

# DHS Science and Technology Directorate

## Center for Applied Internet Data Analysis (CAIDA)

### Cartographic Capabilities for Critical Cyberinfrastructure

#### Global Cybersecurity challenges

Today the “cyber threat” is one of the most serious economic and national security challenges we face as a nation. As the Internet has become an indispensable resource and a norm of everyday life for millions of people, America’s economic prosperity in the 21<sup>st</sup> century crucially depends upon Cybersecurity. Yet thorough understanding of the structure, dynamics, and vulnerabilities of the global Internet is lacking. Versatile measurement infrastructures, reliable, representative, high quality Internet data sets, and advanced analysis tools are scarce and rarely available to researchers and developers.

#### Cartographic Capabilities for Critical Cyberinfrastructure

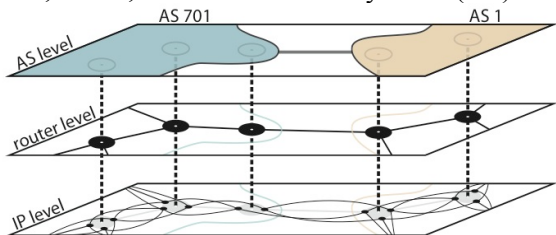
This project integrates strategic Internet measurement and data analysis capabilities to deliver annotated Internet topology maps that advance our ability to identify, monitor, and model critical cyber infrastructure.

#### Dedicated measurement infrastructure

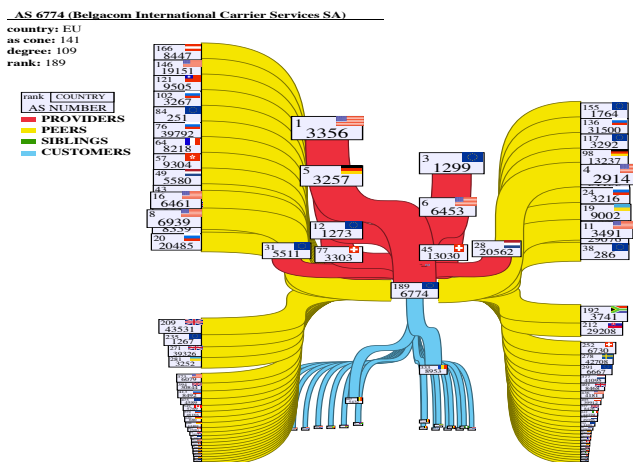
CAIDA designed and deployed a measurement architecture Archipelago (Ark) for conducting ongoing and on-demand Internet measurements. Ark monitors (120 and growing) are distributed all over the world.



The monitors collect connectivity and latency data for a wide cross-section of the commodity Internet. We use these data to derive maps of the Internet at various granularity levels: IP, router, and Autonomous Systems (AS).



#### Increased completeness, accuracy, and richness of topology maps



CAIDA researchers are developing new techniques to collect, analyze, and process Internet measurement data. Our flagship product is the Internet Topology Data Kits (ITDK), regularly produced and distributed to network and security researchers and analysts. ITDKs contain richly annotated topology maps of the observable Internet at multiple granularity levels, providing a more detailed and validated topological view than has been previously available.

This project has also delivered techniques for more accurate geolocation of IP addresses, detecting anomalies in traceroute data, inference of business relationships and ranking of Internet Service Providers (ISP), novel visualizations of Internet topology, and IPv6 topology maps.

#### Improved security and situational awareness

Results of this project enable empirical research of critical cyberinfrastructure and deepen our insight into the structure, behavior, and evolution of the global Internet. CAIDA researchers continue to increase the number of Ark vantage points (global monitors), refine measurement methods, and improve analysis and inference algorithms.

#### Performers, partners, and stakeholders

All data curation, processing and analysis activities are conducted at the University of California, San Diego. We rely on volunteer individuals and organizations hosting our Ark monitors at multiple locations around the globe. We manage hundreds of accounts for commercial, government (DHS, DoD, FCC, NSA), and academic network and security researchers who download our datasets.



**Homeland Security**

Science and Technology

To learn more about Internet Measurement and Attack Modeling (IMAM), contact Ann Cox, Program Manager, at [Ann.Cox@hq.dhs.gov](mailto:Ann.Cox@hq.dhs.gov).