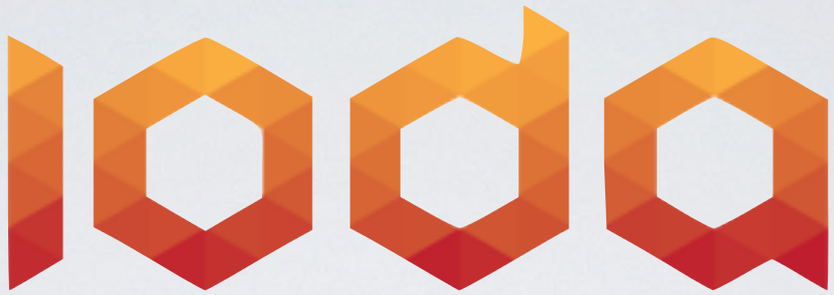
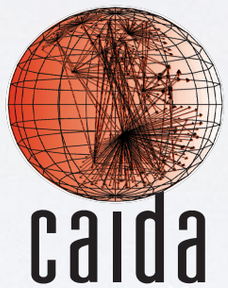


Internet Outage Detection & Analysis

http://www.caida.org/projects/ioda

Alberto Dainotti
alberto@caida.org



Center for Applied Internet Data Analysis
University of California, San Diego

FOCUS

Macroscopic Internet Outages

- Large-scale Internet connectivity disruption
  (*keywords: Internet "outage", "black out", "shutdown", "kill-switch"*)

- *E.g., a connectivity black-out significantly affecting a large network operator or a large geographical area*

- Potential causes: *natural disasters, cyber attacks, physical attacks (terrorism, war, …), bugs and misconfigurations, government orders, …*

INTERNET OUTAGES

why so relevant?

Public Safety

The Internet is a critical infrastructure

Virtually every element of modern life is now dependent on cyber infrastructure. As a result, our Nation's economic and national security relies on the security of the assets and operations of critical communications infrastructure. Past terrorist attacks and catastrophic natural disasters emphasized the need to focus our national attention on protecting the Nation's critical infrastructure and making it more resilient. Moving forward, it is

While the Communications Sector has few significant dependencies, other critical infrastructure sectors are dependent on the Communications Sector. As such, the Communications Sector is one of the few sectors that can affect all other sectors. At a minimum, each sector depends on services from the Communications Sector to support its operations and associated day-to-day communication needs for corporate and organizational networks and services (e.g., Internet connectivity, voice services, and video teleconferencing capabilities). Some sectors

US Department of Homeland Security,
National Infrastructure Protection Plan (NIPP) 2013

INTERNET OUTAGES

why so relevant?

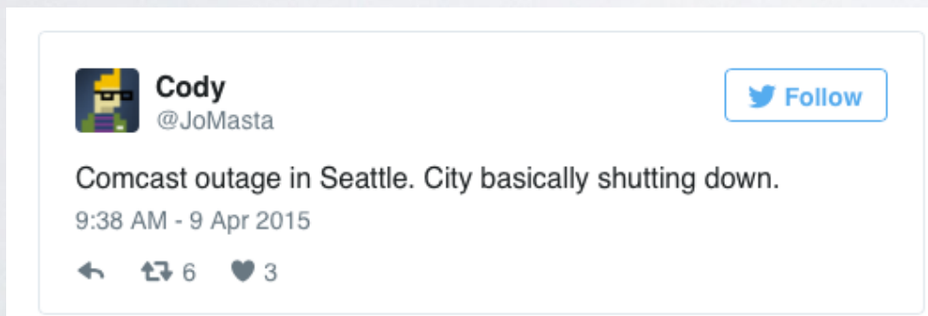
Financial and reputational costs

Services are meant to be always on

CLOUD

5-minute outage costs Google $545,000 in revenue

DYLAN TWENEY @DYLAN20 AUGUST 16, 2013 4:06 PM



How Much Will Today's Internet Outage Cost?

Some companies lose tens of thousands of dollars for every *minute* of a DDoS attack.

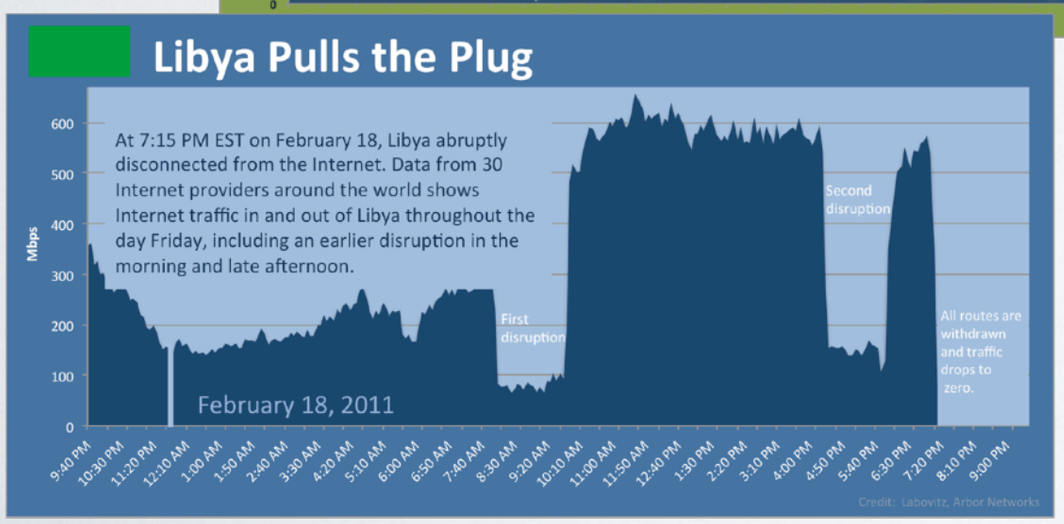
ADRIENNE LAFRANCE | OCT 21, 2016 | TECHNOLOGY

INTERNET OUTAGES

why so relevant?

Human Rights

censorship and political violence



HOME » NEWS » WORLD NEWS » AFRICA AND INDIAN OCEAN » EGYPT

How Egypt shut down the internet

Virtually all internet access in Egypt is cut off today as the go to contain the street protests that threaten to topple Presider Mubarak.

2K 0 0 2K Email

Police fire tear gas towards protesters in Suez, Egypt Photo: AFP/GETTY

INTERNET OUTAGES

why so relevant?

Human Rights

censorship and political violence

QUARTZ
Africa

#KEEPITON

More African governments blocked the internet to silence dissent in 2016

B | Center for Technology Innovation at BROOKINGS

OCTOBER 2016

Internet shutdowns cost countries $2.4 billion last year

INTERNET OUTAGES

So what's the problem?

There is lack of understanding of *when, how often, why, how* large Internet outages happen

There is lack of a general rigorous framework to obtain *empirical data* about - and to characterize - these events

IODA PROJECT

Bio Sketch

Started in Sep. 2012 with an NSF award from a program to *Transition to Practice* Cybersecurity research

Funding also provided by DHS S&T

- **Goal:** prototype an operational capability to monitor the Internet 24/7 to detect and analyze Internet blackouts affecting large networks / geographical areas

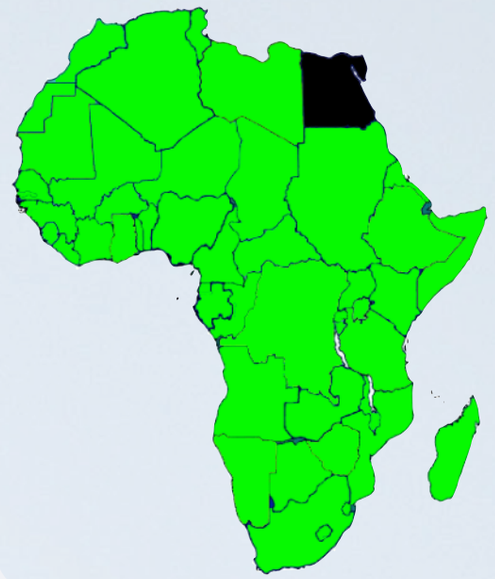
- **Project Website:** http://www.caida.org/projects/ioda
- **Experimental service**: *https://ioda.caida.org*

BEFORE IODA

methodologies used for post-event manual analysis

- Country-level Internet Blackouts during the Arab Spring

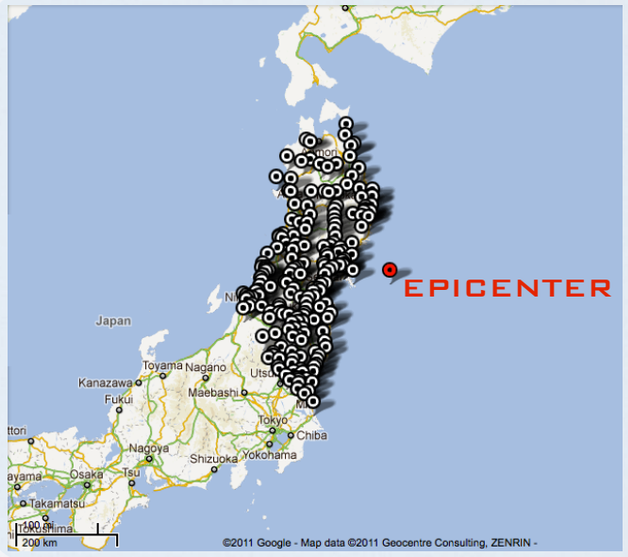
Dainotti et al. "Analysis of Country-wide Internet Outages Caused by Censorship" ACM Internet Measurement Conference 2011



Egypt, Jan 2011
Government orders to shut down the Internet

- Natural disasters affecting the infrastructure

Dainotti et al. "Extracting Benefit from Harm: Using Malware Pollution to Analyze the Impact of Political and Geophysical Events on the Internet" ACM SIGCOMM CCR 2012



Japan, Mar 2011
Earthquake of Magnitude 9.0

OUR METHODOLOGY

combining various types of measurements

- **multiple types of sources for inference**

  - Routing Plane [BGP]

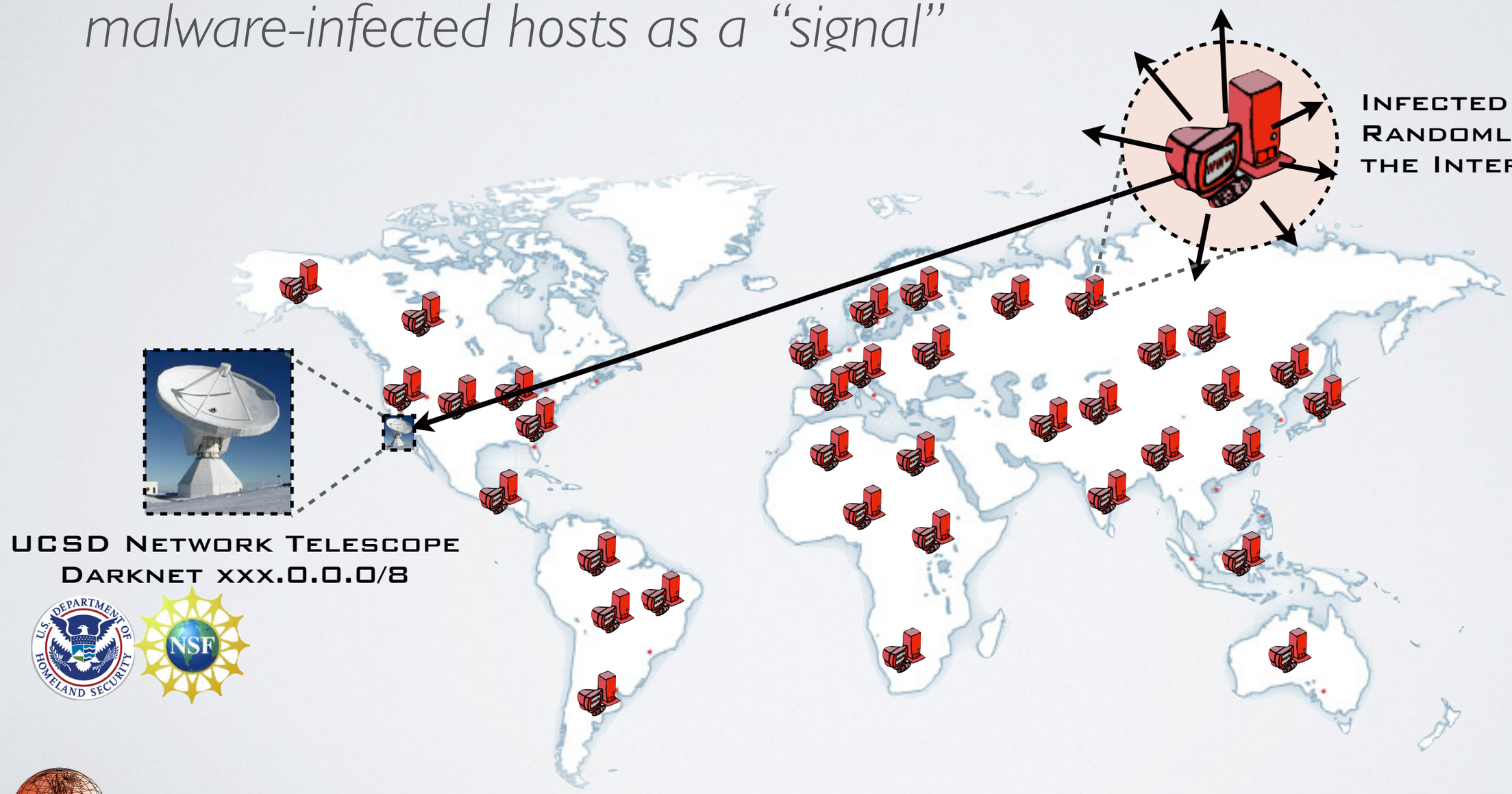
  - Data Plane
    - Active probing
    - Passive traffic analysis [IBR]

- **meta-data** to extract *liveness* signals for various aggregations *(e.g., countries, ASNs)*
- **visualize and compare signals**

IBR

"Extracting benefit from harm.."

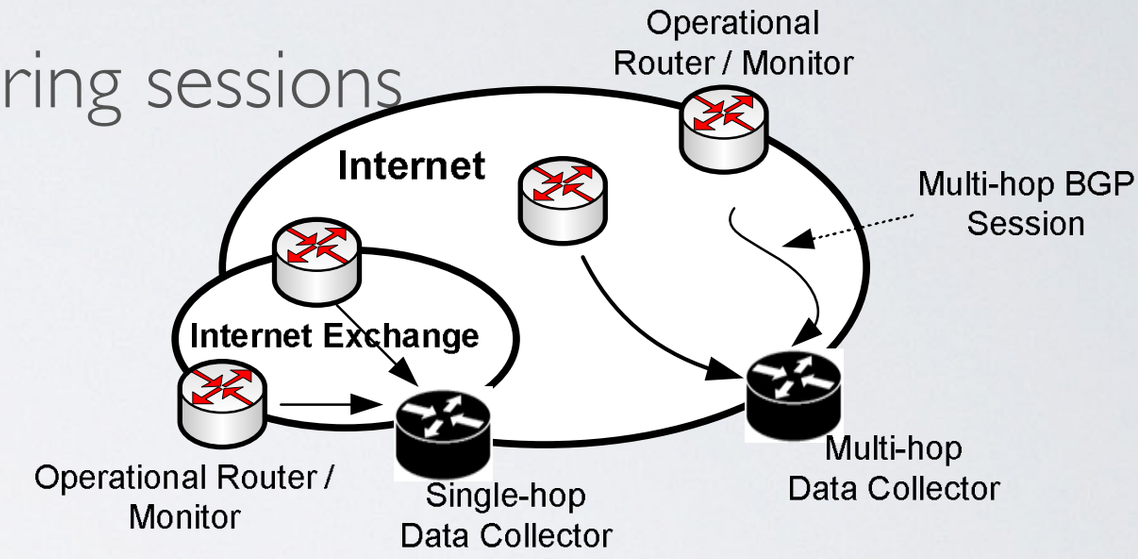
- Use *Internet Background Radiation (IBR), mostly generated by malware-infected hosts as a "signal"*



BGP

Monitoring Global Internet ***Routing***

- BGP measurement projects establish peering sessions with ASes to receive their routing tables (no exchange of other traffic)



- RouteViews (Univ. Oregon): *371 peers*
- RIPE RIS (RIPE NCC): *508 peers*

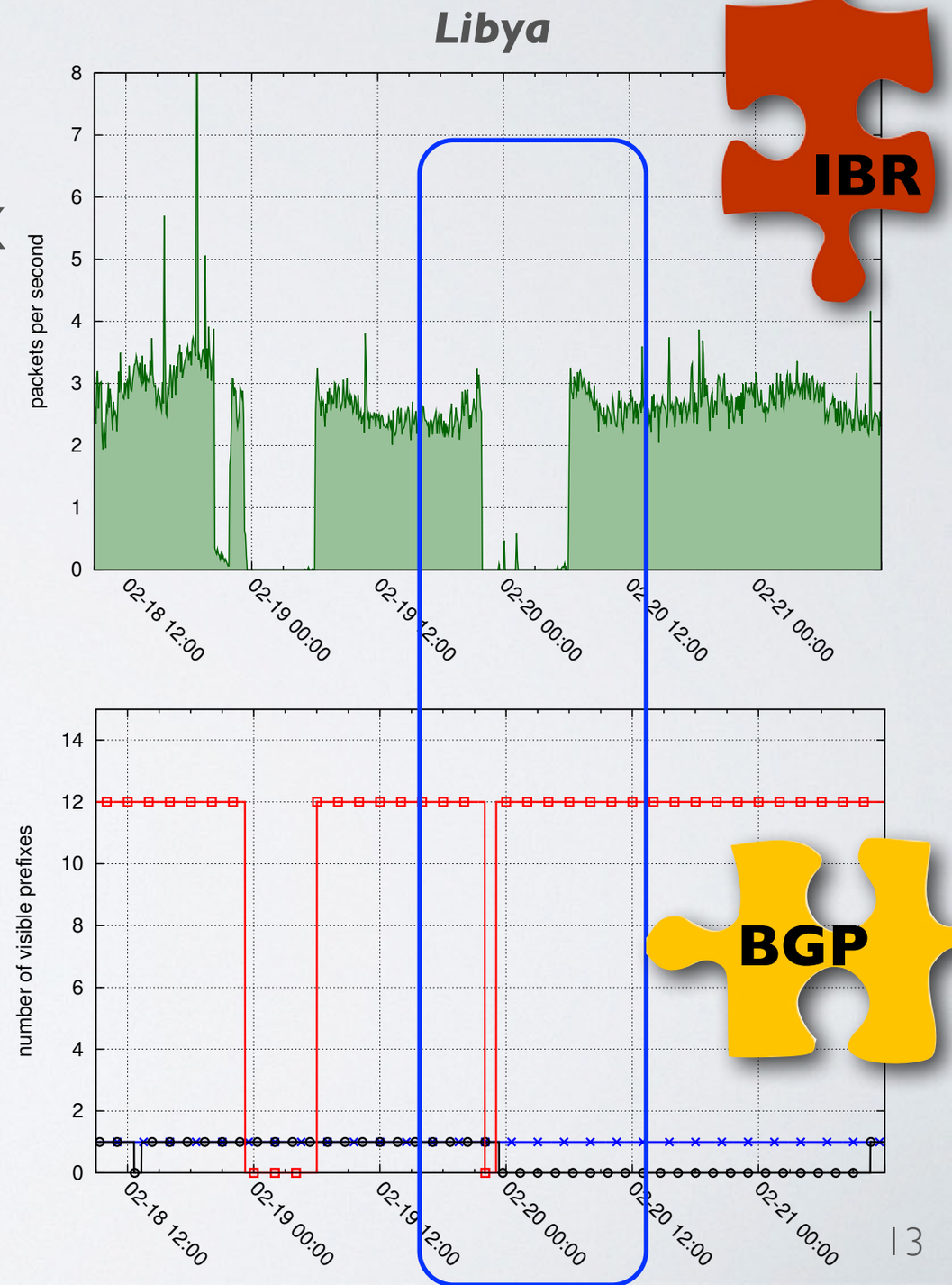
http://www.routeviews.org

https://www.ripe.net/data-tools/stats/ris

TELESCOPE + BGP

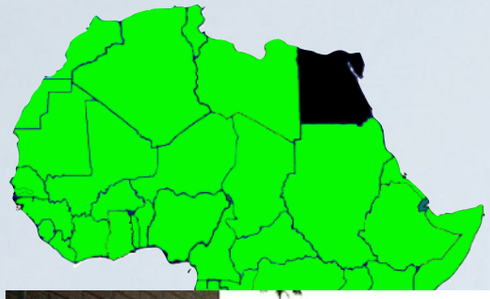
Complementarity

- Contrasting telescope traffic with BGP measurements **revealed a mix of blocking techniques** that was not publicized by others
- The second Libyan outage involved overlapping of ***BGP withdrawals*** and ***packet filtering***



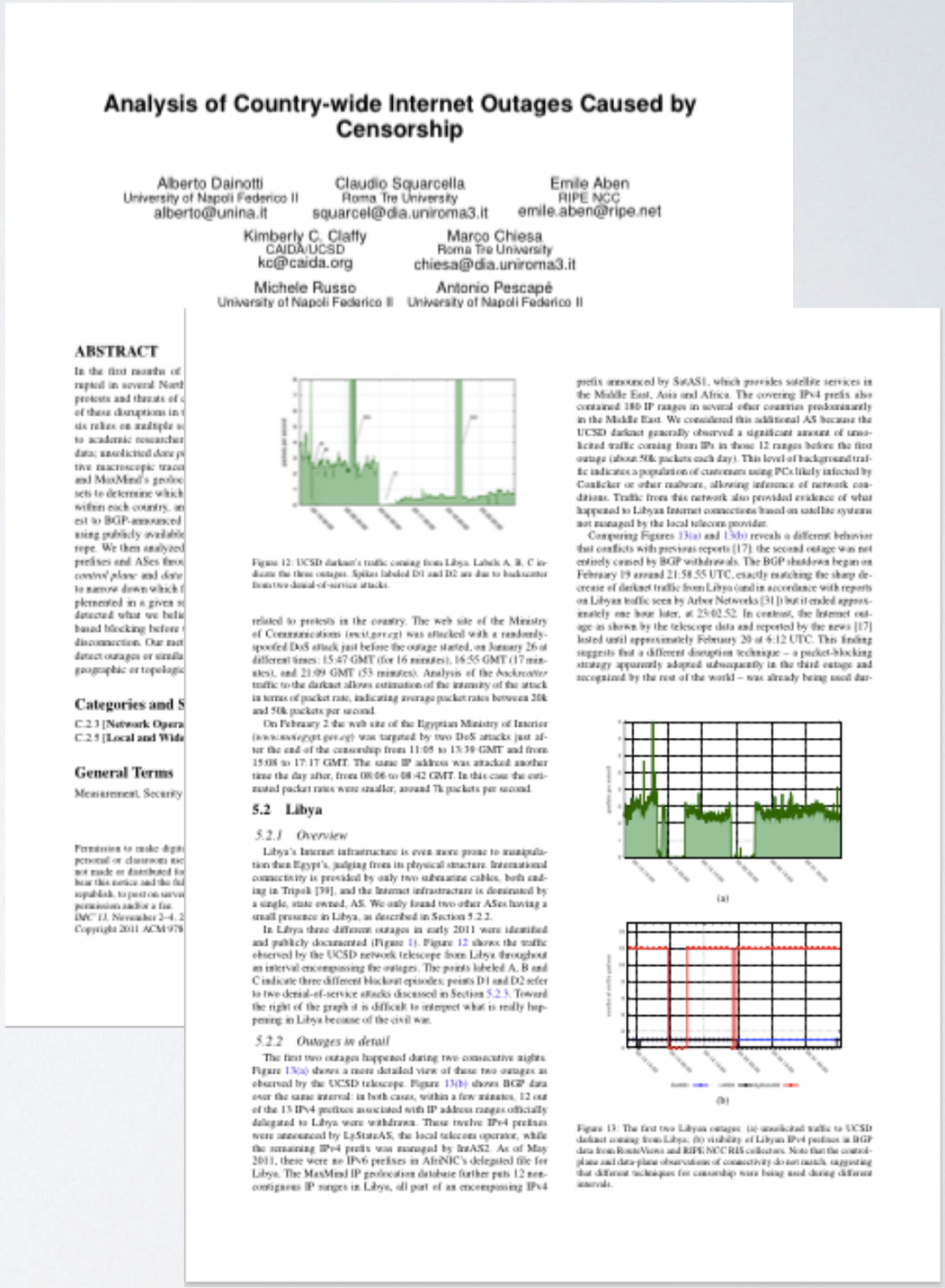
BEFORE IODA

post-event manual analysis



Egypt, Jan 2011
Government orders to shut down the Internet

4 months of work



Analysis of Country-wide Internet Outages Caused by Censorship

Alberto Dainotti, University of Napoli Federico II, alberto@unina.it
Claudio Squarcella, Roma Tre University, squarcel@dia.uniroma3.it
Emile Aben, RIPE NCC, emile.aben@ripe.net
Kimberly C. Claffy, CAIDA/UCSD, kc@caida.org
Marco Chiesa, Roma Tre University, chiesa@dia.uniroma3.it
Michele Russo, University of Napoli Federico II
Antonio Pescapé, University of Napoli Federico II

ABSTRACT

Dainotti et al. "Analysis of Country-wide Internet Outages Caused by Censorship" ACM Internet Measurement Conference 2011

Center for Applied Internet Data Analysis
University of California San Diego

IODA GOALS

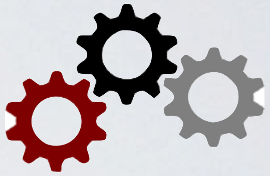
applied research

Analysis of Country-wide Internet Outages Caused by Censorship

Alberto Dainotti, University of Napoli Federico II, alberto@unina.it
Claudio Squarcella, Roma Tre University, squarcel@dia.uniroma3.it
Emile Aben, RIPE NCC, emile.aben@ripe.net
Kimberly C. Claffy, CAIDA/UCSD, kc@caida.org
Marco Chiesa, Roma Tre University, chiesa@dia.uniroma3.it
Michele Russo, University of Napoli Federico II, mic.russo83@gmail.com
Antonio Pescapé, University of Napoli Federico II, pescape@unina.it

ioda

manual analysis	→	automated
post-event	→	near-realtime detection
a couple of events	→	24/7 monitoring whole Internet
4 months of work	→	in few minutes



IODA CHALLENGES

Why this is a tough problem

- refine/extend inference methodologies
- automate inference methodologies
- complex data
- noisy data
- big data
- heterogeneous data
- velocity
- lack of tools
- distributed system
- visualization for dashboards and data exploration
- lots of infrastructure to maintain/operate
- ….
- all with relatively few money/people/time..

IODA CHALLENGES

Why this is a tough problem

- refine/extend inference methodologies
- automate inference methodologies
- complex data
- noisy data
- big data
- heterogeneous data
- velocity
- lack of tools
- distributed system
- visualization for dashboards and data exploration
- lots of infrastructure to maintain/operate
- ….
- all with relatively few money/people/time..

IODA CHALLENGES

Why this is a tough problem

- refine/extend inference methodologies
- automate inference methodologies
- complex data
- noisy data
- big data
- heterogeneous data
- velocity
- lack of tools
- distributed system
- visualization for dashboards and data exploration
- lots of infrastructure to maintain/operate
- ….
- all with relatively few money/people/time..

IODA CHALLENGES

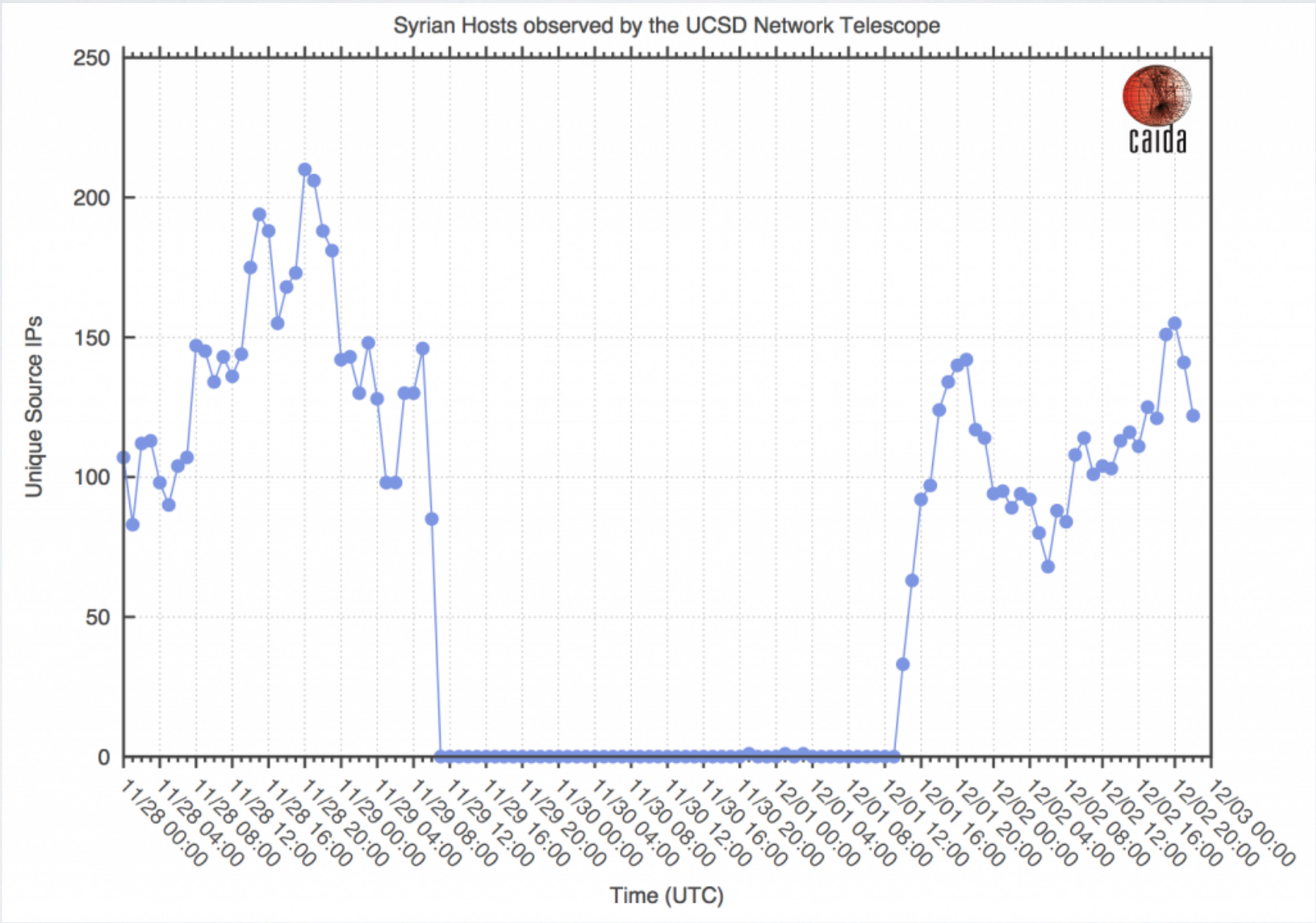
Why this is a tough problem

- refine/extend inference methodologies
- automate inference methodologies
- complex data
- noisy data
- big data
- heterogeneous data
- velocity
- lack of tools
- distributed system
- visualization for dashboards and data exploration
- lots of infrastructure to maintain/operate
- ….
- all with relatively few money/people/time..

IODA FIRST YEARS

documenting events on our blog

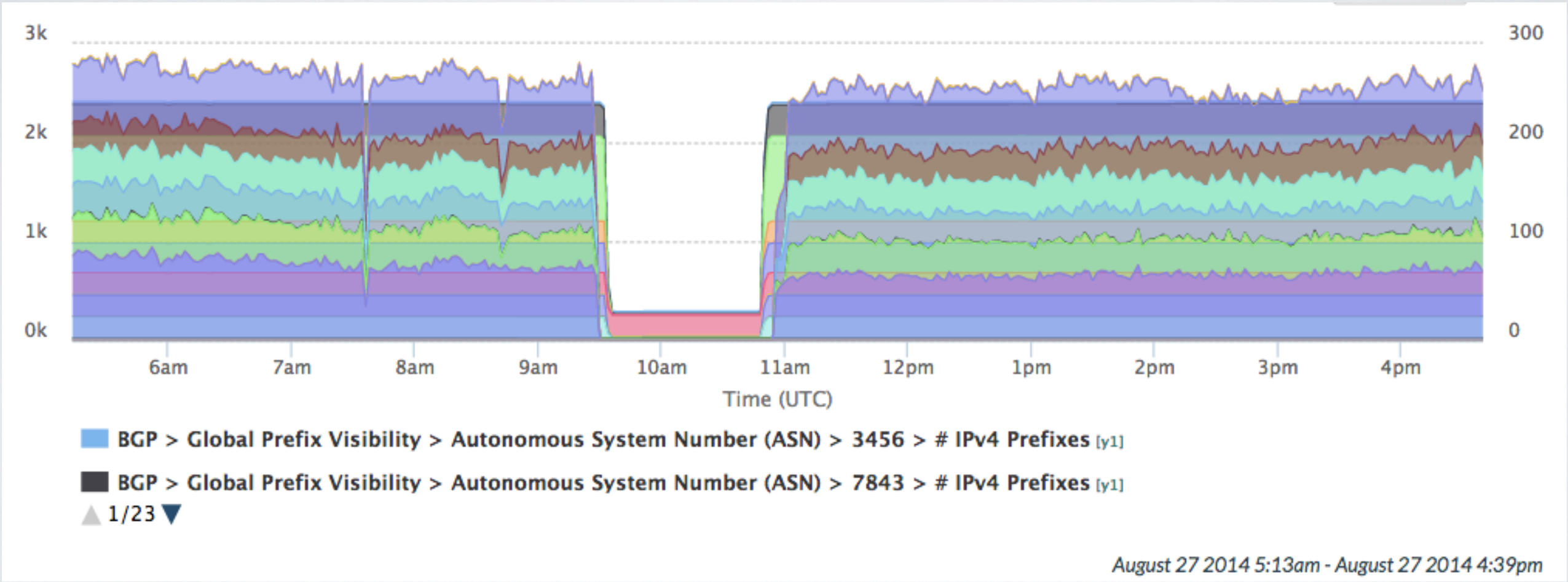
Syria disappears from the Internet — Nov 2012



IODA FIRST YEARS

documenting events on our blog

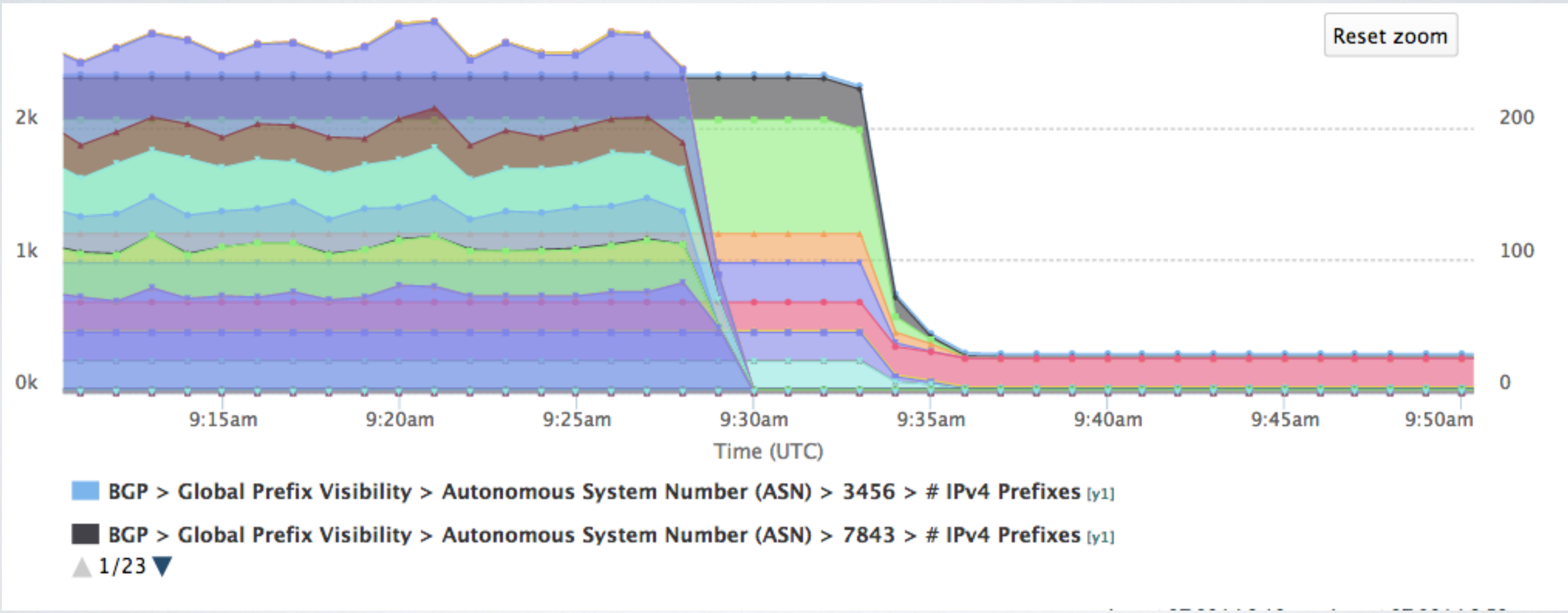
Time Warner Cable outage 27th August 2014



IODA FIRST YEARS

documenting events on our blog

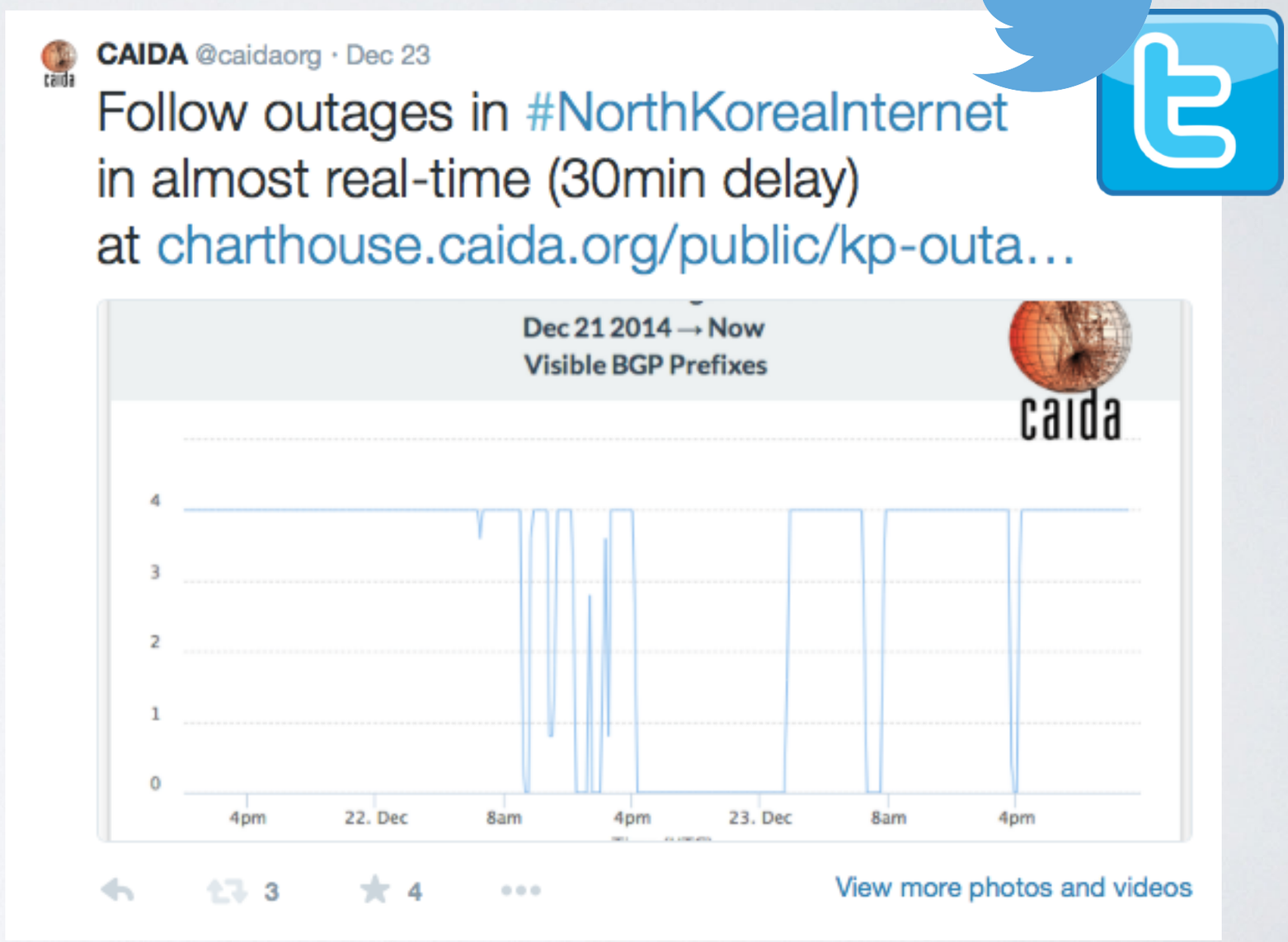
Time Warner Cable outage 27th August 2014



IODA AFTER 2 YEARS

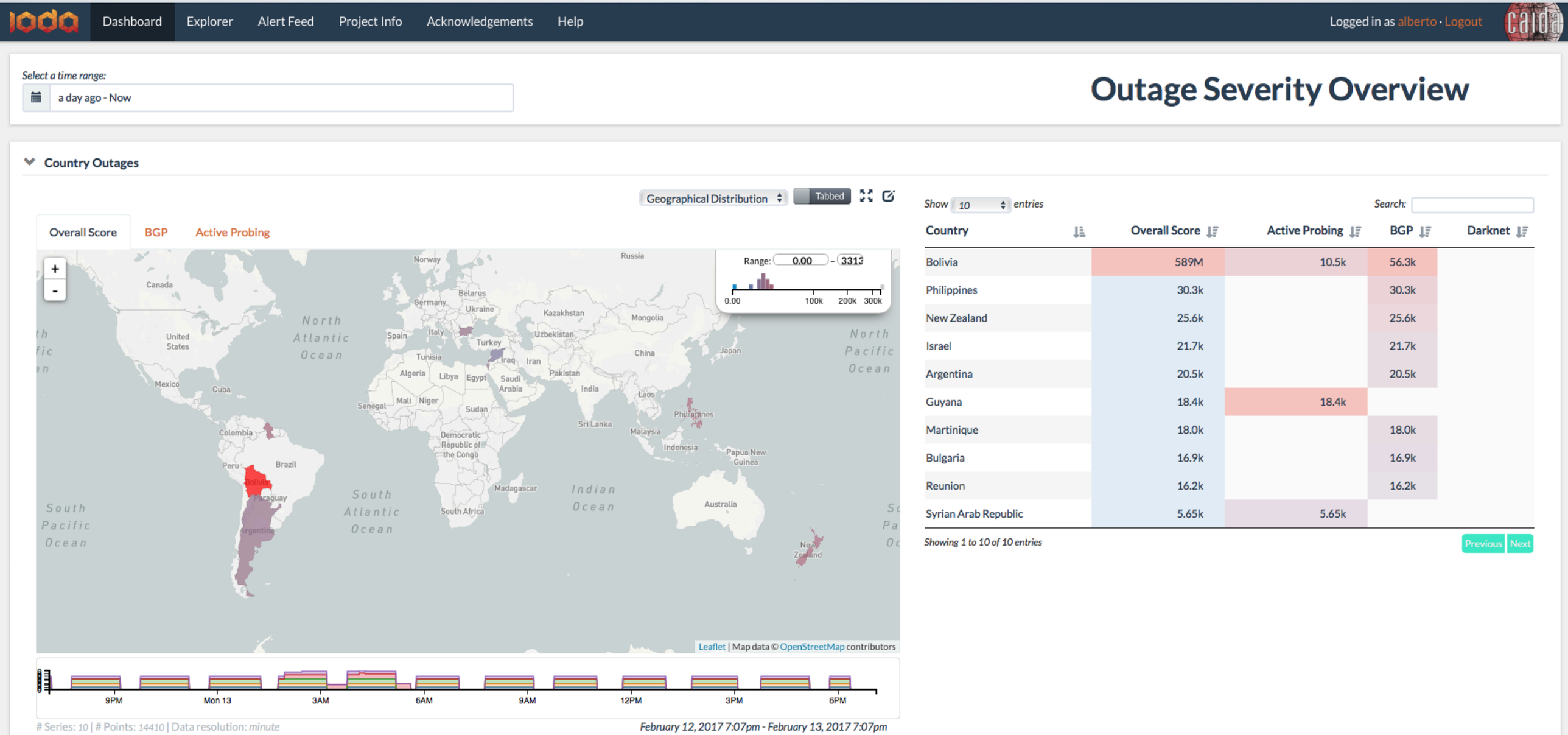
live Internet monitoring

In 2014 we made it possible for anybody to follow the North Korean disconnection almost live



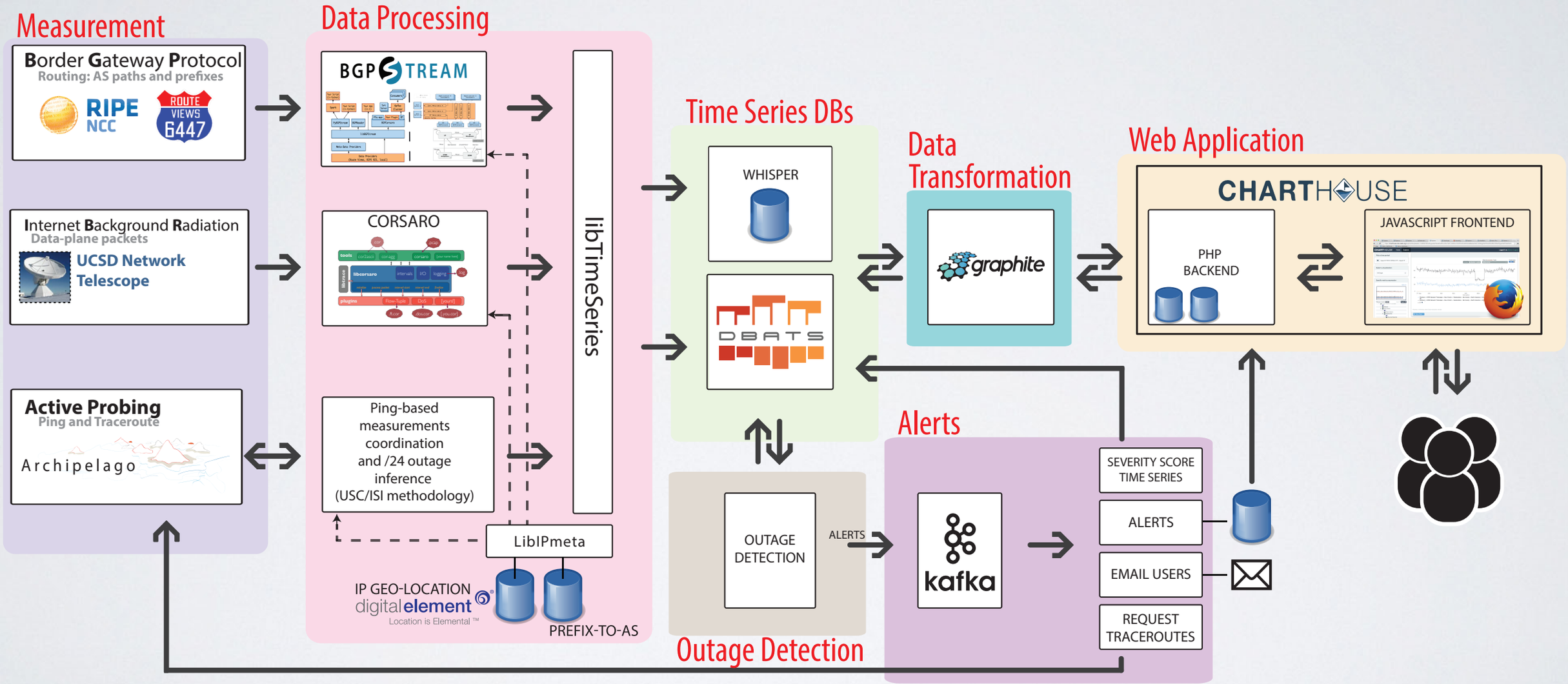
IODA AFTER 4 YEARS (TODAY)

live detection and monitoring



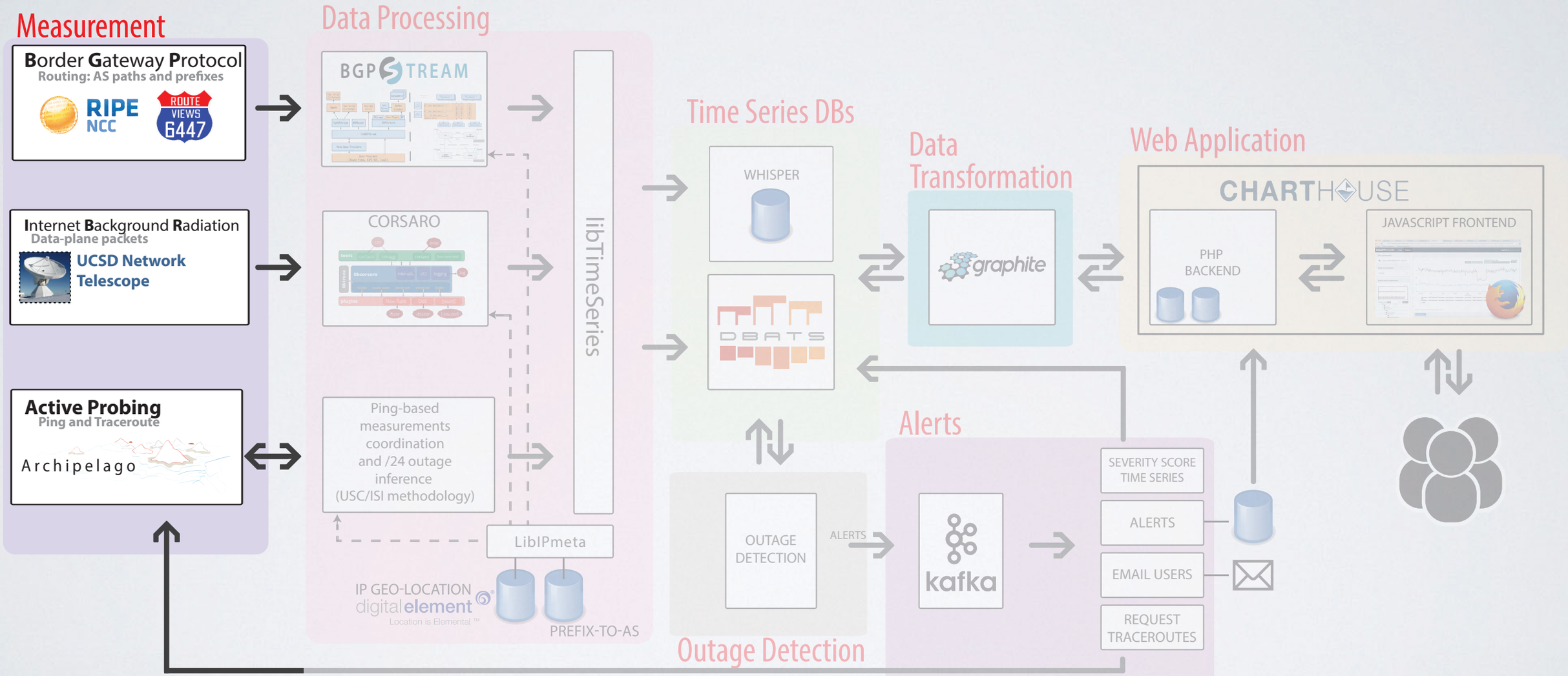
IODA'S CITY MAP

high-level system view



IODA'S CITY MAP

high-level system view



IODA'S CITY MAP

high-level system view

Measurement

Border Gateway Protocol
Routing: AS paths and prefixes
RIPE NCC
ROUTE VIEWS 6447

Internet Background Radiation
Data-plane packets
UCSD Network Telescope

Active Probing
Ping and Traceroute
Archipelago

Data Processing

BGPSTREAM

CORSARO

Ping-based measurements coordination and /24 outage inference (USC/ISI methodology)

libTimeSeries

LibIPmeta

IP GEO-LOCATION digitalelement Location is Elemental ™

PREFIX-TO-AS

Time Series DBs

WHISPER

DBATS

Data Transformation

graphite

Web Application

CHARTHOUSE

PHP BACKEND

JAVASCRIPT FRONTEND

Alerts

OUTAGE DETECTION

ALERTS

kafka

SEVERITY SCORE TIME SERIES

ALERTS

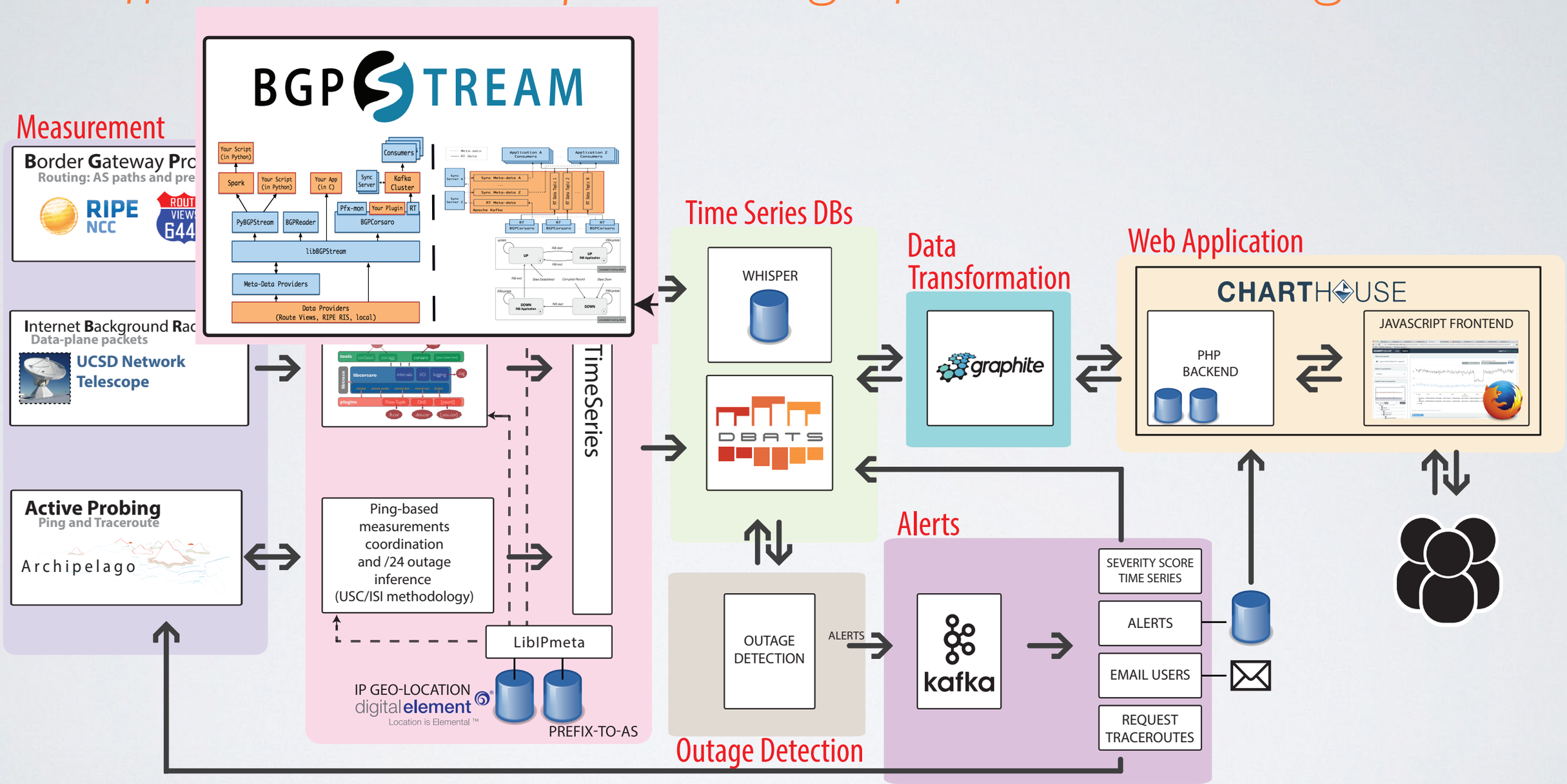
EMAIL USERS

REQUEST TRACEROUTES

Outage Detection

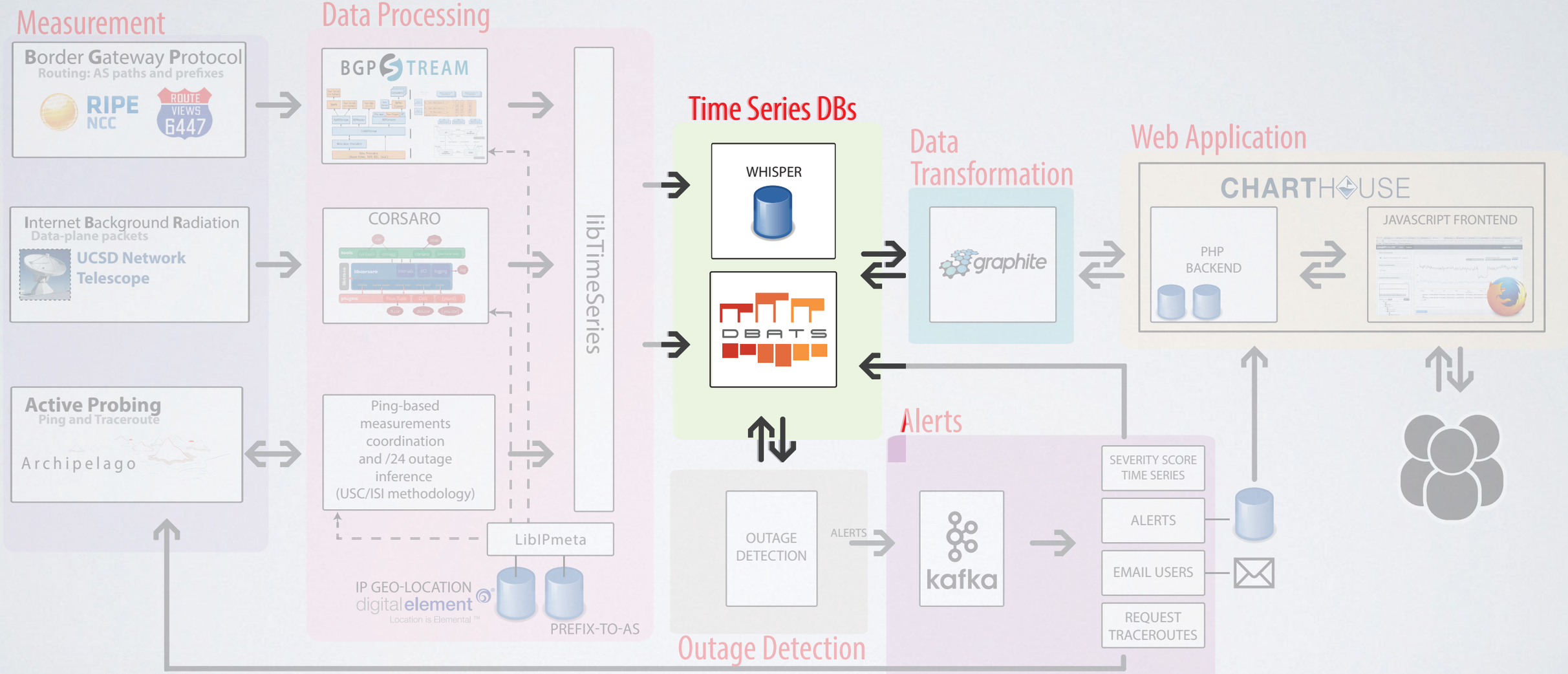
BGPSTREAM

efficient scalable processing of Internet routing data



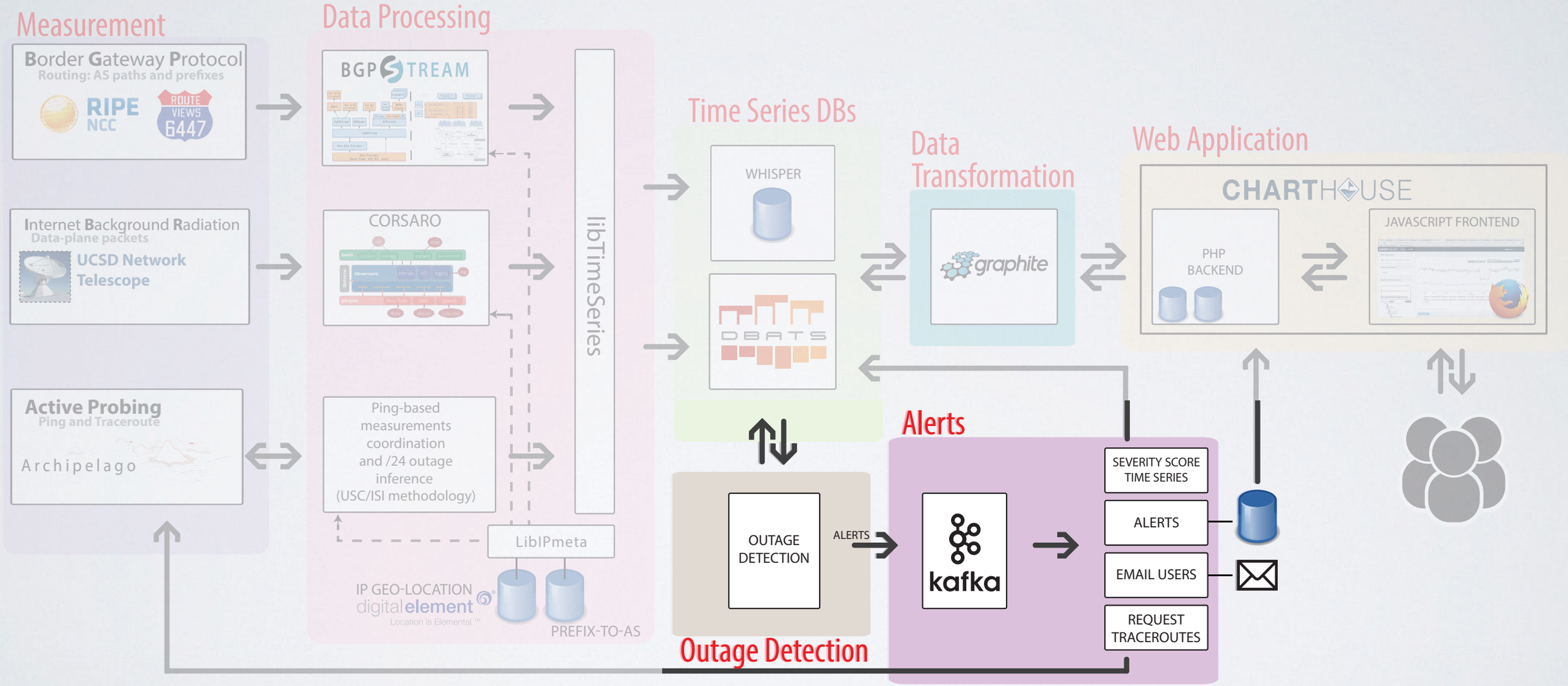
IODA'S CITY MAP

high-level system view



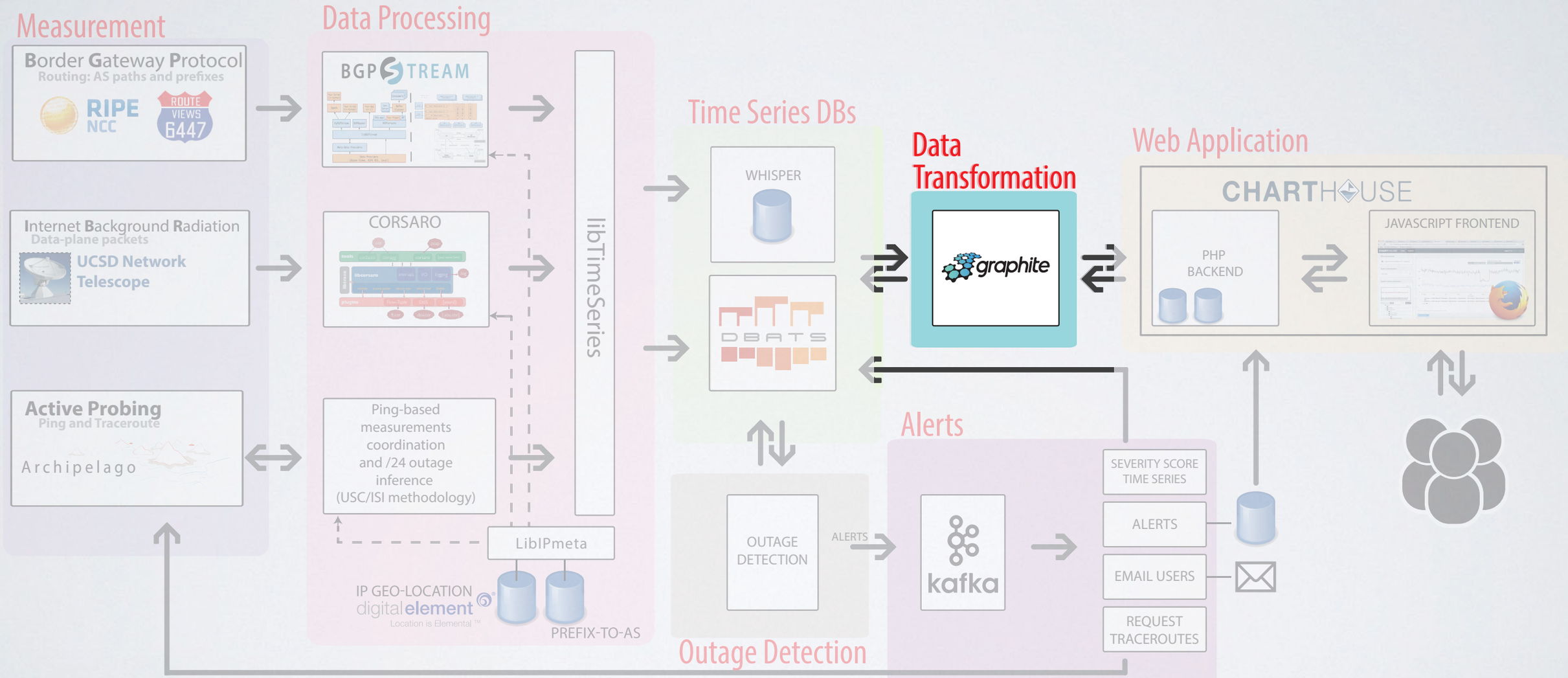
IODA'S CITY MAP

high-level system view



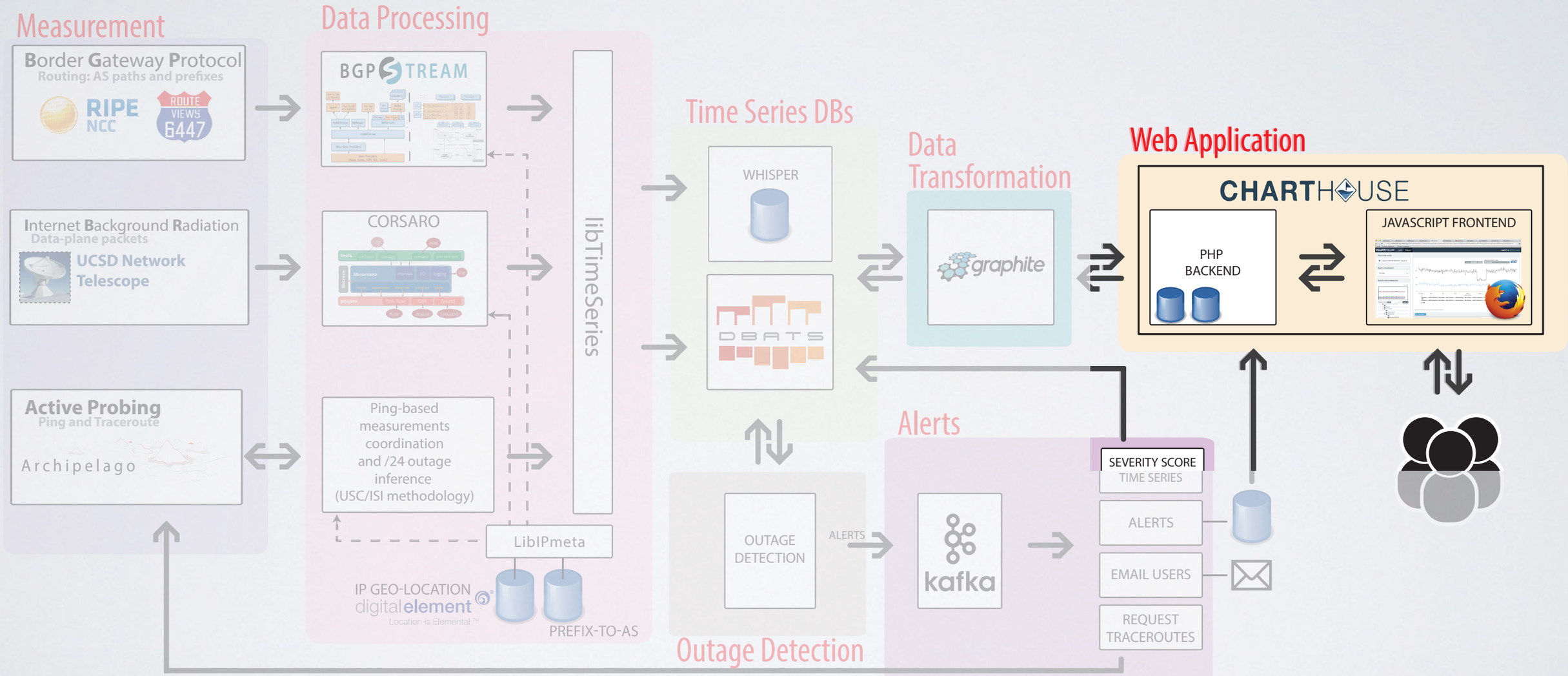
IODA'S CITY MAP

high-level system view

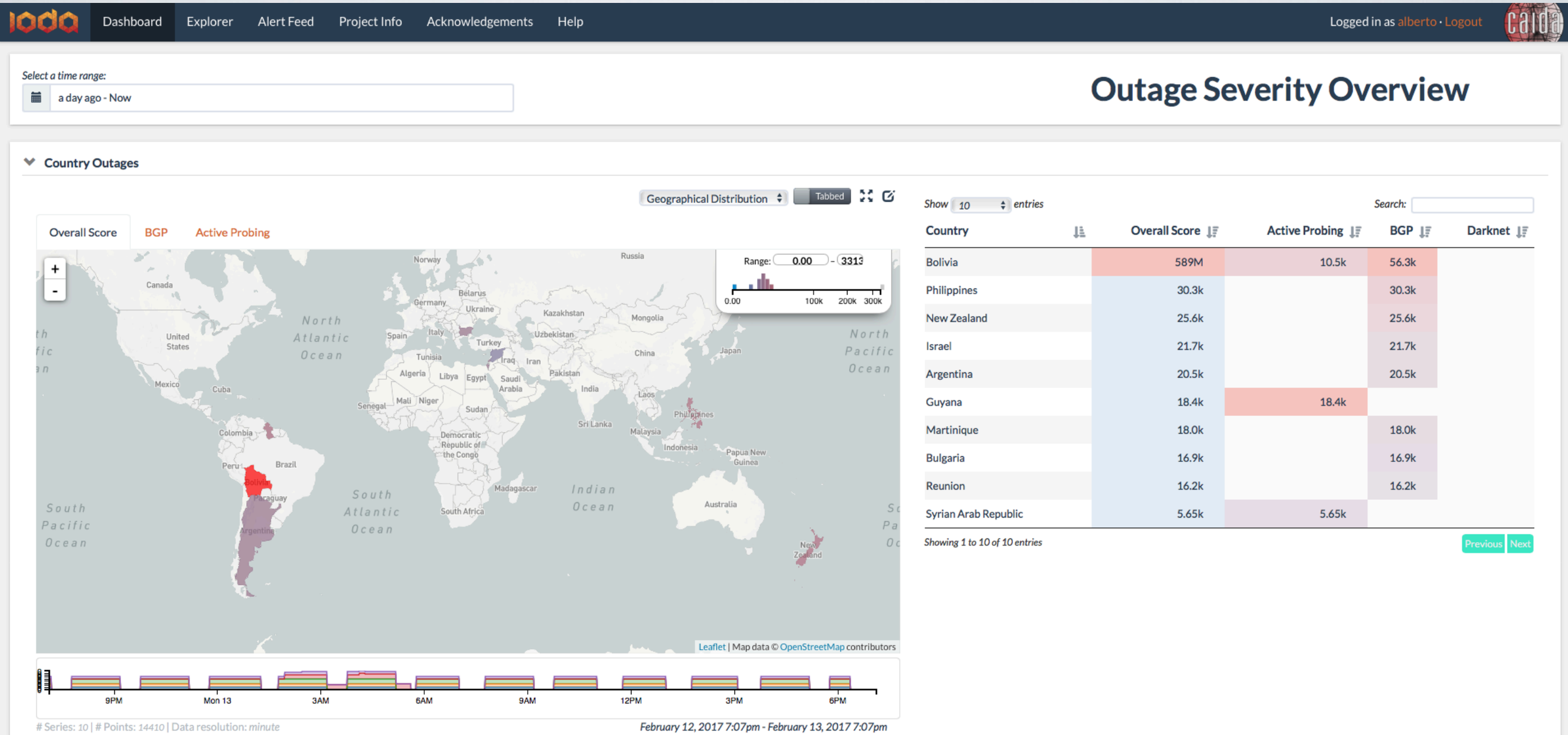


IODA'S CITY MAP

high-level system view

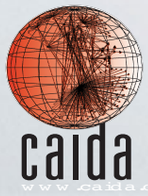


IODA DEMO


Dashboard
Explorer
Alert Feed
Project Info
Acknowledgements
Help
Logged in as alberto · Logout
Select a time range:
a day ago - Now
Outage Severity Overview
Country Outages
Geographical Distribution
Tabbed
Overall Score
BGP
Active Probing
Range: 0.00 - 3313
0.00
100k
200k
300k
Norway
Russia
Canada
Belarus
Germany
Ukraine
Kazakhstan
Mongolia
United States
Spain
Italy
Turkey
Uzbekistan
China
Japan
North Atlantic Ocean
North Pacific Ocean
Tunisia
Algeria
Libya
Egypt
Saudi Arabia
Iraq
Iran
Pakistan
India
Laos
Philippines
Mexico
Cuba
Senegal
Mali
Niger
Sudan
Sri Lanka
Malaysia
Indonesia
Papua New Guinea
Colombia
Democratic Republic of the Congo
Peru
Brazil
Bolivia
Paraguay
Argentina
Madagascar
South Africa
Australia
New Zealand
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
Leaflet | Map data © OpenStreetMap contributors
9PM
Mon 13
3AM
6AM
9AM
12PM
3PM
6PM
Series: 10 | # Points: 14410 | Data resolution: minute
February 12, 2017 7:07pm - February 13, 2017 7:07pm
Show 10 entries
Search:
Country
Overall Score
Active Probing
BGP
Darknet
Bolivia 589M 10.5k 56.3k
Philippines 30.3k 30.3k
New Zealand 25.6k 25.6k
Israel 21.7k 21.7k
Argentina 20.5k 20.5k
Guyana 18.4k 18.4k
Martinique 18.0k 18.0k
Bulgaria 16.9k 16.9k
Reunion 16.2k 16.2k
Syrian Arab Republic 5.65k 5.65k
Showing 1 to 10 of 10 entries
Previous
Next

THANKS

ioda.caida.org



Center for Applied Internet Data Analysis
University of California San Diego