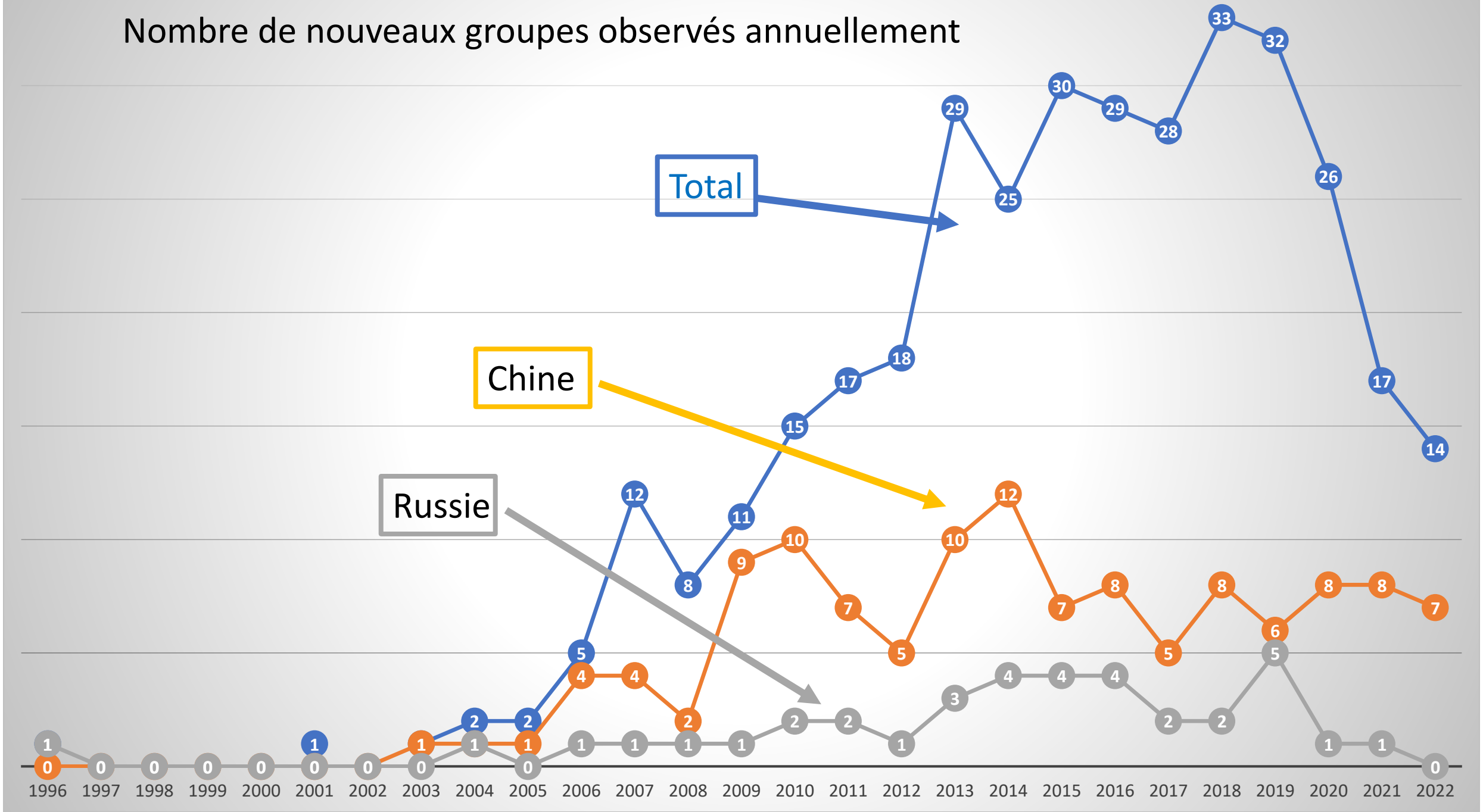
Les APT. Essai d'interprétation géopolitique

Daniel Ventre, CNRS, Laboratoire CESDIP (UMR 8183)

Colloque AMUSEC

Luminy, 26 Mai 2023


Nombre de nouveaux groupes observés annuellement
Total
Chine
Russie
1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022
1 0 0 0 0 0 1 0 0 1 1 0 1 1 2 2 5 12 8 11 15 17 18 29 25 30 29 28 33 32 26 17 14
0 0 0 0 0 0 0 1 1 1 4 4 2 9 10 7 5 10 12 7 8 5 8 6 8 8 7
1 0 0 0 0 0 0 0 1 0 1 1 1 1 2 2 1 3 4 4 4 2 2 5 1 1 0

Quelques écueils pour le chercheur SHS

Y voir clair dans la nébuleuse

APT 1, aka…

- Operation Siesta
- Group 3
- Shanghai Group
- BrownFox
- Comment Panda
- Comment Group
- Operation Oceansalt
- Operation Seasalt
- PLA Unit 61398
- Comment Crew
- Byzantine Candor
- ShadyRAT
- Byzantine Hades
- TG-8223
- Brown Fox
- GIF89a

APT 10, aka…

- APT 10 (by Mandiant)
- Chinese Chess
- Red Apollo
- Stone Panda (by Crowdstrike)
- POTASSIUM (by Microsoft)
- MenuPass (by Fireeye)
- Menupass Team, menuPass, menuPass Team
- Happyyongzi
- DustStorm
- CVNX
- HOGFISH
- Cloud Hopper
- BRONZE RIVERSIDE

APT 17, aka…

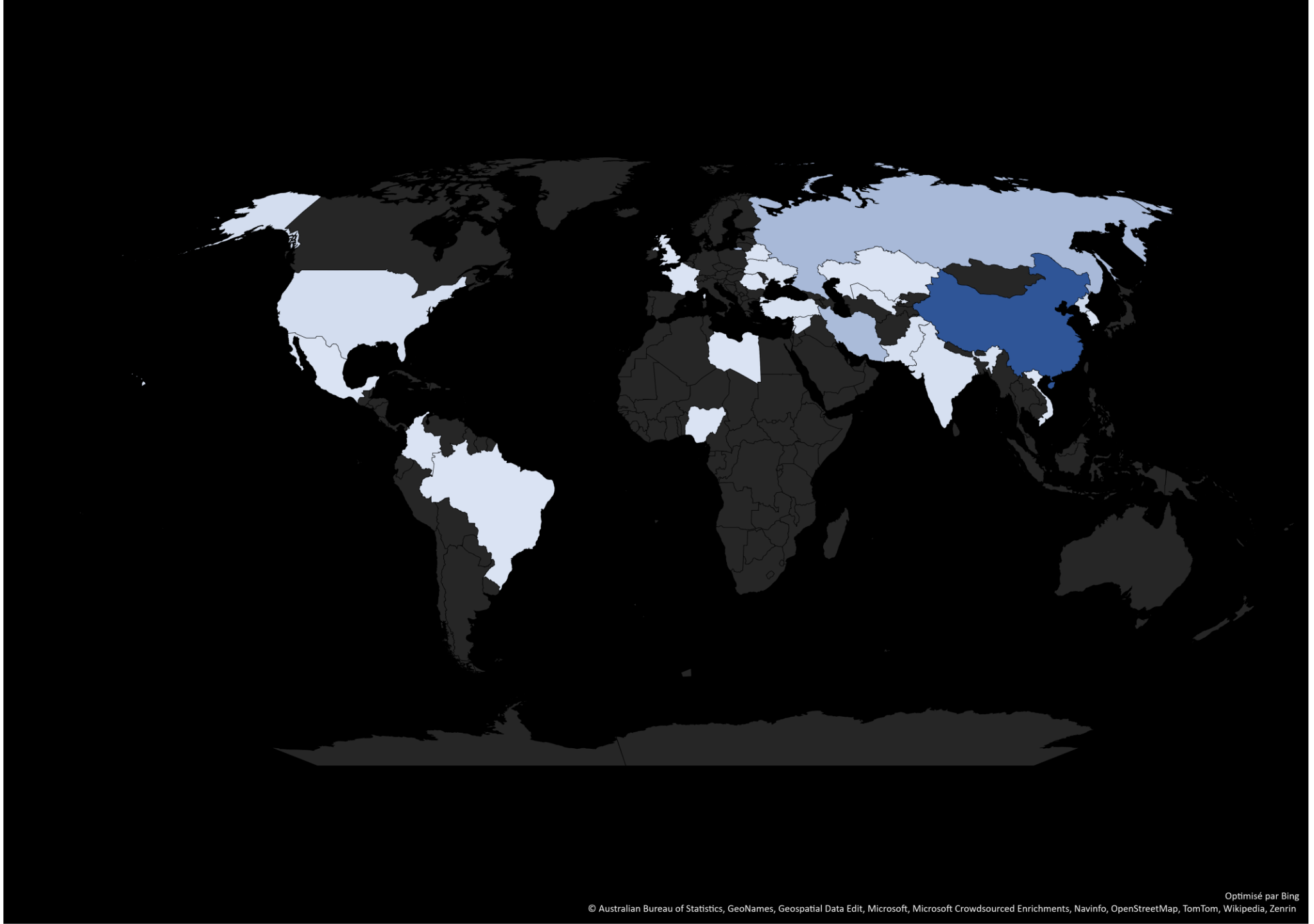
- APT 17 (Mandiant)
- Tailgater Team (Symantec)
- Elderwood (Symantec)
- Elderwood Gang (Symantec)
- Sneaky Panda (CrowdStrike)
- SIG22 (NSA)
- Beijing Group (SecureWorks)
- Bronze Keystone (SecureWorks)
- TG-8153 (SecureWorks)
- TEMP.Avengers (FireEye)
- Dogfish (iDefense)
- Deputy Dog (iDefense)
- ATK 2 (Thales)

Groupes mais aussi sous-groupes

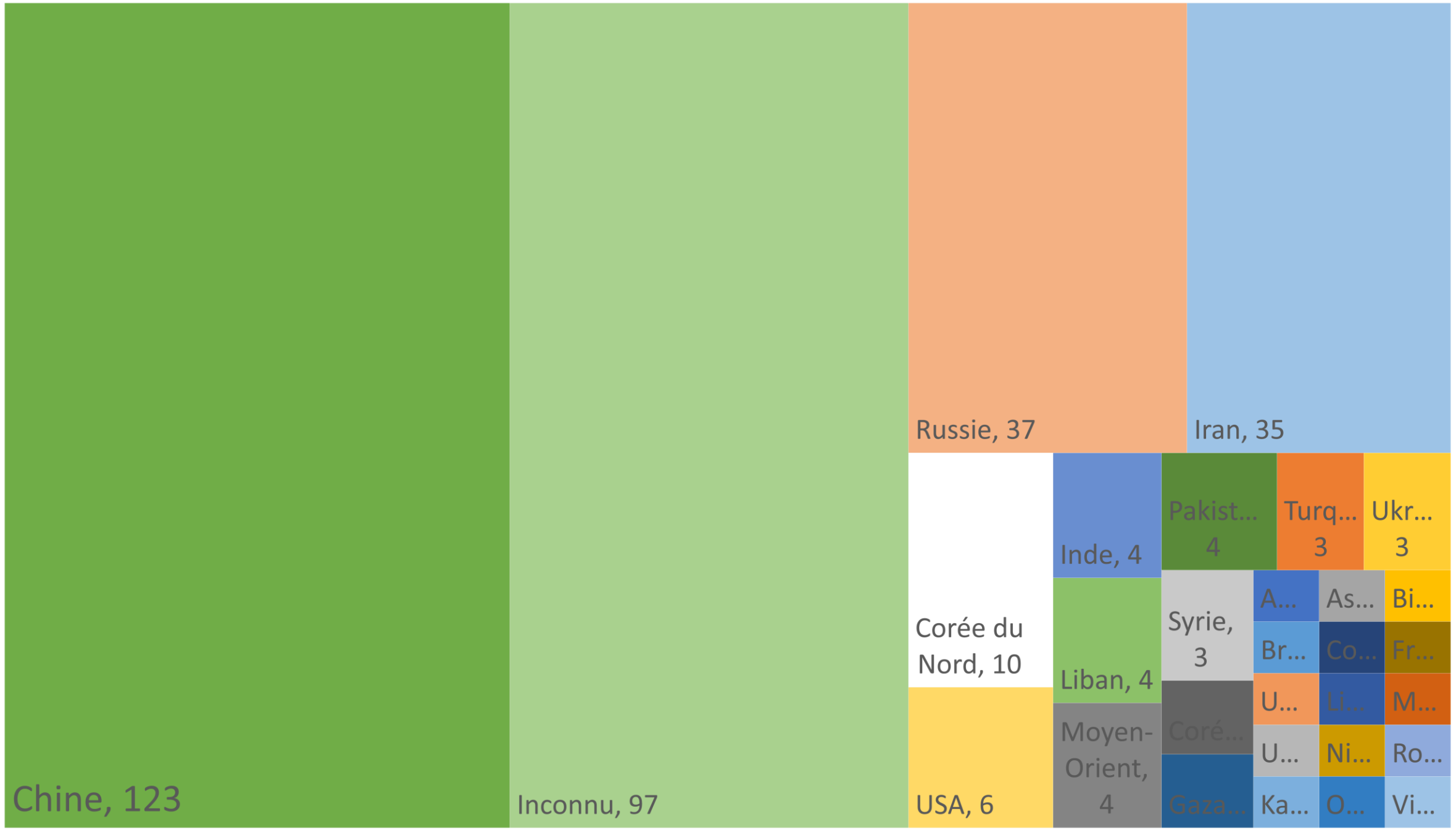
- Andariel, sous-groupe de Lazarus (Corée du nord)
- Earth Longzhi, Earth Baku, Grayfly, Blackfly sont des sous-groupes de l’APT41 (Chine)
- Etc.

Dimension spatiale

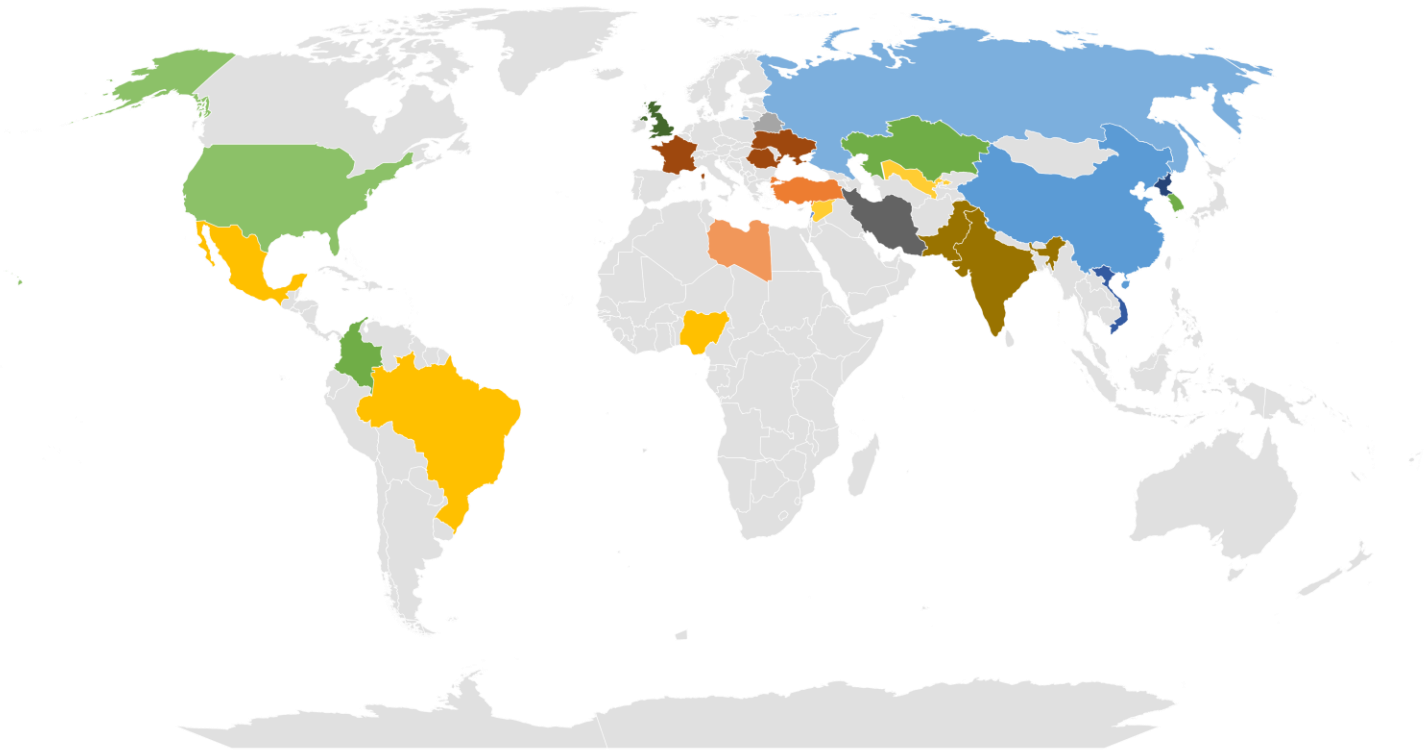
D’où attaquent les APT?


Optimisé par Bing
© Australian Bureau of Statistics, GeoNames, Geospatial Data Edit, Microsoft, Microsoft Crowdsourced Enrichments, Navinfo, OpenStreetMap, TomTom, Wikipedia, Zenrin

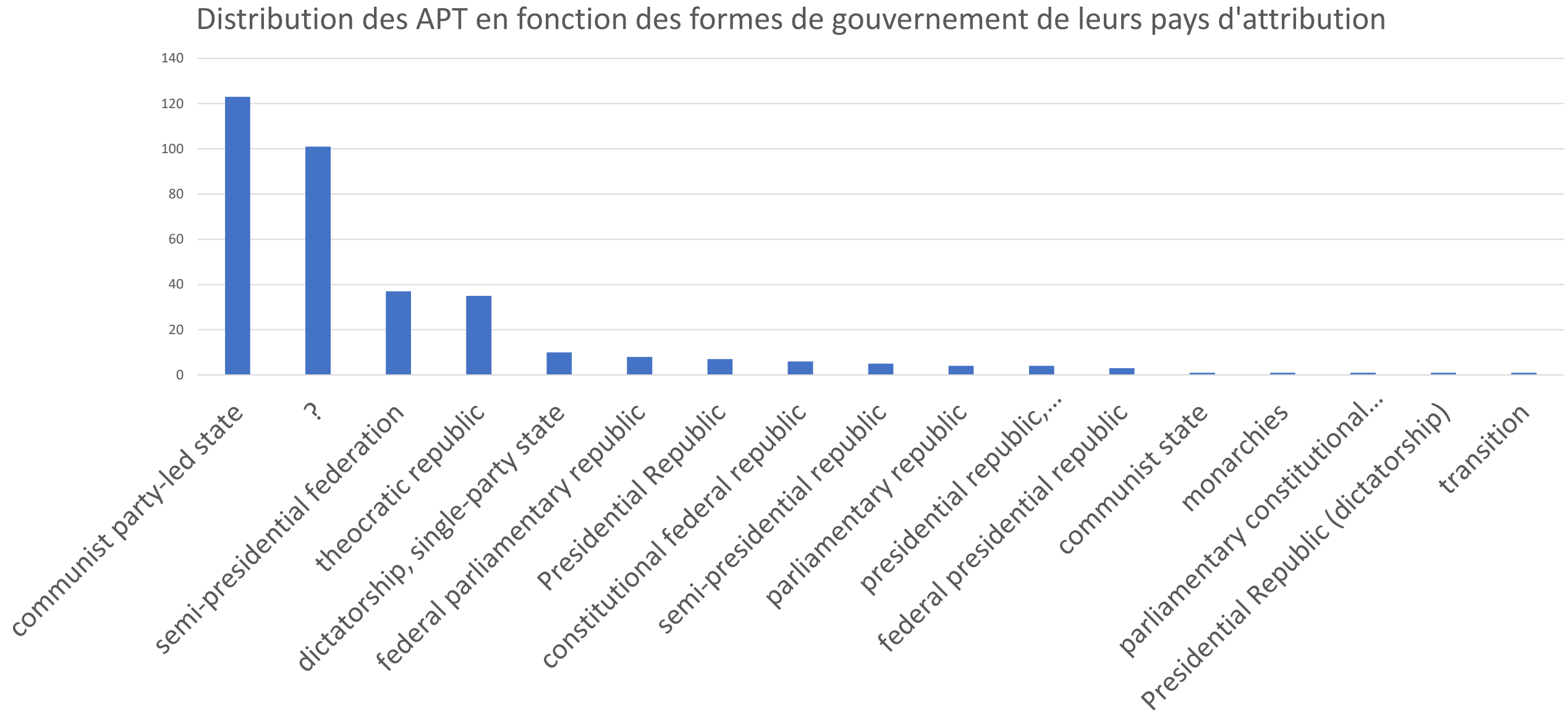
Nombre de groupes APT identifiés et leurs pays d'attribution, sur la période 1996-2023



Type de gouvernement des Etats où sont présentes les APT



- ?
- Presidential Republic
- Presidential Republic (dictatorship)
- federal presidential republic
- communist party-led state
- presidential republic
- dictatorship, single-party state
- semi-presidential republic
- theocratic republic
- federal parliamentary republic
- monarchies
- parliamentary constitutional monarchy
- parliamentary republic
- transition
-
- presidential republic, authoritarism
- semi-presidential federation
- constitutional federal republic
- communist state



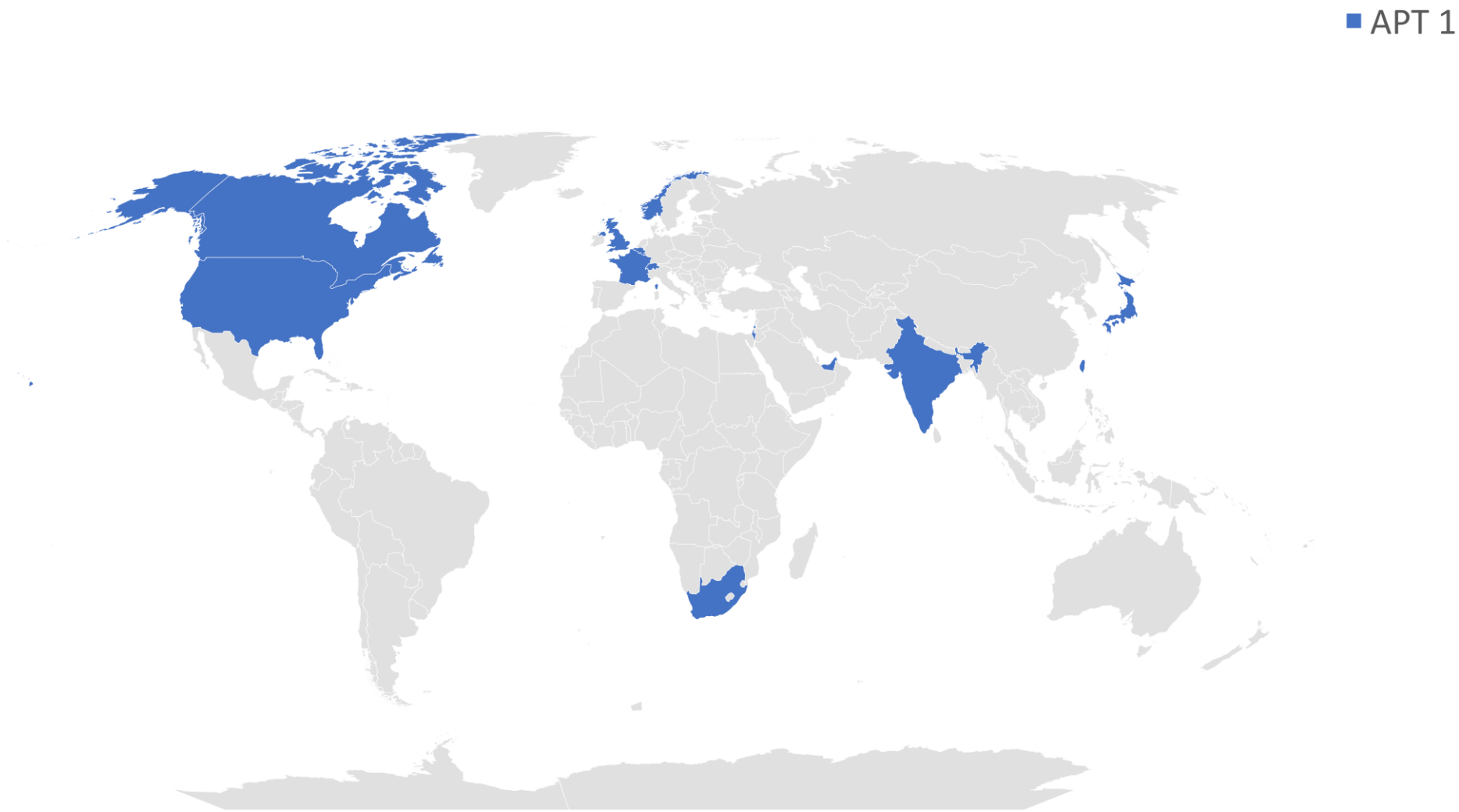
Nomenclature CIA

Où frappent-elles (leur surface d’attaque)?

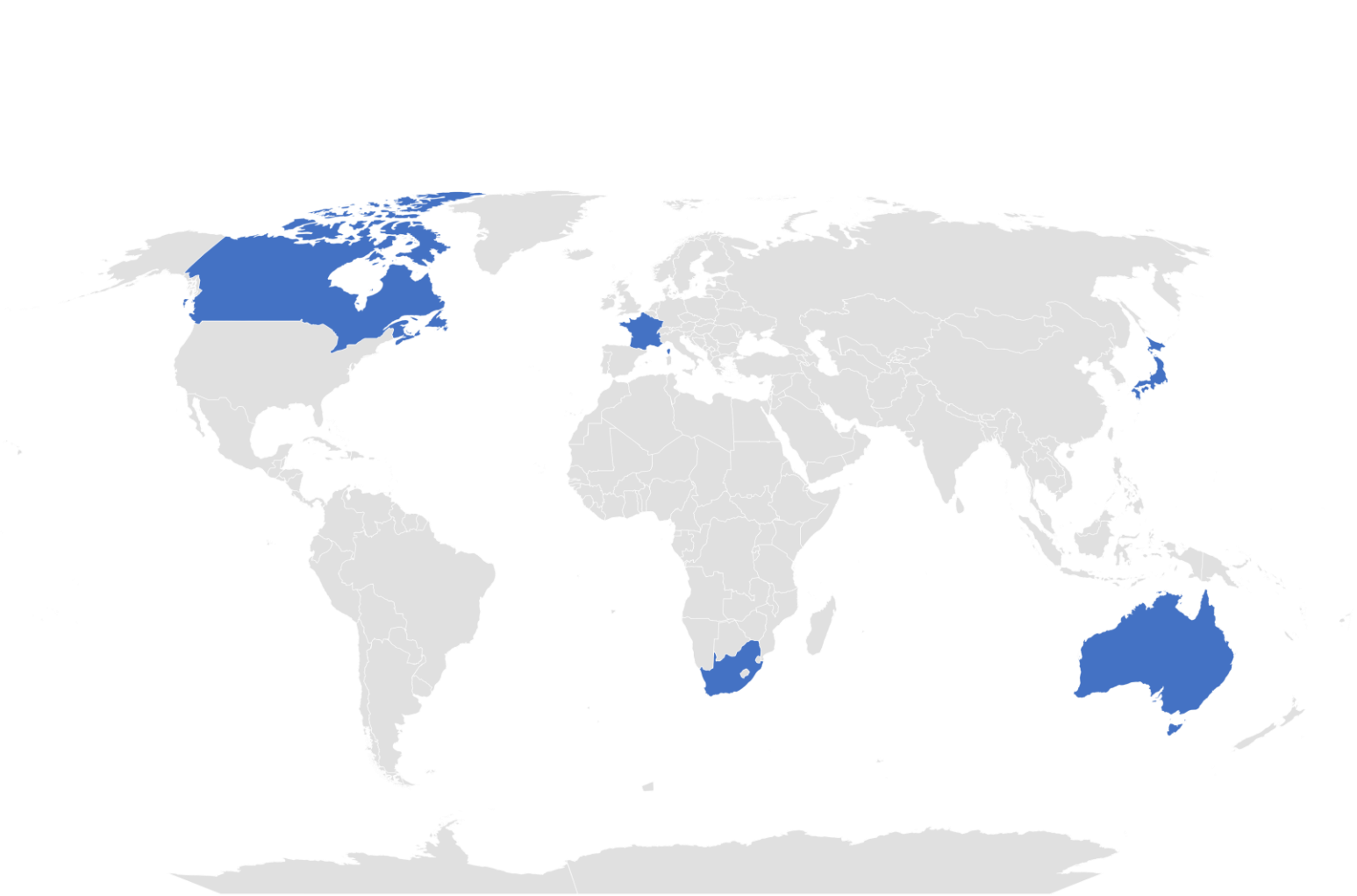
→ cartographies réalisées à partir des données publiées sur divers sites (Electronic Transactions Development Agency, MITRE, etc.

A chaque APT sa surface d’attaque?

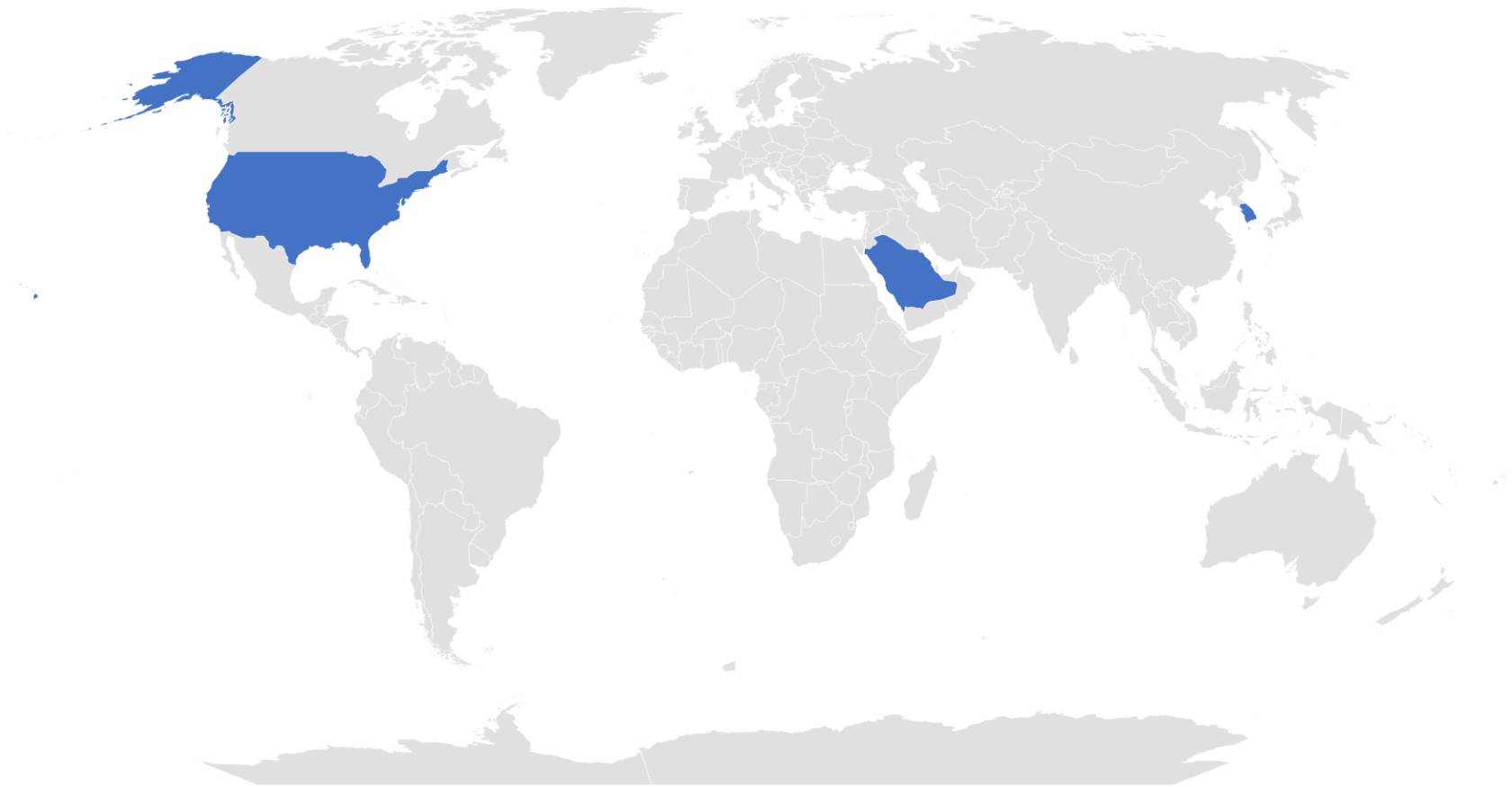
Surface d’attaque d'APT1 (Chine?)



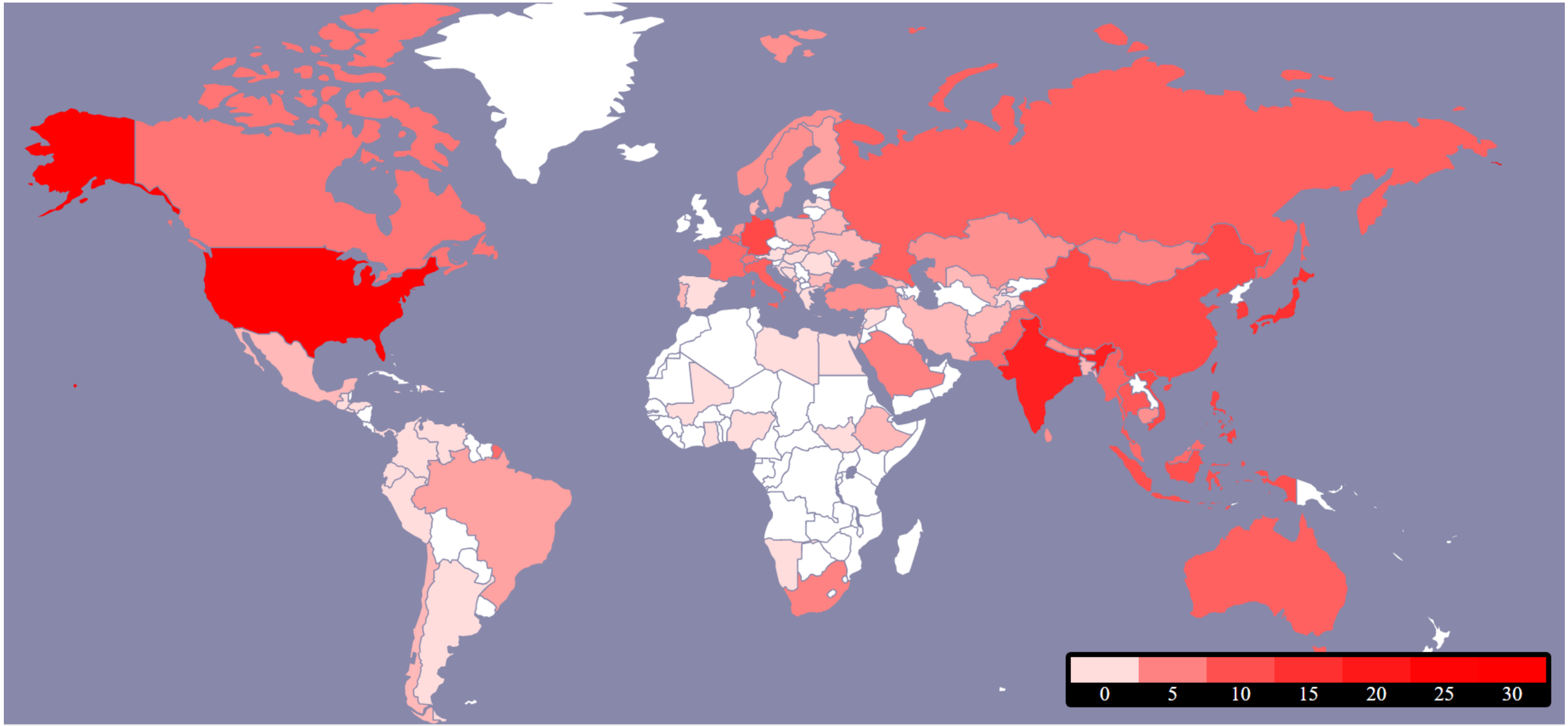
Surface d’attaque d'APT 10 (Chine?)



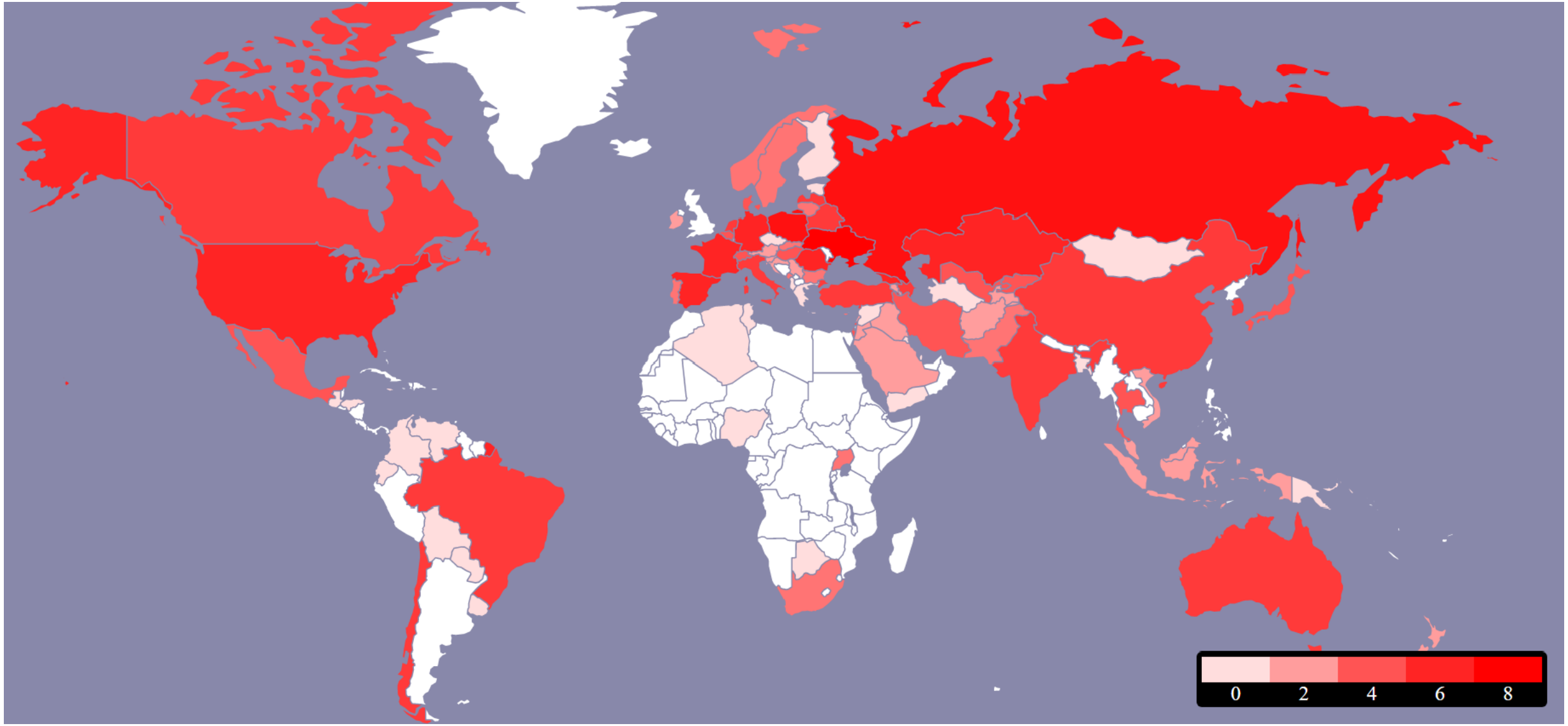
Surface d’attaque d'APT 33 (Iran?)



Surface d’attaque des APT étatiques chinoises ?

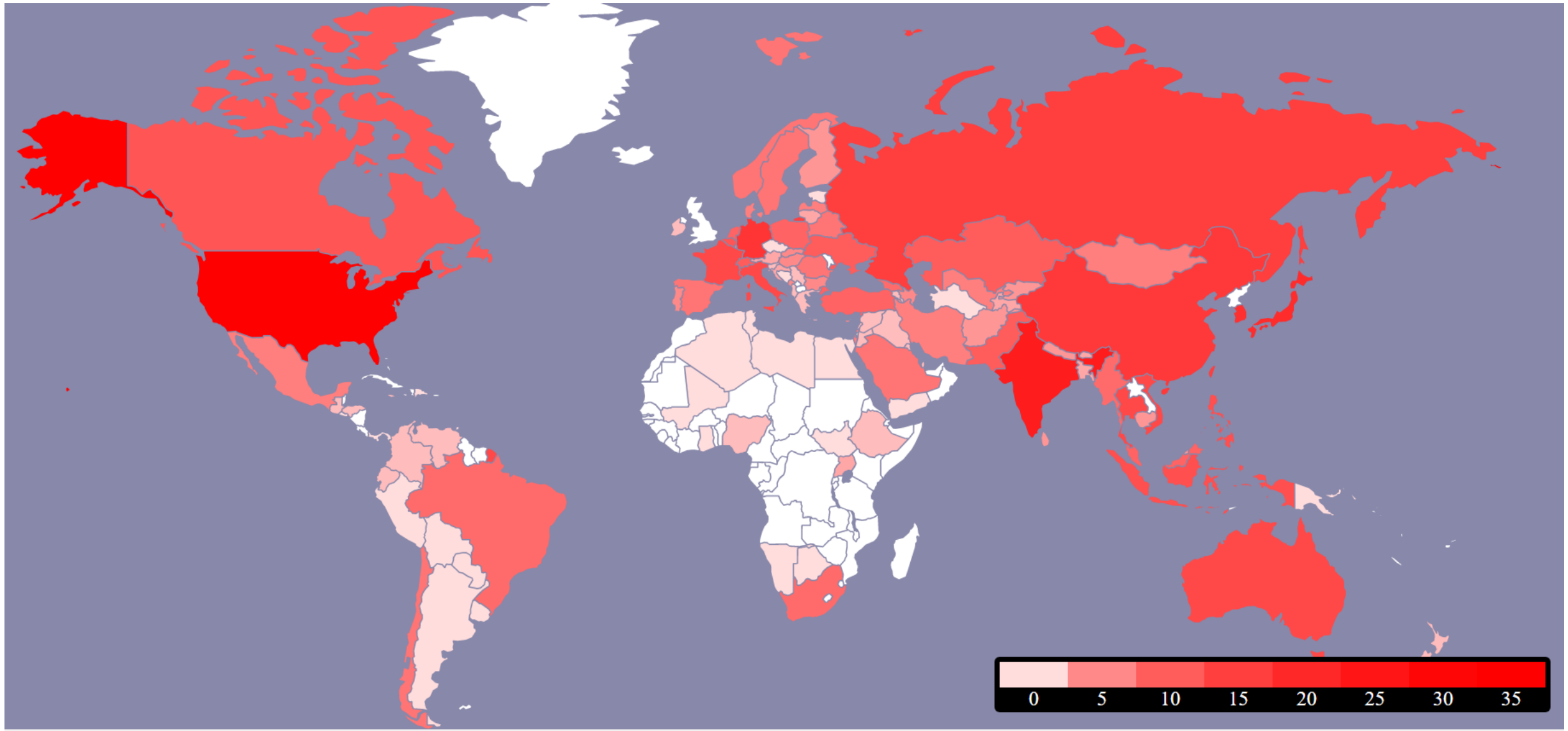

0
5
10
15
20
25
30

Surface d’attaque des APT étatiques russes ?


0
2
4
6
8

Surface d’attaque des APT étatiques russes + chinoises ?

Interpréter la carte ci-après en termes géopolitiques


0
5
10
15
20
25
30
35

Une dimension régionale des attaques?

D'où émanent les attaques APT touchant le Japon? (origine des APT attaquant le Japon)