APTs: des liens entre crime et Etat… et autres questions de RI soulevées par les APTs

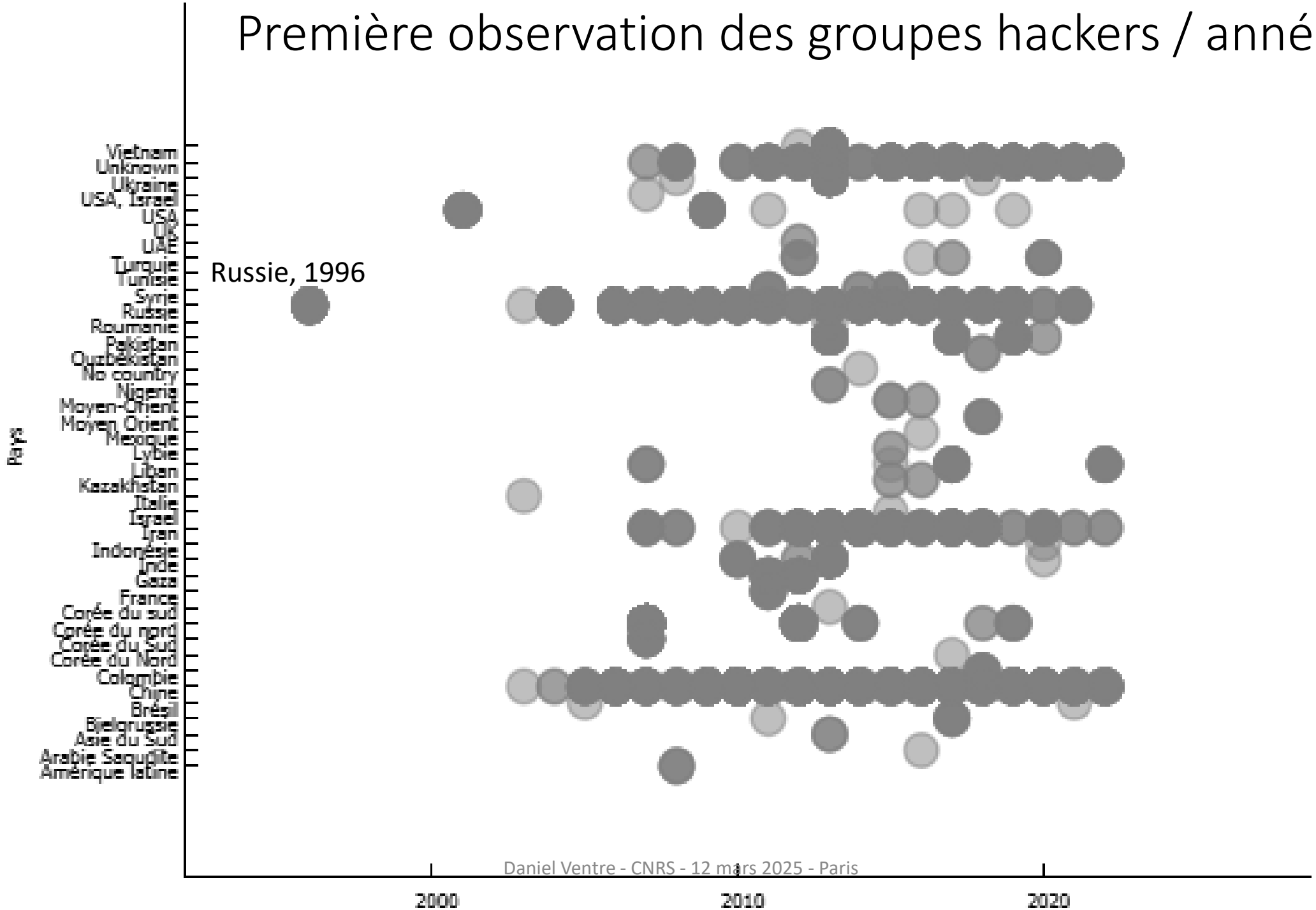
12 MARS 2025 – Campus CYBER

Daniel VENTRE – CNRS / Laboratoire CESDIP

Rappels sur les origines de l'expression

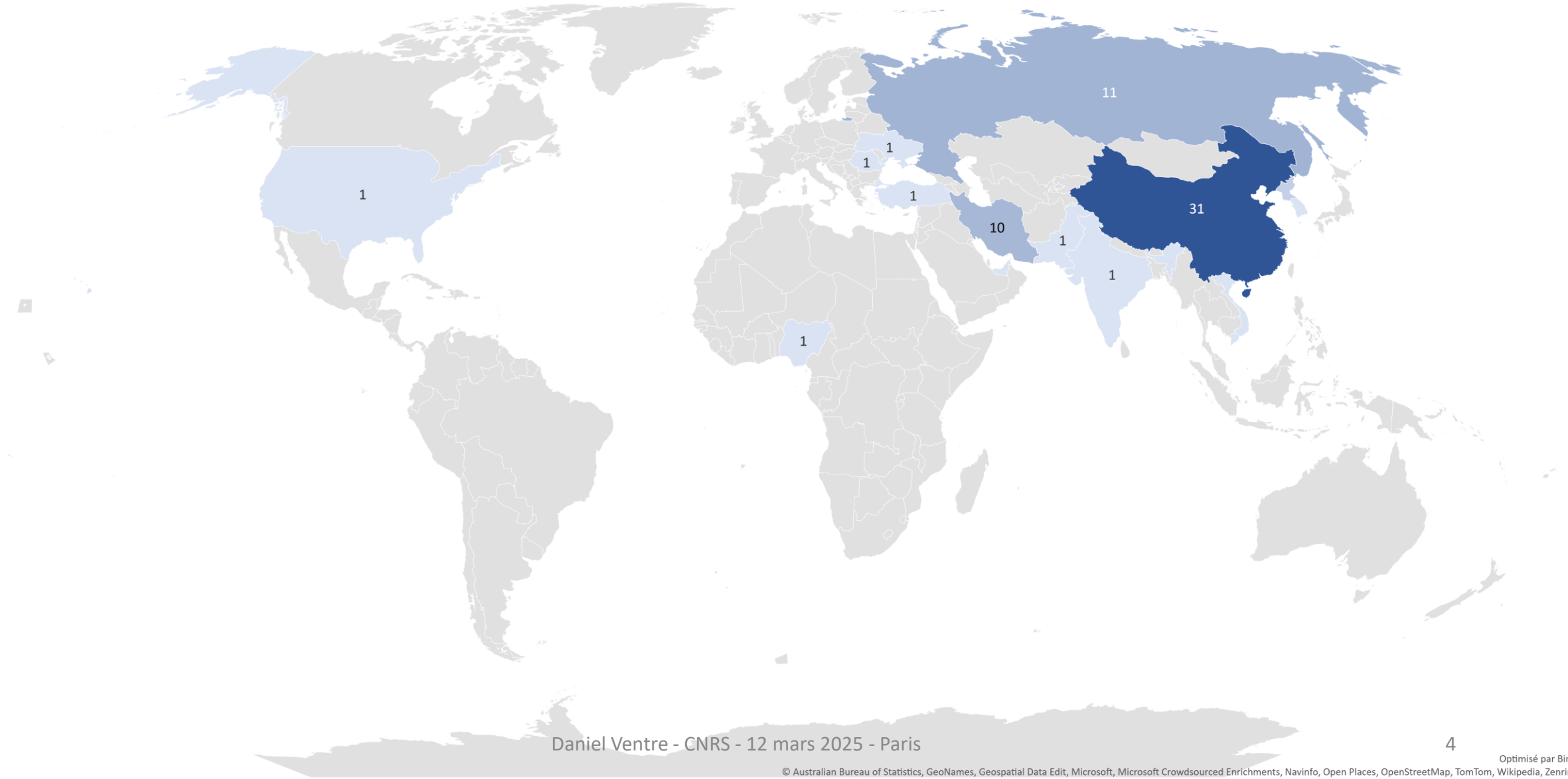
- L'expression apparaît fin des années 1990
- Aux USA
- Introduite par un militaire
- Pour désigner des opérations de cyber-espionnage étrangères

Première observation des groupes hackers / année / pays



Russie, 1996

Pays hébergeant des APTs (base it.) (nombre de groupes). Reconstitué d'après la base créée par Giorgio Di Tizio, Michele Armellini, & Fabio Massacci. (2022)



Evolution terminologique

- Initialement APT désignait une technique d'attaque

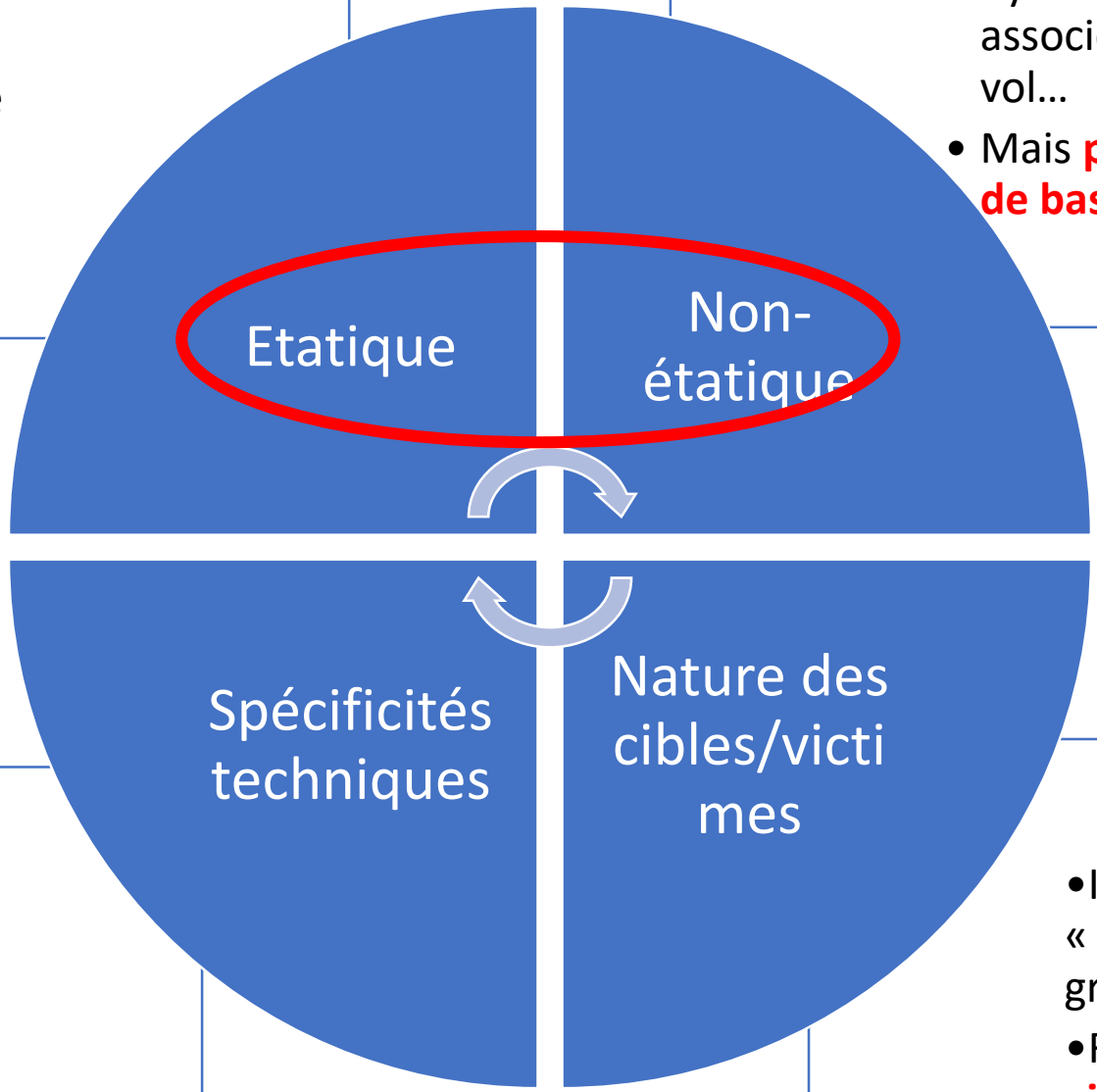
- Désormais APT désigne aussi les « groupes » qui utilisent ces méthodes d'attaques

Un vocabulaire de la violence

- Vocabulaire « **militaire** » ou de « **guerre**) (stratégie, campagnes, assauts); Stratégique (plutôt que tactique)
- Renseignement, **espionnage** (Covert, targeted, undetected, espionnage…) Furtivité, invisibilité

Une violence qui conjugue les efforts de l'étatique et du non-étatique

- Cybercrime indépendant, associé, commandité, vol…
- Mais **pas une criminalité de base ordinaire**



Objectifs « stratégiques »

- **Haut niveau**, complexité, pas commun
- Temporalité (**attaques long terme**)

- Infrastructures « **critiques** », Etats, grandes industries
- Risques essentiels, **vitaux**, déstabilisation

- **En raison des spécificités propres aux APTs** [contraintes techniques, capacitaires de haut niveau + nature stratégique des cibles et objectifs + durée), **on attribue généralement les APT aux Etats**
  - Leurs armées, leurs agences de renseignement
- **Ou à des groupes non-étatiques mais cooptés** par l'Etat, **affiliés**, etc.
- On dit qu'avec les APTs, **les lignes se trouvent brouillées entre les catégories: à la croisée de l'étatique et du criminel, du militaire et du civil…**
- **On évoque l'existence de relations de différente nature: cooptation / sous-traitance / contrainte / relation marchande / …**

La question des liens entre l'Etat et le cybercrime

L'existence d'une relation entre Etatique et non-étatique est au cœur des considérations sur les APTs

Dispose-t-on des éléments suffisants pour étudier ces relations?

Pour étudier les APTs on dispose de plusieurs sources d'informations

1 - Rapports d'agences/services **étatiques** sur les APTs

2 - Rapports d'entreprises **privées** sur les APTs

3 – **Données en ligne** : MITRE, ETDA (*497 groups listed (409 APT, 54 other, 34 unknown)*, projets de recherche…

Ces sources sont à la fois **données « techniques » et** commentaires**, analyses, descriptions,** alertes de sécurité…

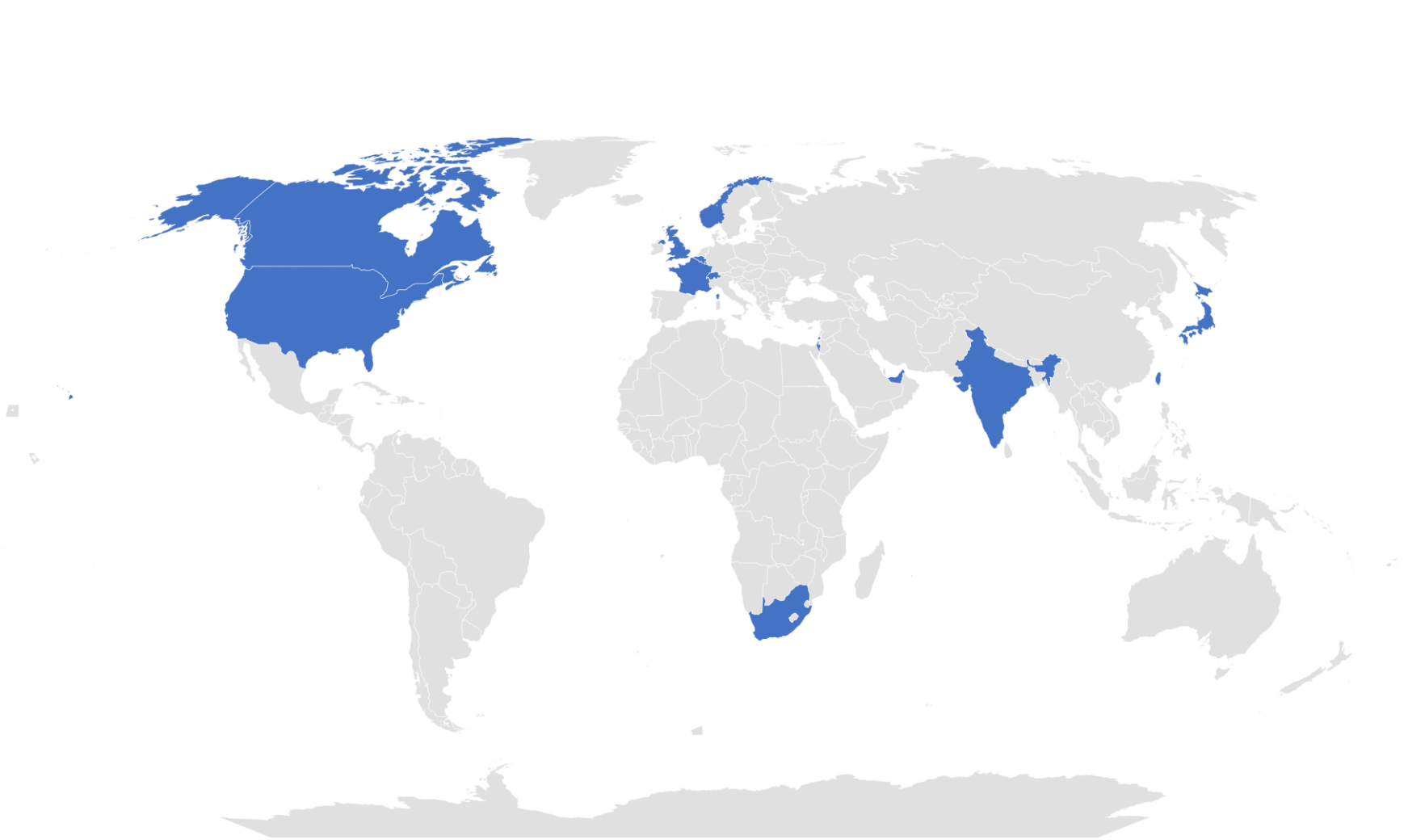
a) Les données permettent par exemple de localiser les APTs (leurs espaces nationaux d'origine) et de cartographier leurs surfaces d'attaques (géographique, sectorielle)

- La **géolocalisation** des sources d'attaques ne renseigne toutefois ni sur la nature « étatique » ou « non étatique » de l'opération APT

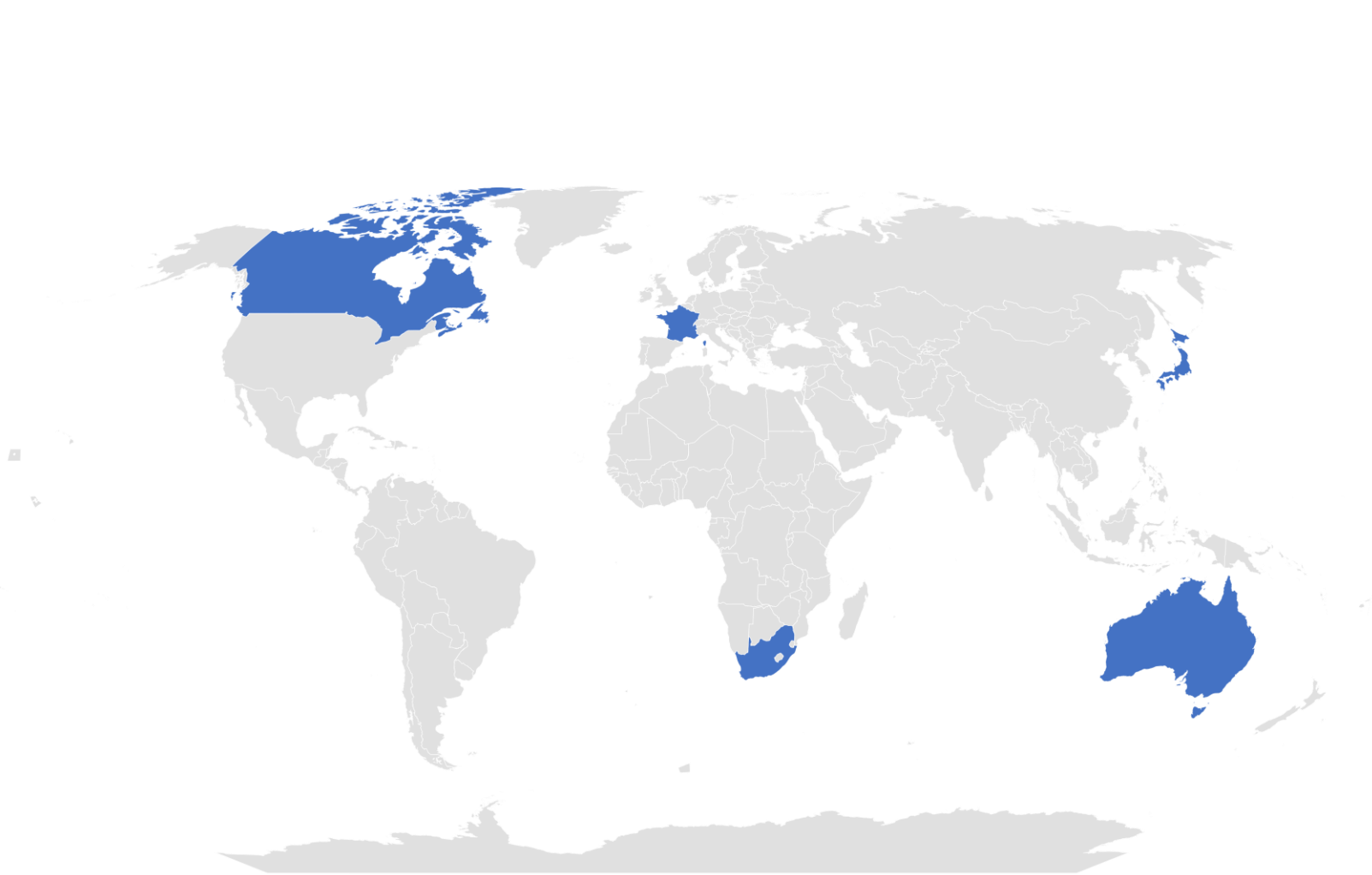
- La **surface d'attaque** associée à une APT peut-elle donner des **indices** quant à la **nature politique/géopolitique** de l'opération (les Etats visés sont des « adversaires ») ?
  - → on pourrait en déduire que l'Etat est à la manœuvre?
  - Mais doit-on alors exclure la mobilisation dans ces actions politiques, d'acteurs du cybercrime?
  - Non
  - Par contre on ne dispose pas des éléments probants (en open data) pour le démontrer

Les APTs ont généralement des surfaces d’attaques délimitées

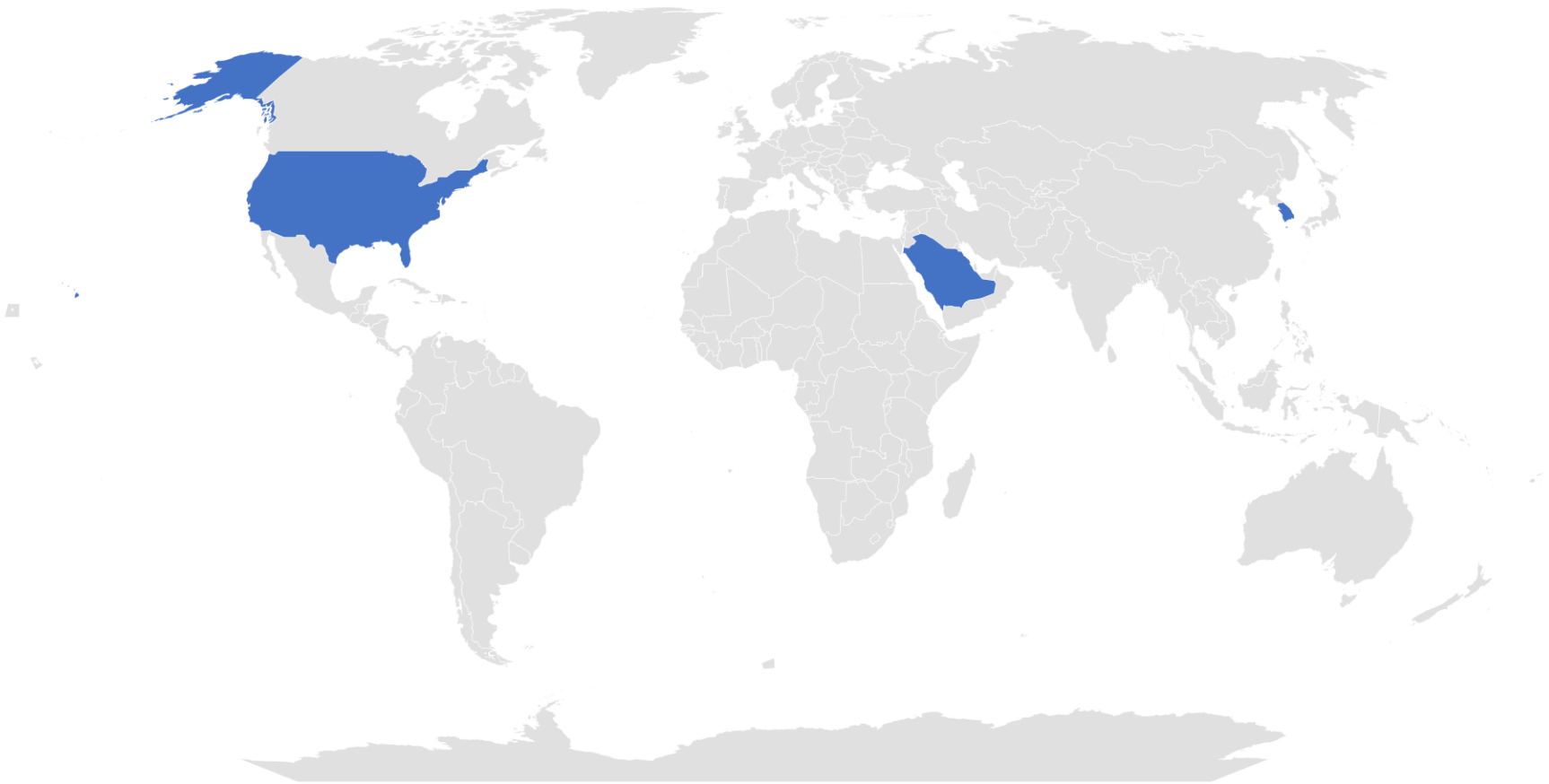
Surface d’attaque d'APT1 (Chine?)



Surface d’attaque d'APT 10 (Chine?)



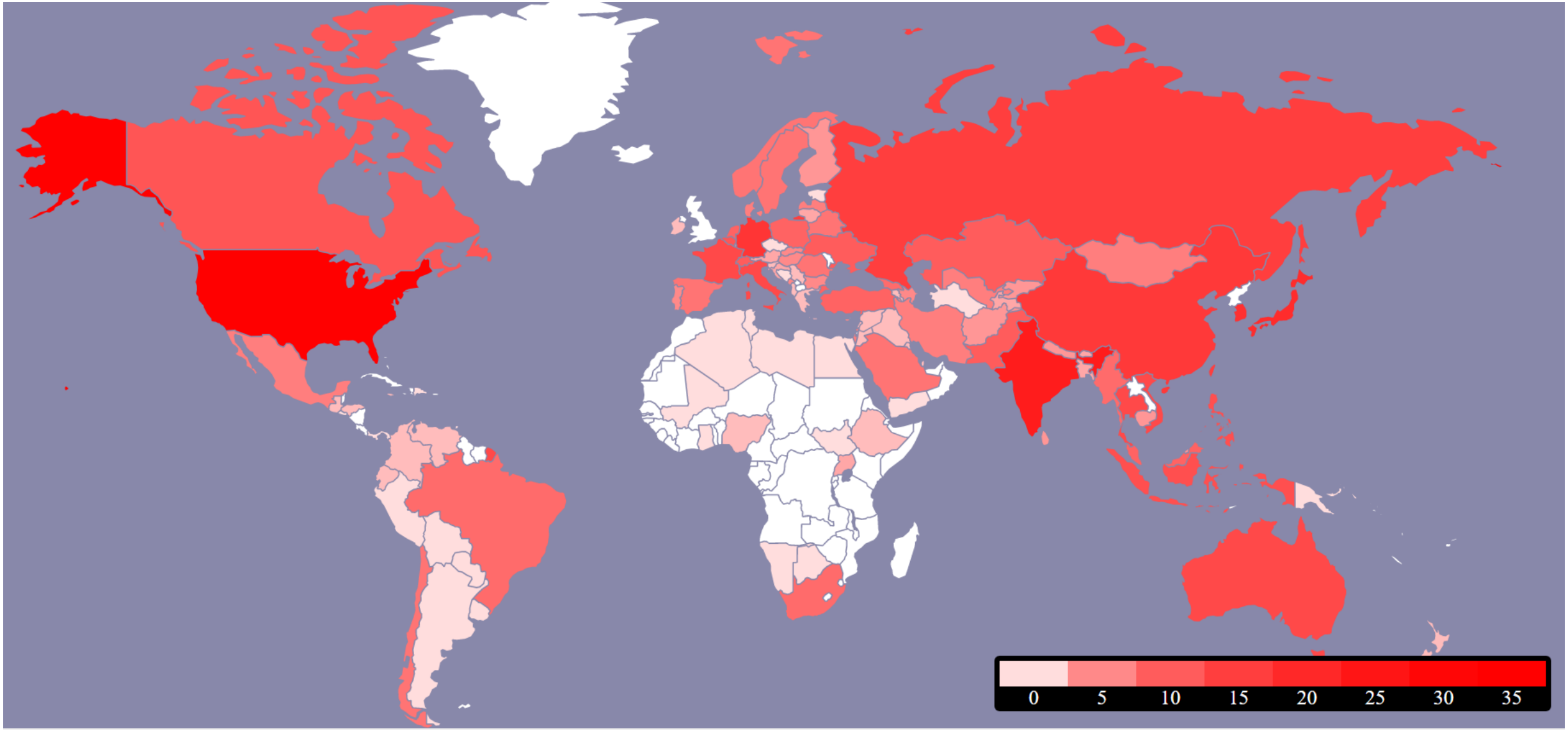
Surface d’attaque d'APT 33 (Iran?)



Surface d’attaque totale des APT russes + chinoises ?

La quasi-totalité des pays de la planète se trouvent ainsi touchés par les attaques émanant des deux principaux pays pourvoyeurs d’APTs

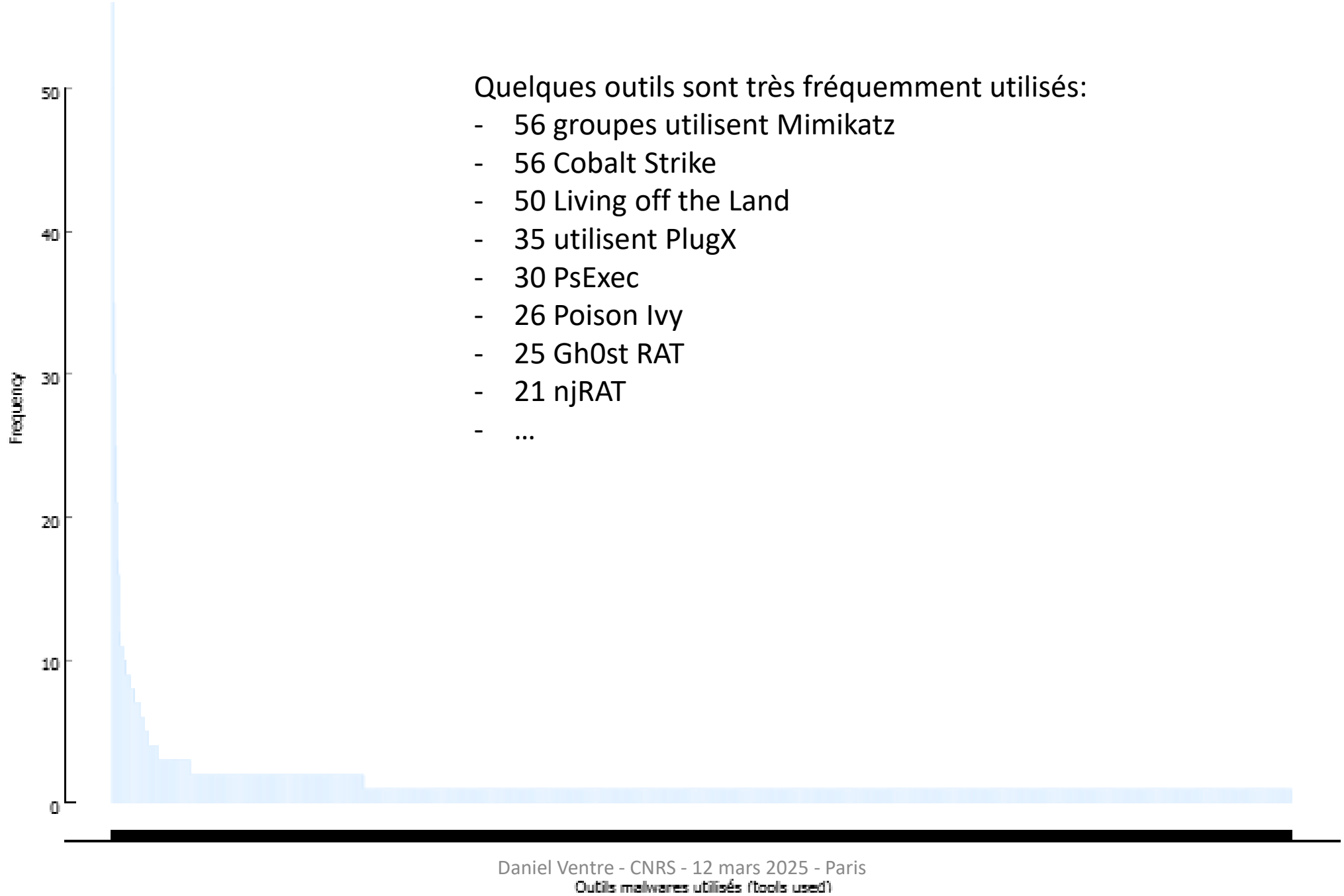
L’ampleur de la surface touchée autorise-t-elle à penser que la tâche serait trop importante pour les seuls acteurs strictement étatiques, et qu’il y a nécessairement interventions/aides tierces?


0
5
10
15
20
25
30
35

b) L’utilisation par les APTs d’outils d’attaques ou de méthodes également utilisés par le cybercrime?

- N’est pas un indicateur suffisant de l’existence de liens formels entre Etat et cybercrime

- Tout au plus y a-t-il emprunt d’outils



Quelques outils sont très fréquemment utilisés:

- 56 groupes utilisent Mimikatz
- 56 Cobalt Strike
- 50 Living off the Land
- 35 utilisent PlugX
- 30 PsExec
- 26 Poison Ivy
- 25 Gh0st RAT
- 21 njRAT
- …

c) Les mentions « state-sponsored », « on behalf of the state »…

- Ces mentions, « étiquettes », sont accolées à certains groupes APTs dans les bases disponibles

- Mais on ne dispose pas des critères qui ont guidé ces choix (comment distingue-t-on, sur la base de quelles informations)

- Et les étiquettes ne disent rien de la nature véritable des liens, de leur force, de leur composition :
  - « state-sponsored » peut être totalement étatique ou soutenu par l'Etat;
  - « on behalf » ne dit pas qui commandite, comment, etc.

Conclusion

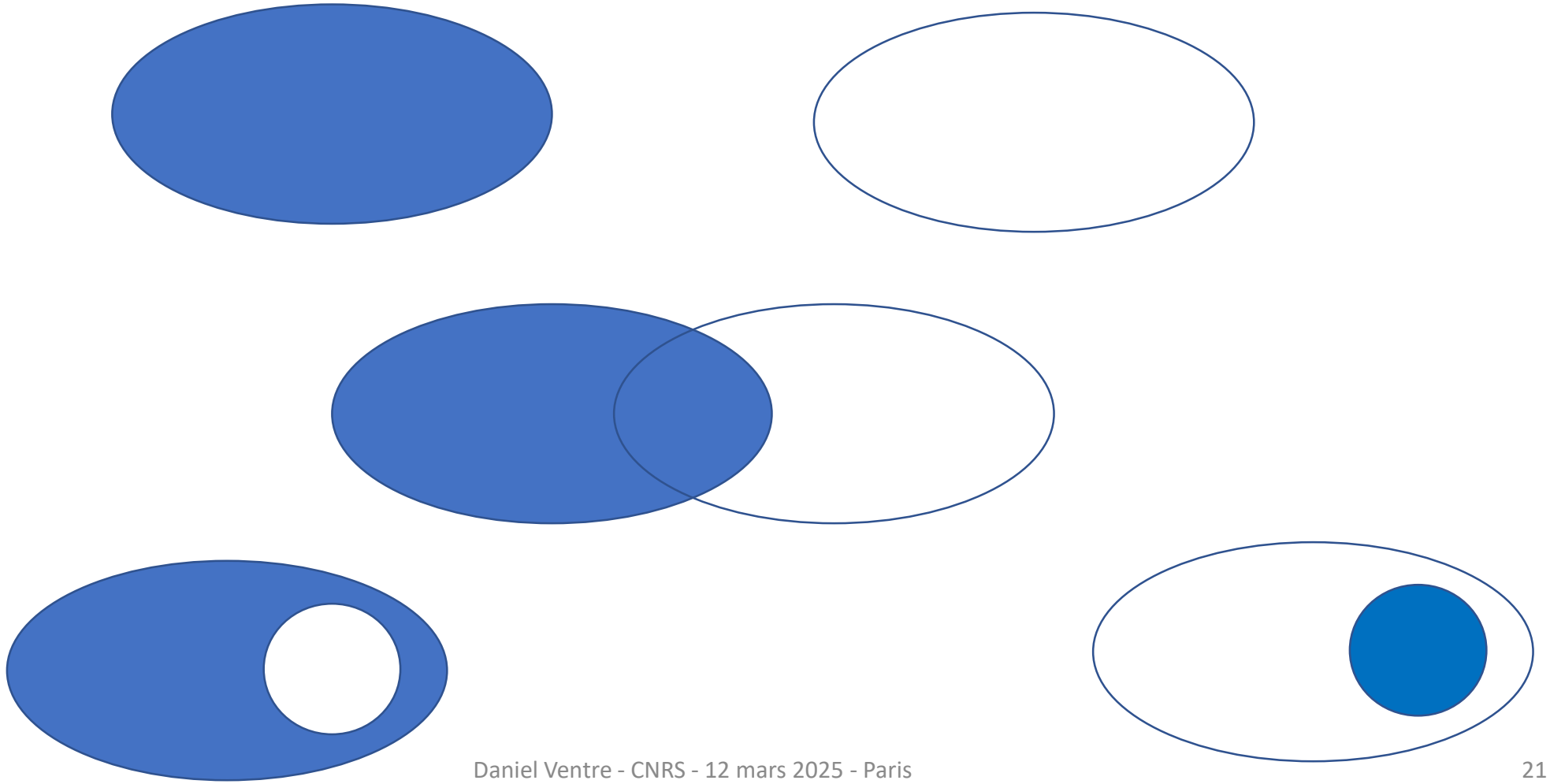
- Les données (open source) sont encore trop insuffisantes selon moi pour étudier très précisément les liens Etat-Crime.

- Il faut donc être vigilant: ne pas céder aux discours qui ne seraient que des fictions, des construction intellectuelles sans connexion au réel

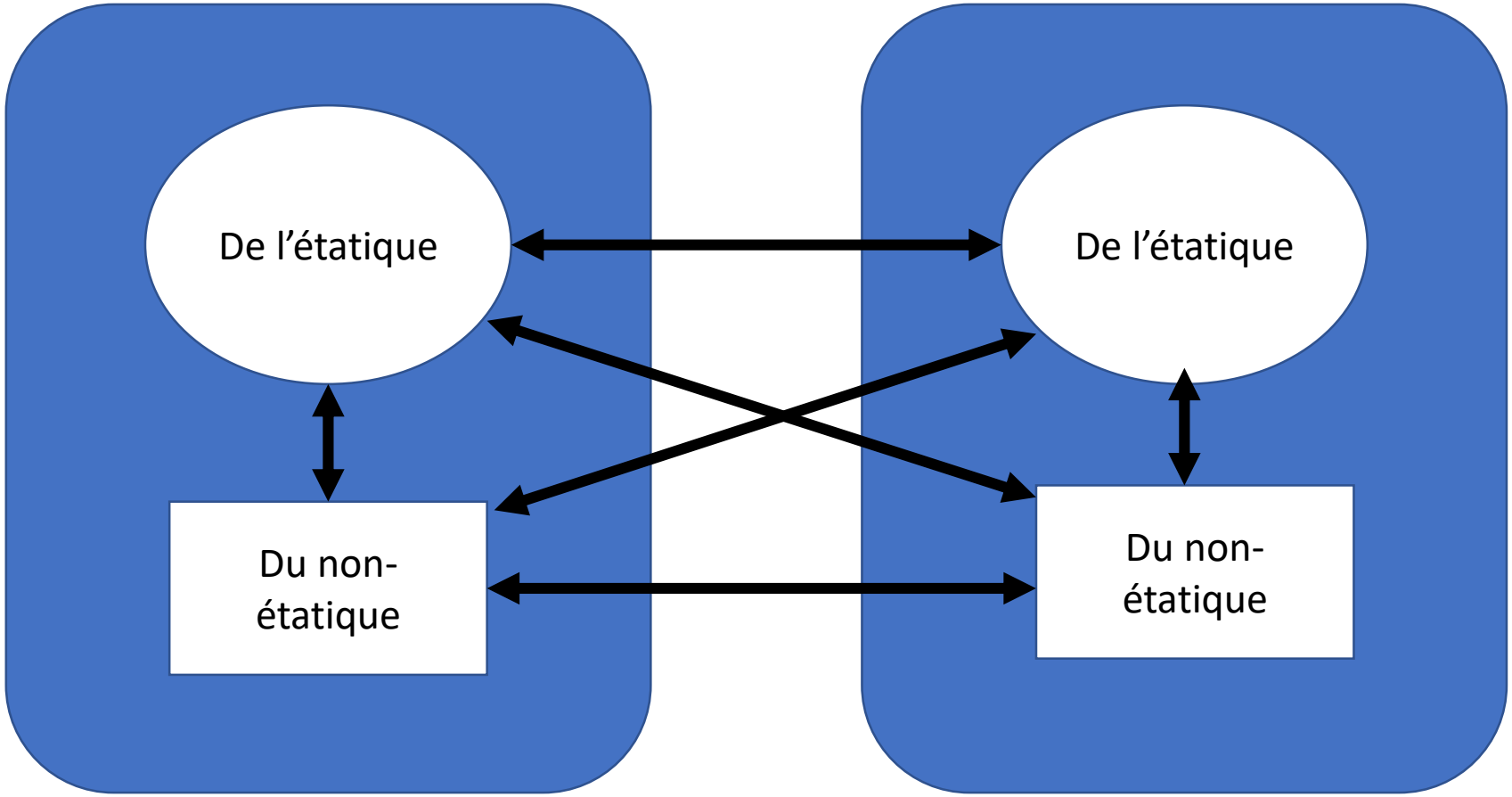
- On a du point de vue des RI quantité de sujets pertinents autour des APTs (souveraineté, droit, conflictualité, acteurs de cybersécurité versus constructeurs de la cybermenace …) **= que font les APTs aux RI, ou que révèlent les APTs du fonctionnement du SI ?**

- Mais j'en retiendrai deux:

1) Le lien Etat - crime



2) Travailler autour de la distinction entre étatique et non-étatique, dans un contexte RI. Avec simplement deux espaces nationaux, et ces deux grandes catégories, on a 6 configurations en binômes possibles. Et bien plus si on divise l'étatique et le non-étatique en leurs n potentielles composantes.



Pour cela il faut enrichir les bases existantes avec des données nouvelles