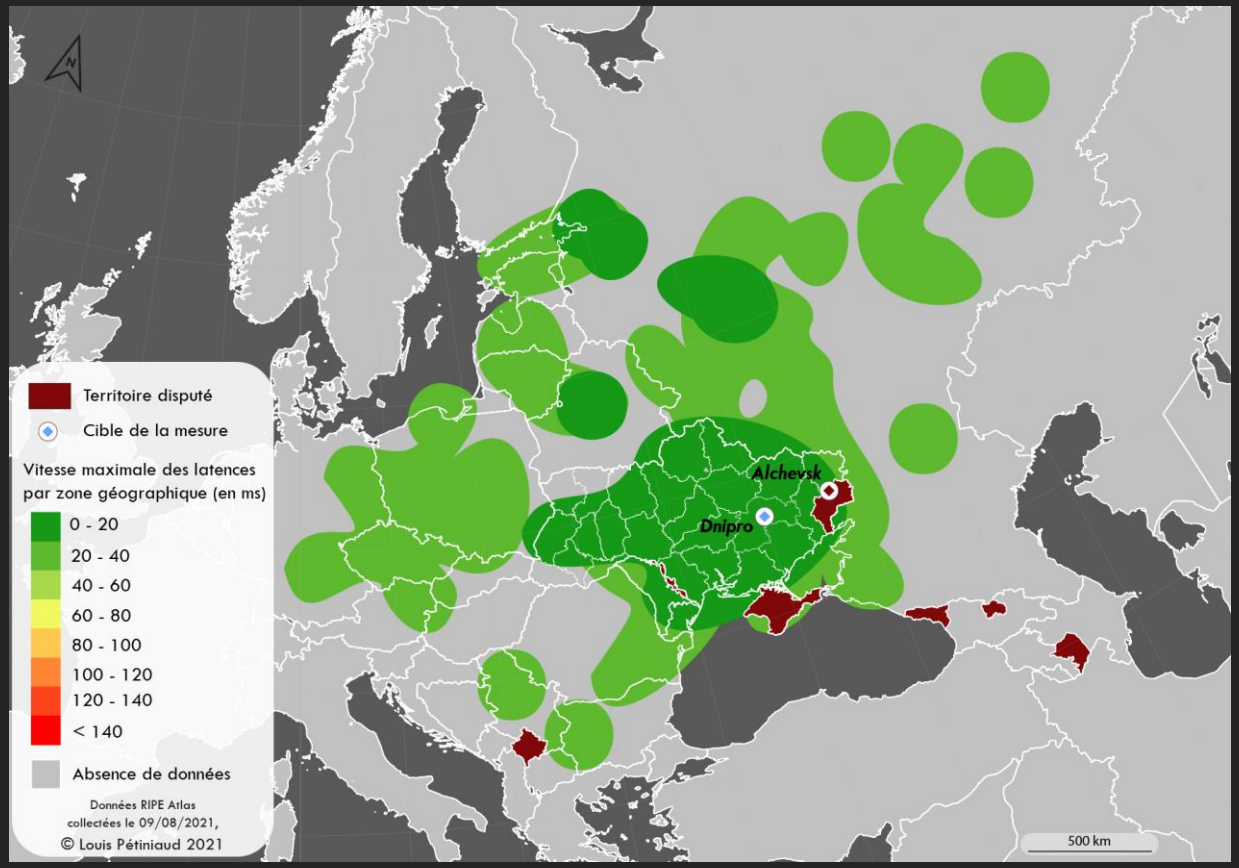


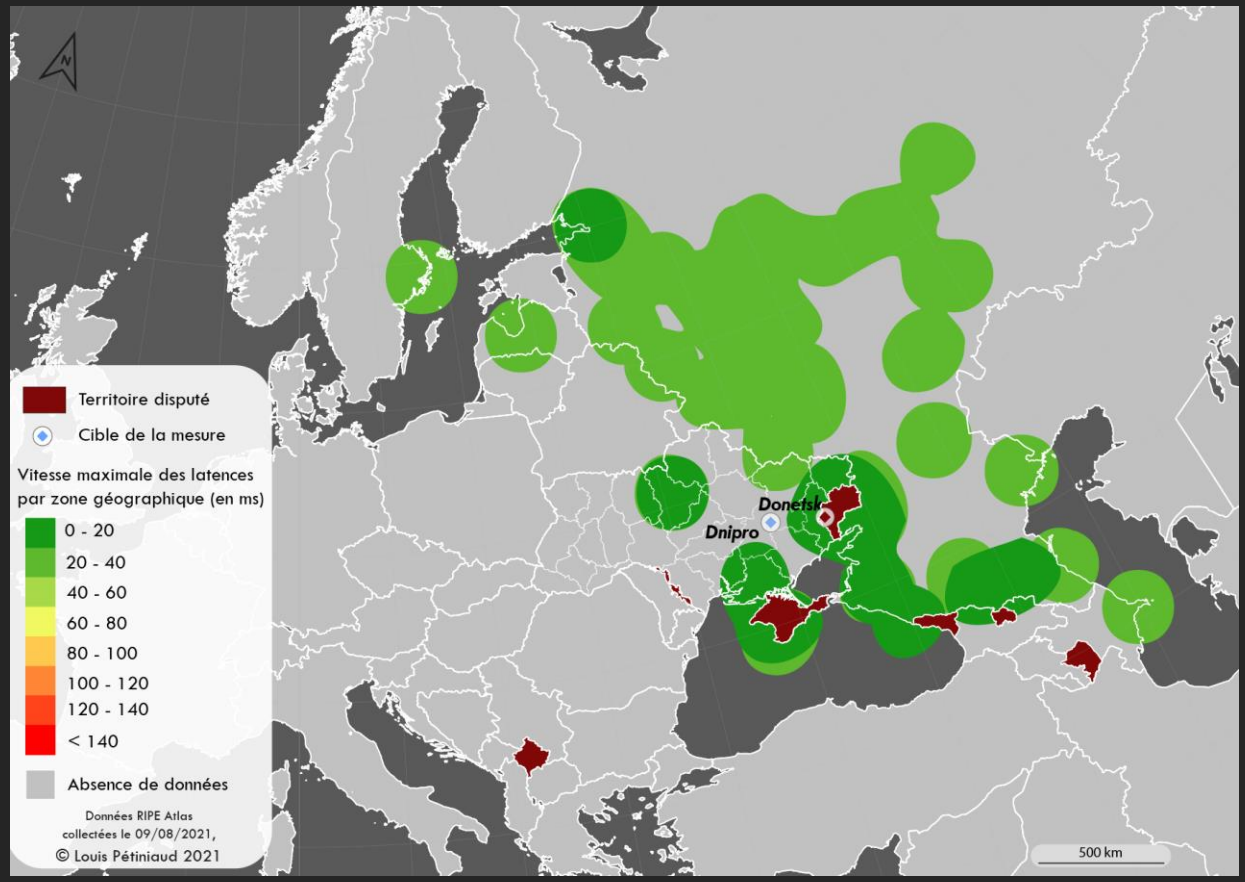
Dans le Donbass « séparatiste » en 2020, une dépendance forte aux réseaux russes



Des différences de latences importantes de part et d'autre de la « frontière »

Traceroutes (RIPE Atlas) sur Dnipro (Ukraine) et Donetsk (contrôlé par Moscou)





Quelles conséquences potentielles des dépendances logiques

- Filtrage / blocage
  - Dans le cadre d'un conflit ouvert
  - Moyen de pression
- Espionnage
  - Détournement et inspection des données y compris chiffrées
- Renforcement général de **l'appropriation territoriale** à travers l'infrastructure (logique)
  - Intégration *de facto* au projet (complexe) de « Runet souverain » fondé sur le contrôle
  - Censure des plateformes et services occidentaux vient s'appliquer *de facto*

2022 - Conflit de haute intensité, infrastructures, et architecture

- Février 2022 : invasion de l'Ukraine par la Russie
- Importance relative des réseaux physiques et logiques
  - Difficile à évaluer, besoin de recul, d'informations, et de tri

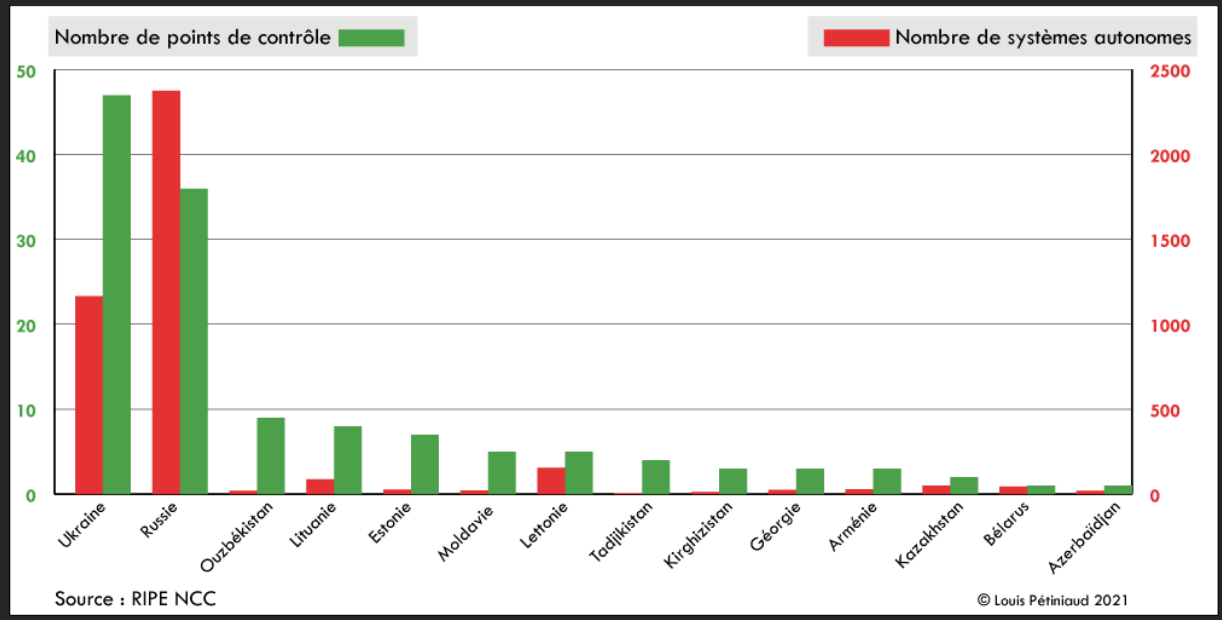
- Deux dynamiques d'intérêt
  - Attaques contre infrastructures physiques
  - Reroutage de trafic

Attaques contre infrastructures

- Pour le moment : relativement faible et/ou peu efficaces
  - Réseau ukrainien est décentralisé donc résilient
  - Réparations fréquentes

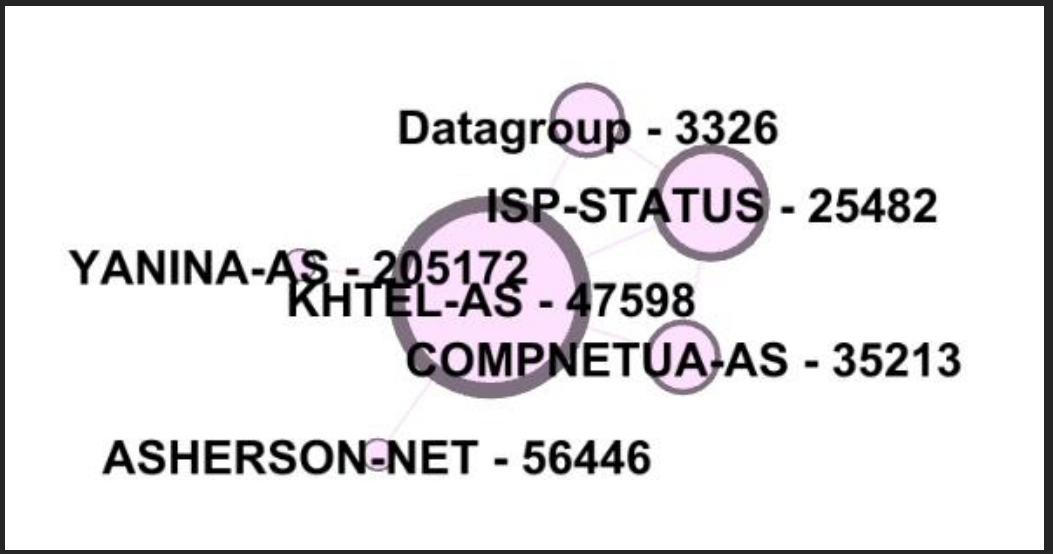
- Y a-t-il un objectif russe de viser les infrastructures ?

  - **Différentes hypothèses :**
  - Besoin pour leurs propres communications
    - En partie confirmé
  - Outil de renseignement pour la Russie
    - ?
  - Conservation des infras pour « l'après »
    - Probable => facilite le contrôle de l'information + espoir d'une guerre rapide
    - Cas de Marioupol



Reroutages de trafic

- Phénomène croissant, beaucoup plus rapide que pour le Donbass, mais changeant rapidement
  - Différents exemples relevés dans les régions du sud notamment, mais à confirmer : sources changeantes sur AS 47598



AS number	47598
AS name	KHTEL-AS
organization	PE "Khersontelecom"
country	Ukraine
AS rank	5207
customer cone	4 asn, 5 prefix, 2816 address
AS degree	7 global, 7 transit, 4 provider, 0 peer, 3 customer

AS Rank ▲	AS neighbors ▽	Organization		AS customer cone ▽	number of paths	relationship
74	3326	PRIVATE JOINT STOCK COMP...		615	487	provider
284	12883	PRIVATE JOINT-STOCK COMP...		149	46	provider
364	201776	Miranda-Media Ltd		108	405	provider
1782	35213	TOV "Kompjuternie Merezhi"		15	48	provider
29754	205172	FOP Hudz Yanina Valeriivna		1	194	customer
52281	56446	PC Kherson Telecom		1	195	customer
57728	49168	PE Brok-X		1	205	customer

  - Graphes du réseau ukrainien 2022 : plus complexes à lire

Quelles conséquences en 2022 ?
Enjeux de l'accès à Internet en situation de conflit

- Communications interpersonnelles
- Organisation collective
- Information et diversité de l'information
- Services publics (Diia) / privés (banques, achats, etc.)

Conclusions : plus de questions que de réponses

- Quel(s) type(s) de leviers une dépendance réseau entraîne-t-elle ?
- Dans quelles situations pourraient être activés ces leviers ?
- Quel est l'efficacité opérationnelle d'une déconnexion ?
- Quels sont les effets pour les populations ?

- Questions de recherche
- Routage et droit international : sanctions ?