MapKIT—Mapping Key Internet Terrain

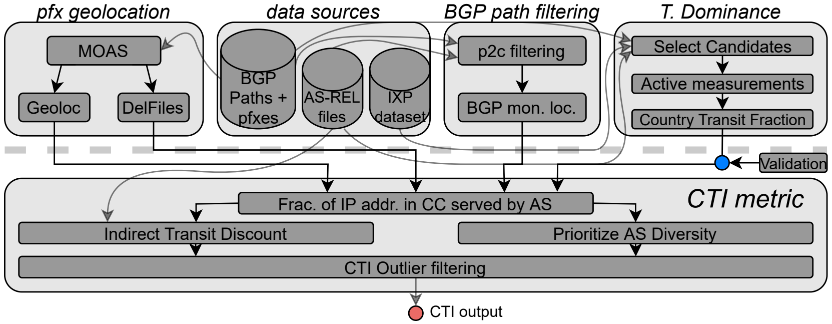
Challenge:

- Hackers, terrorists or nation states, can disrupt, intercept or manipulate the Internet traffic of entire countries or regions by targeting structural weaknesses of the Internet topology.
- Goal: Identify strategic points in the macroscopic Internet topology constitute ***key terrain in the cyberspace*** battlefield.
- Collecting and interpreting data about the Internet connectivity of a country is challenging.

Solution:

- Through a novel multi-layer mapping effort, we aim at identifying important components of the Internet topology of a country/region— Autonomous Systems (ASes), Internet Exchange Points (IXPs), PoPs, colocation facilities, and physical cable systems which represent the "key terrain" in cyberspace.

NSF CNS-1705024 and CNS-1703592
PIs: Alberto Dainotti, Paul Barford
mapkit.cc.gatech.edu
dainotti@gatech.edu



pfx geolocation: MOAS, Geoloc, DelFiles

data sources: BGP Paths + pfxes, AS-REL files, IXP dataset

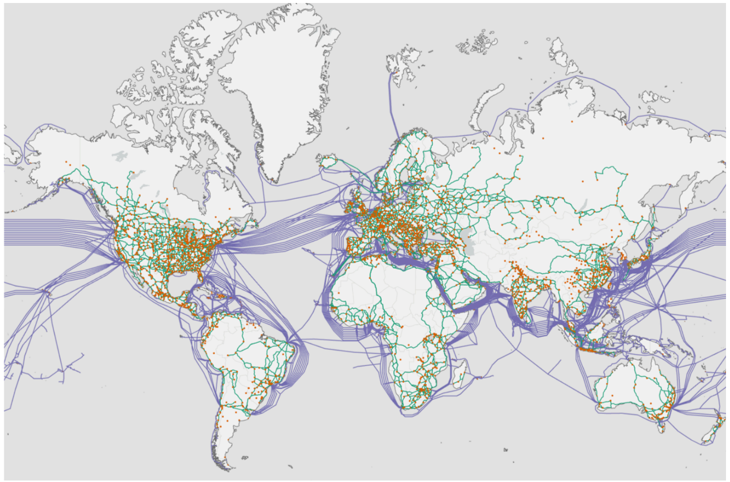
BGP path filtering: p2c filtering, BGP mon. loc.

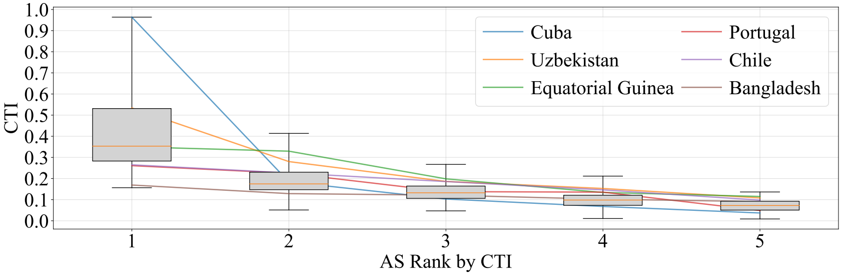
T. Dominance: Select Candidates, Active measurements, Country Transit Fraction

Validation

CTI metric: Frac. of IP addr. in CC served by AS, Indirect Transit Discount, Prioritize AS Diversity, CTI Outlier filtering

CTI output





Scientific Impact:

Contribute to a better understanding and modeling of key weakness of the Internet infrastructure in countries that expose them to targeted attacks by state actors and organized groups

Data and models also relevant to resiliency of critical infrastructure (e.g., preparedness to natural disasters)

Provide input for political scientists and international relations researchers to reason about "opportunity and willingness" to engage into large-scale cyber conflict

Broader Impact and Broader Participation:

- The Internet is a critical infrastructure on which all other critical infrastructures depend: safety and prosperity of our society as well as international relations depend on cybersecurity. Yet the exposure of a country's Internet macroscopic infrastructure to targeted attacks with potential massive impact is unclear. This project tries to bridge this crucial gap.