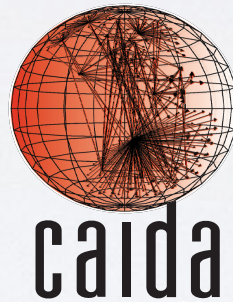


# **Internet Outage Detection & Analysis**

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

**Alberto Dainotti**  
**[alberto@caida.org](mailto: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**

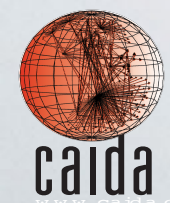
The Internet is a critical infrastructure

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*



Center for Applied Internet Data Analysis  
University of California San Diego

# 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



Cody  
@JoMasta

Follow

Comcast outage in Seattle. City basically shutting down.

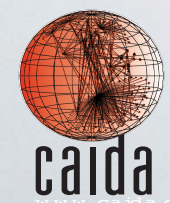
9:38 AM - 9 Apr 2015

6 3

## 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



Center for Applied Internet Data Analysis  
University of California San Diego



# INTERNET OUTAGES

*why so relevant?*

## Human Rights

ensorship and political violence



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

## How Egypt shut down the internet

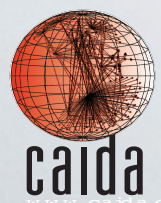
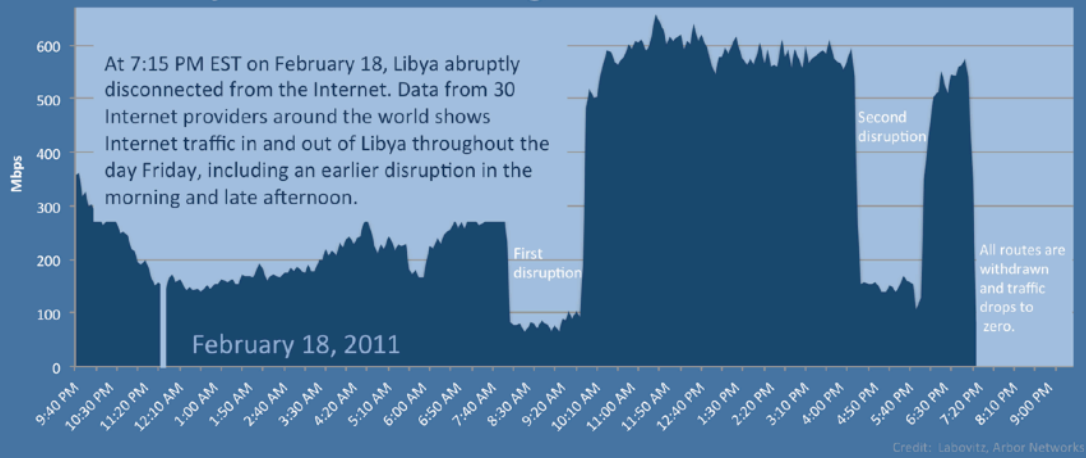
Virtually all internet access in Egypt is cut off today as the govt to contain the street protests that threaten to topple President Mubarak.

2K 0 0 2K Email



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

## Libya Pulls the Plug



Center for Applied Internet Data Analysis  
University of California San Diego

# INTERNET OUTAGES

*why so relevant?*

## Human Rights

ensorship and political violence

QUARTZ  
*Africa*

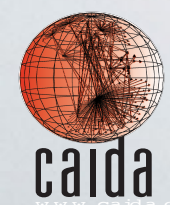
#KEEPITON

## 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**



Center for Applied Internet Data Analysis  
University of California San Diego



# 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

**ioda** *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*

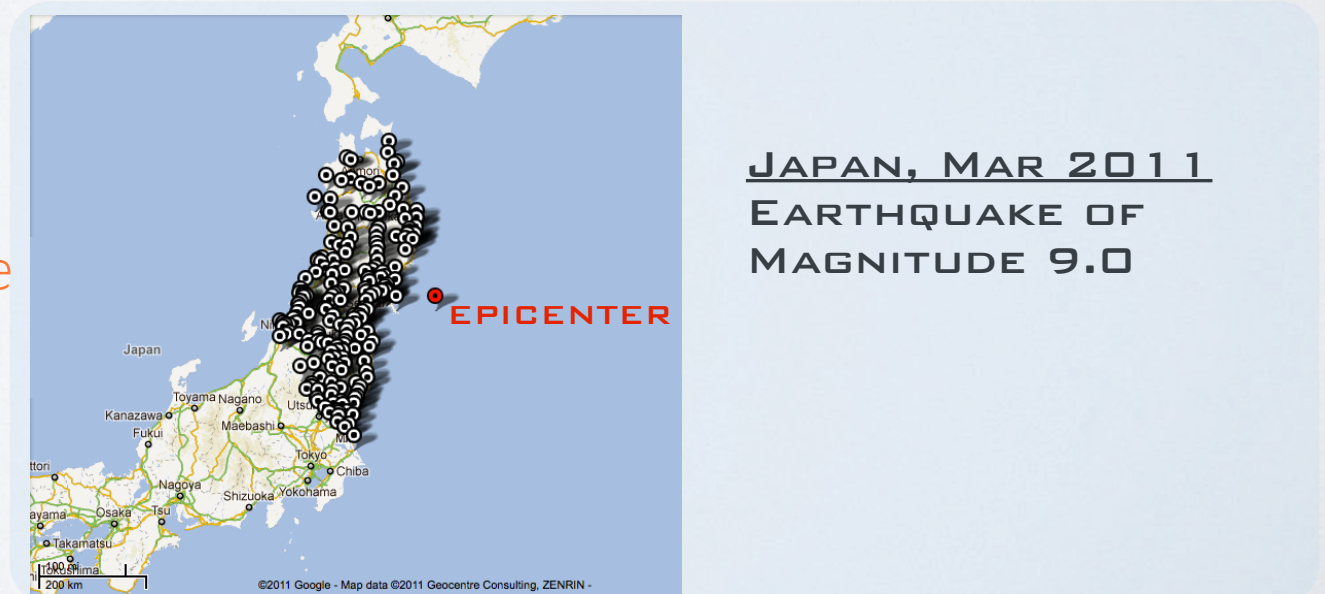
- Country-level Internet Blackouts during the Arab Spring

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



- 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*



# OUR METHODOLOGY

*combining various types of measurements*

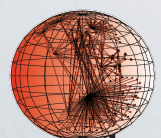
- **multiple types of sources for inference**

- 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**





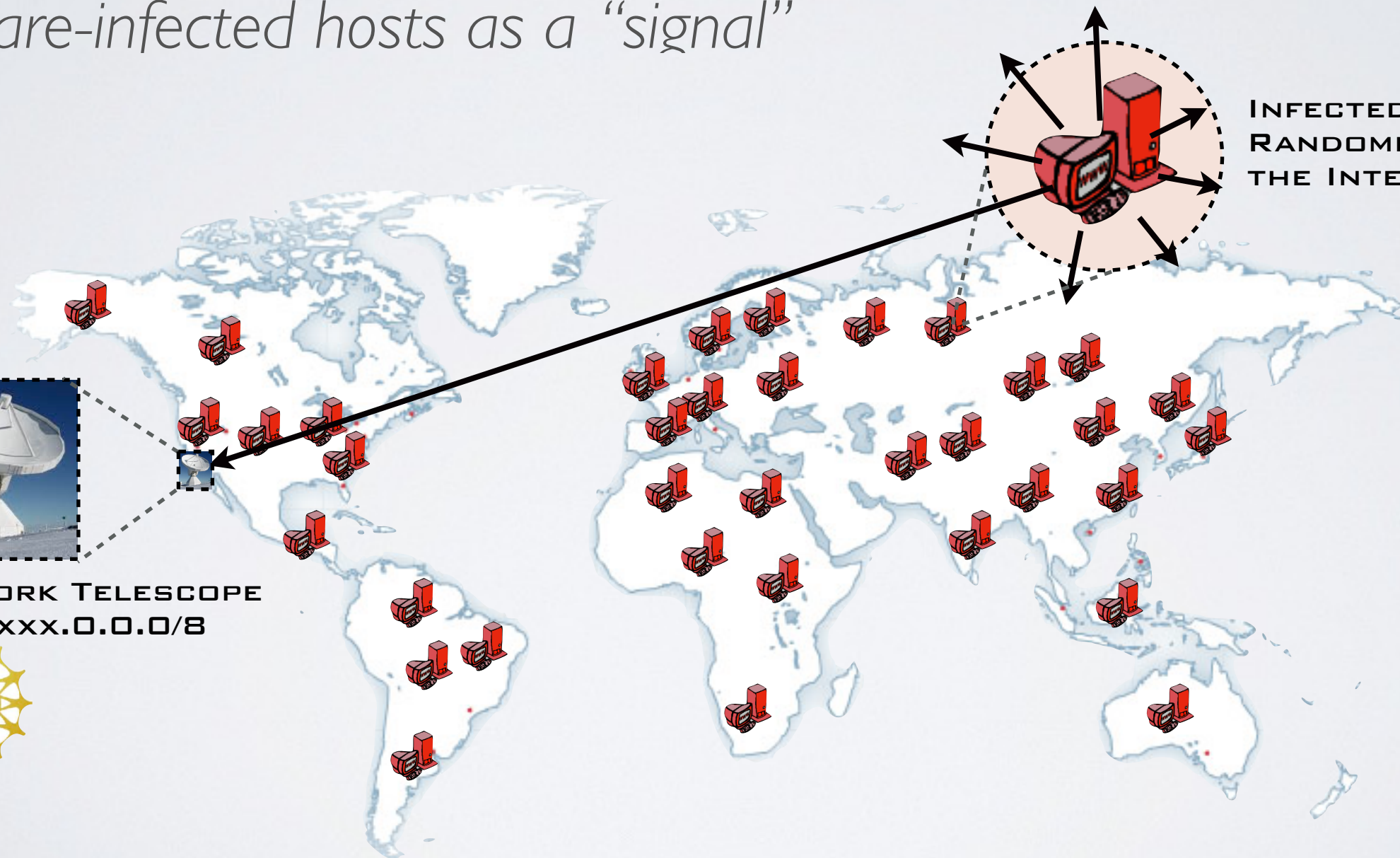
# IBR

*“Extracting benefit from harm..”*

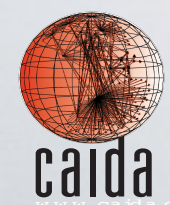


- Use *Internet Background Radiation (IBR)*, mostly generated by *malware-infected hosts* as a “signal”

INFECTED HOST  
RANDOMLY SCANNING  
THE INTERNET



UCSD NETWORK TELESCOPE  
DARKNET XXX.0.0.0/8



Center for Applied Internet Data Analysis  
University of California San Diego

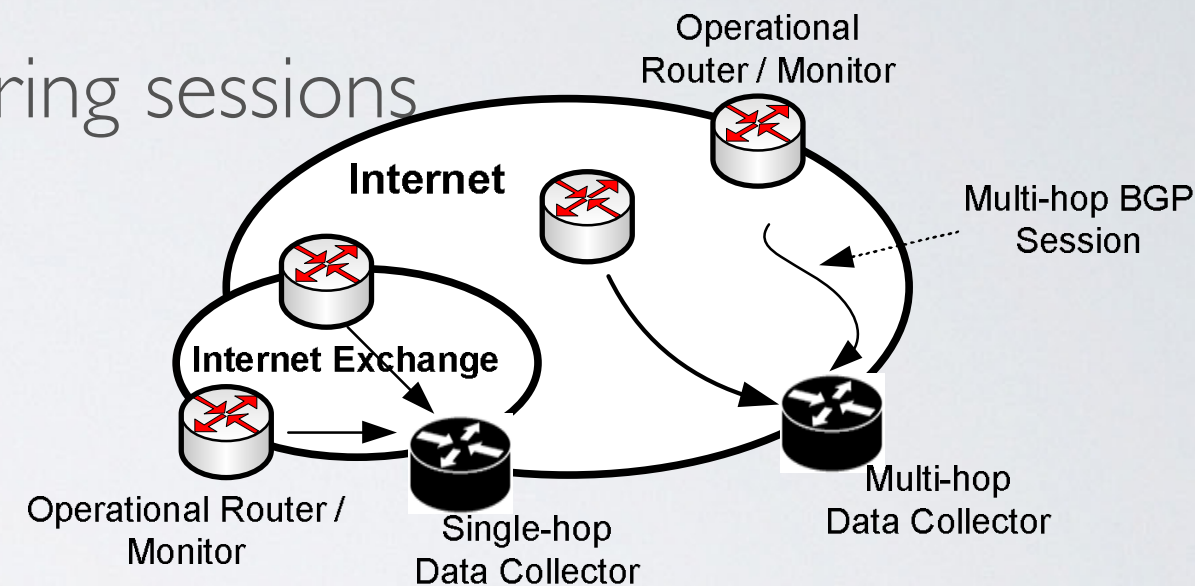
# BGP

## Monitoring Global Internet **Routing**



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

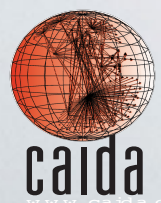
- RouteViews (Univ. Oregon): 371 peers
- RIPE RIS (RIPE NCC): 508 peers



**RIPE  
NCC**

<http://www.routeviews.org>

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



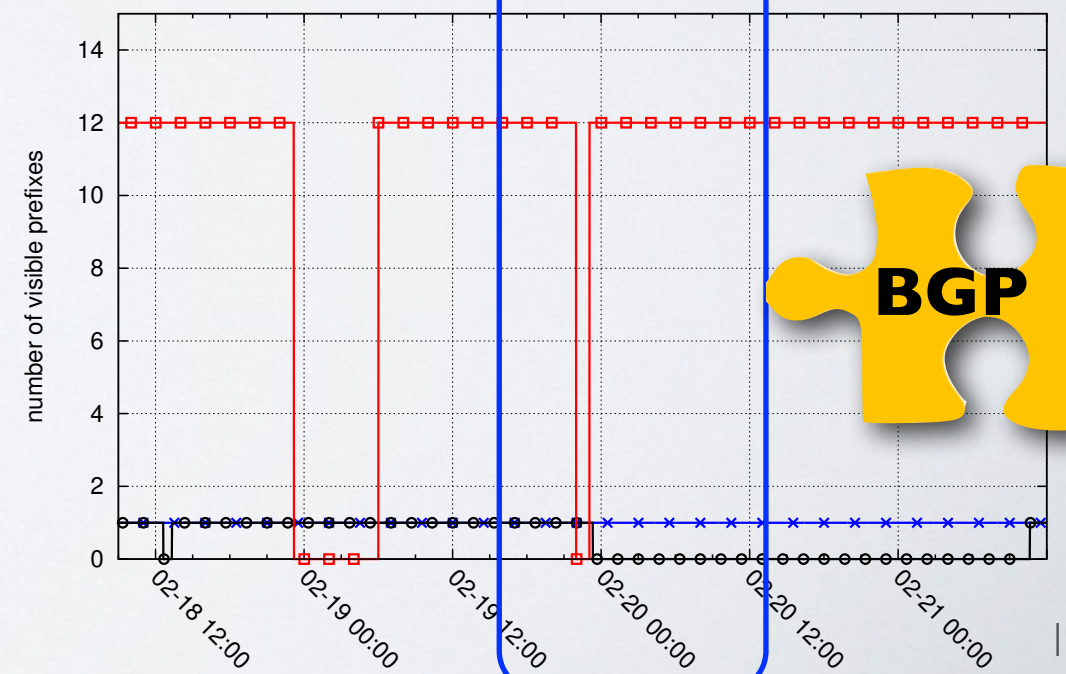
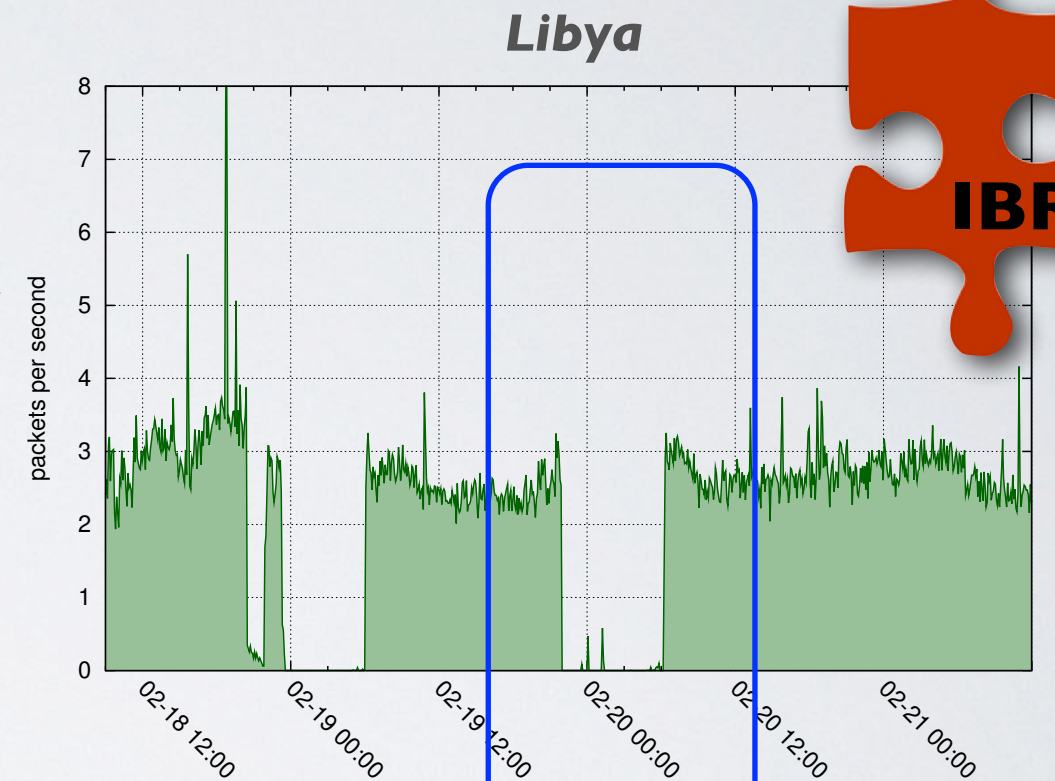
Center for Applied Internet Data Analysis  
University of California San Diego



# 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**

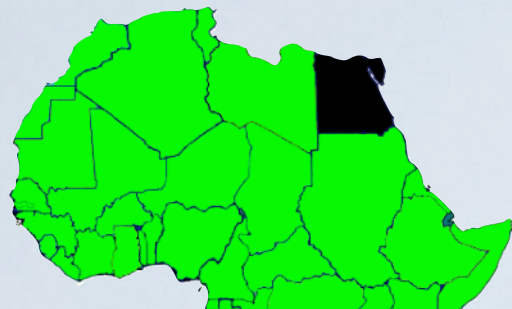


LyStateAS —■—  
IntAS2 —●—  
SatAS1 —×—

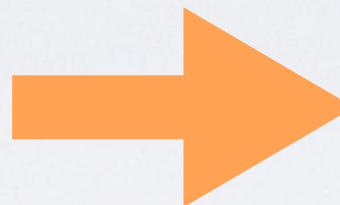


# BEFORE IODA

## 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 Pescapè  
University of Napoli Federico II

#### ABSTRACT

In the first months of rapid... (text continues)

Categories and S  
C.2.3 [Network Opera  
C.2.5 [Local and Wide

General Terms  
Measurement, Security

Permission to make digi  
personal or classroom use  
not made or distributed be  
hear this notice and the ful  
republic, to post on serv  
permission and/or a fee.  
DOI: 10.1145/1928424  
Copyright 2011 ACM 978

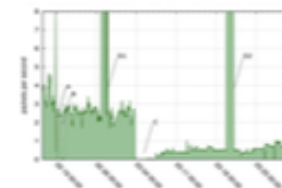


Figure 12: UCSD datanet's traffic coming from Libya. Labels A, B, C indicate the three outages. Spikes labeled D1 and D2 are due to backscatter from two denial-of-service attacks.

related to protests in the country. The web site of the Ministry of Communications (mcc.gov.ly) was attacked with a randomly-spoofed DoS attack just before the outage started, on January 26 at different times: 15:47 GMT (for 16 minutes), 16:55 GMT (17 minutes), and 21:09 GMT (53 minutes). Analysis of the backscatter traffic to the datanet allows estimation of the intensity of the attack in terms of packet rate, indicating average packet rates between 20k and 50k packets per second.

On February 2 the web site of the Egyptian Ministry of Interior (www.moi.gov.eg) was targeted by two DoS attacks: just after the end of the censorship from 11:05 to 15:39 GMT and from 15:06 to 17:17 GMT. The same IP address was attacked another time the day after, from 08:06 to 08:42 GMT. In this case the estimated packet rates were smaller, around 7k packets per second.

#### 5.2 Libya

##### 5.2.1 Overview

Libya's Internet infrastructure is even more prone to manipulation than Egypt's, judging from its physical structure. International connectivity is provided by only two submarine cables, both ending in Tripoli [39], and the Internet infrastructure is dominated by a single, state owned, AS. We only found two other ASes having a small presence in Libya, as described in Section 5.2.2.

In Libya three different outages in early 2011 were identified and publicly documented (Figure 1). Figure 12 shows the traffic observed by the UCSD network telescope from Libya throughout an interval encompassing the outages. The points labeled A, B and C indicate three different blackout episodes; points D1 and D2 refer to two denial-of-service attacks discussed in Section 5.2.3. Toward the right of the graph it is difficult to interpret what is really happening in Libya because of the civil war.

##### 5.2.2 Outages in detail

The first two outages happened during two consecutive nights. Figure 13(a) shows a more detailed view of these two outages as observed by the UCSD telescope. Figure 13(b) shows BGP data over the same interval: in both cases, within a few minutes, 12 out of the 15 IPv4 prefixes associated with IP address ranges officially delegated to Libya were withdrawn. These twelve IPv4 prefixes were announced by LibStateAS, the local telecom operator, while the remaining IPv4 prefix was managed by ItroAS2. As of May 2011, there were no IPv6 prefixes in AfrNIC's delegated file for Libya. The MaxMind IP geolocation database further puts 12 non-contiguous IP ranges in Libya, all part of an encompassing IPv4

prefix announced by SatAS1, which provides satellite services in the Middle East, Asia and Africa. The covering IPv4 prefix also contained 180 IP ranges in several other countries predominantly in the Middle East. We considered this additional AS because the UCSD datanet generally observed a significant amount of unrequested traffic coming from IPs in those 12 ranges before the first outage (about 50k packets each day). This level of background traffic indicates a population of customers using PCs likely infected by Conficker or other malware, allowing inference of network conditions. Traffic from this network also provided evidence of what happened to Libyan Internet connections based on satellite systems not managed by the local telecom provider.

Comparing Figures 13(a) and 13(b) reveals a different behavior that conflicts with previous reports [17]: the second outage was not entirely caused by BGP withdrawals. The BGP shutdown began on February 19 around 21:58:55 UTC, exactly matching the sharp decrease of datanet traffic from Libya (and in accordance with reports on Libyan traffic seen by Arbor Networks [31]) but it ended approximately one hour later, at 23:02:52. In contrast, the Internet outage as shown by the telescope data and reported by the news [17] lasted until approximately February 20 at 6:12 UTC. This finding suggests that a different disruption technique – a packet-blocking strategy apparently adopted subsequently in the third outage and recognized by the rest of the world – was already being used dur-

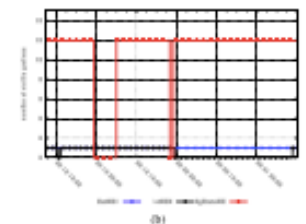
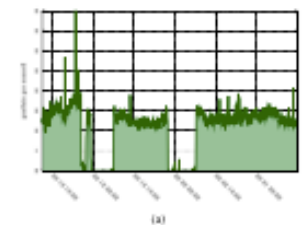
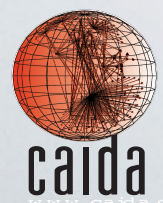


Figure 13: The first two Libyan outages: (a) unolicited traffic to UCSD datanet coming from Libya; (b) visibility of Libyan IPv4 prefixes in BGP data from Roma/Views and RIPE/NCC/RIIS collectors. Note that the control-plane and data-plane observations of connectivity do not match, suggesting that different techniques for censorship were being used during different outages.

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*



**manual analysis**

**post-event**

**a couple of events**

**4 months of work**



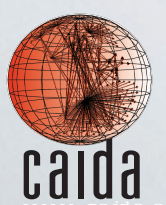
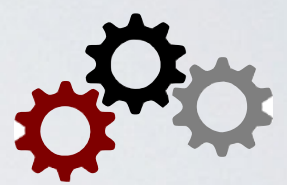
**automated**

**near-realtime detection**

**24/7 monitoring**

**whole Internet**

**in few minutes**



Center for Applied Internet Data Analysis  
University of California San Diego

# 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

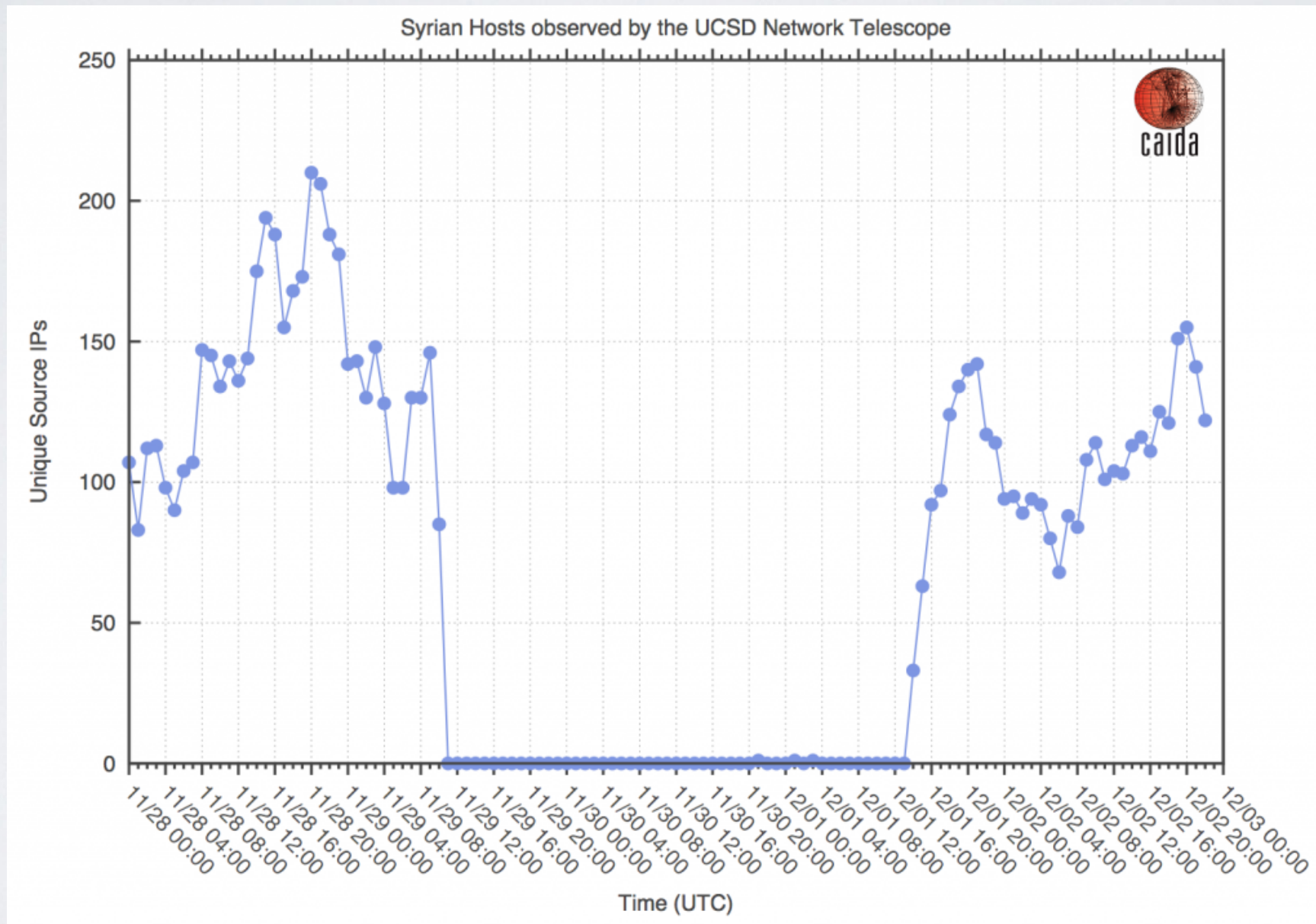
*Why this is a tough problem*

- 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**

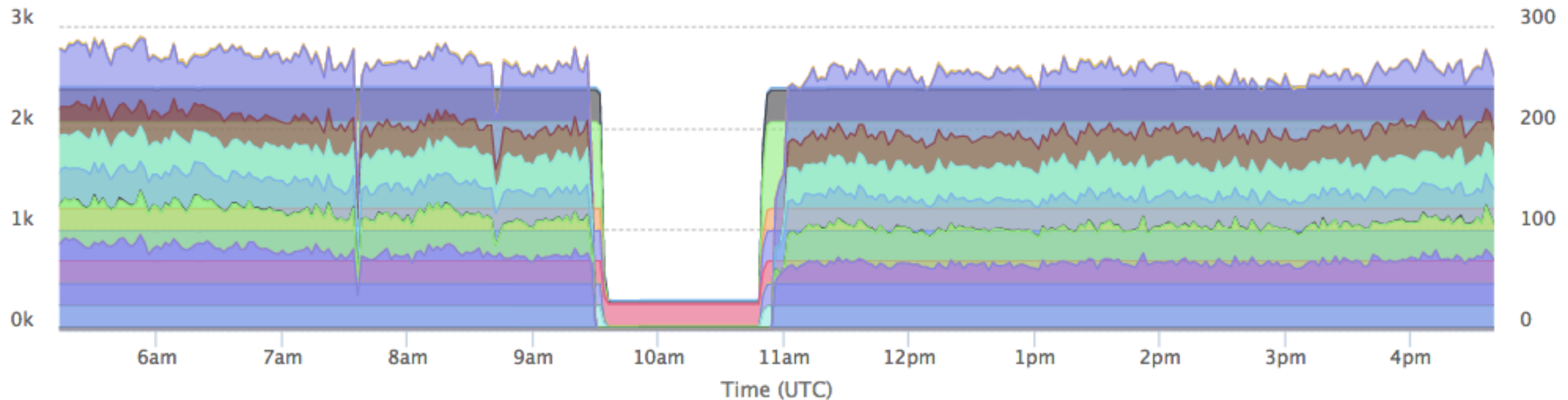




# IODA FIRST YEARS

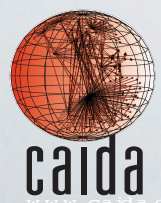
*documenting events on our blog*

**Time Warner Cable outage 27th August 2014**



■ BGP > Global Prefix Visibility > Autonomous System Number (ASN) > 3456 > # IPv4 Prefixes [y1]  
■ BGP > Global Prefix Visibility > Autonomous System Number (ASN) > 7843 > # IPv4 Prefixes [y1]  
▲ 1/23 ▼

August 27 2014 5:13am - August 27 2014 4:39pm



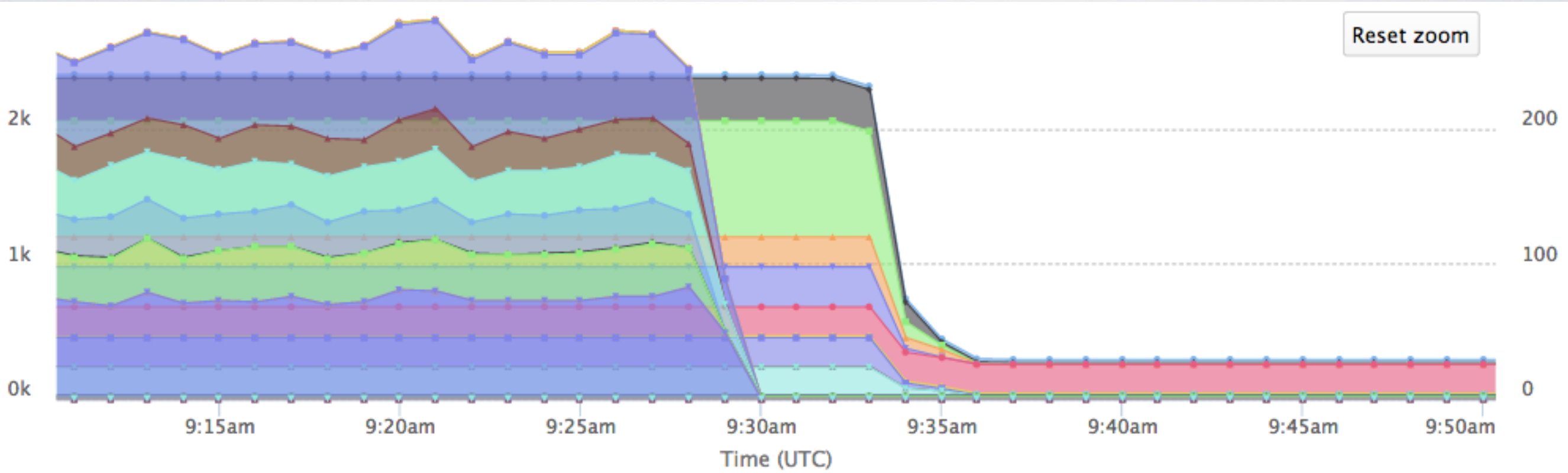
Center for Applied Internet Data Analysis  
University of California San Diego

# IODA FIRST YEARS

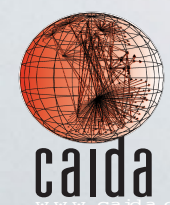
*documenting events on our blog*

## **Time Warner Cable outage 27th August 2014**

Reset zoom



- BGP > Global Prefix Visibility > Autonomous System Number (ASN) > 3456 > # IPv4 Prefixes [y1]
- BGP > Global Prefix Visibility > Autonomous System Number (ASN) > 7843 > # IPv4 Prefixes [y1]
- ▲ 1/23 ▼







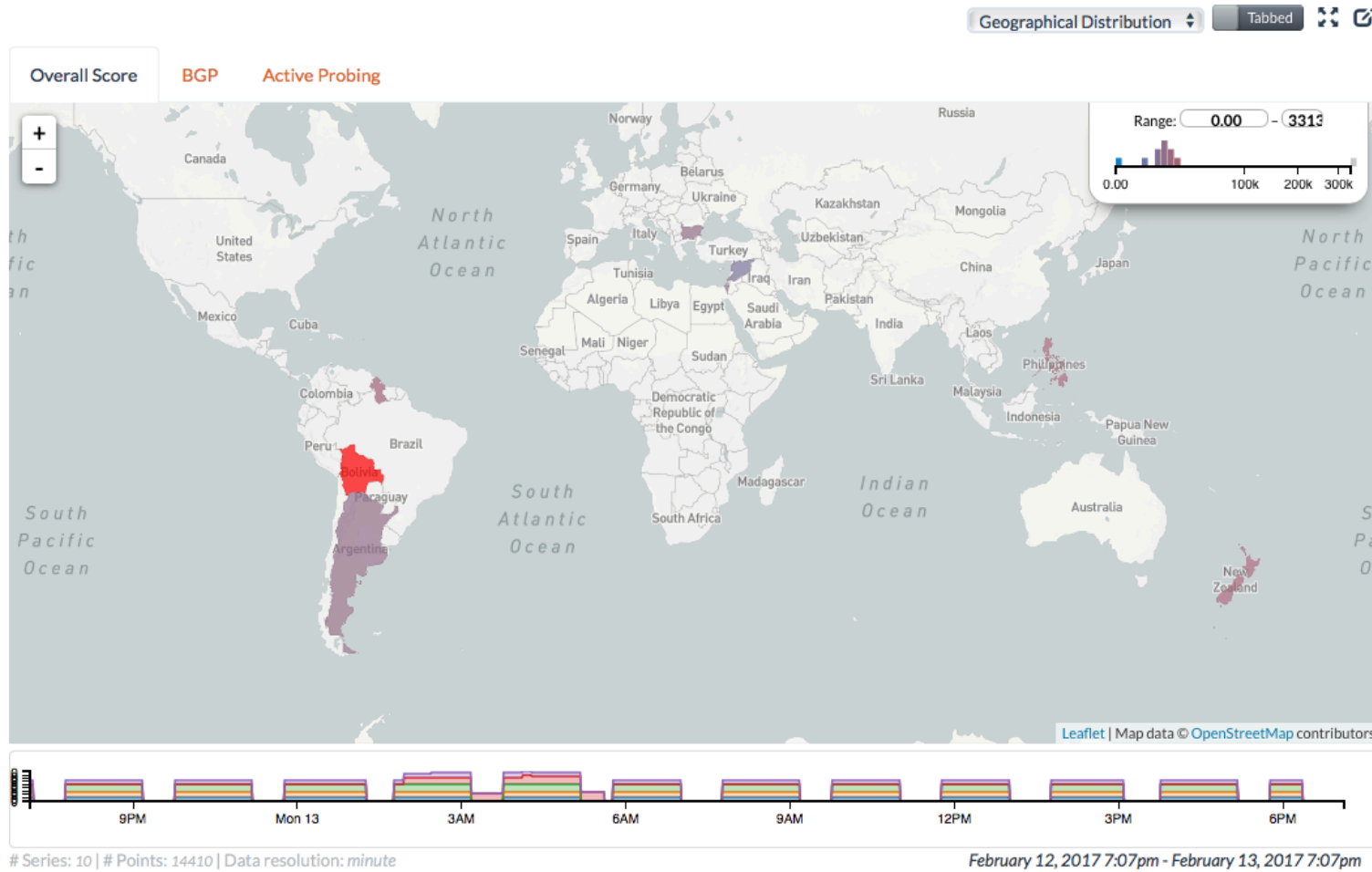
# IODA AFTER 4 YEARS (TODAY)

*live detection and monitoring*

Select a time range:  
a day ago - Now

## Outage Severity Overview

### Country Outages



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          |       |         |

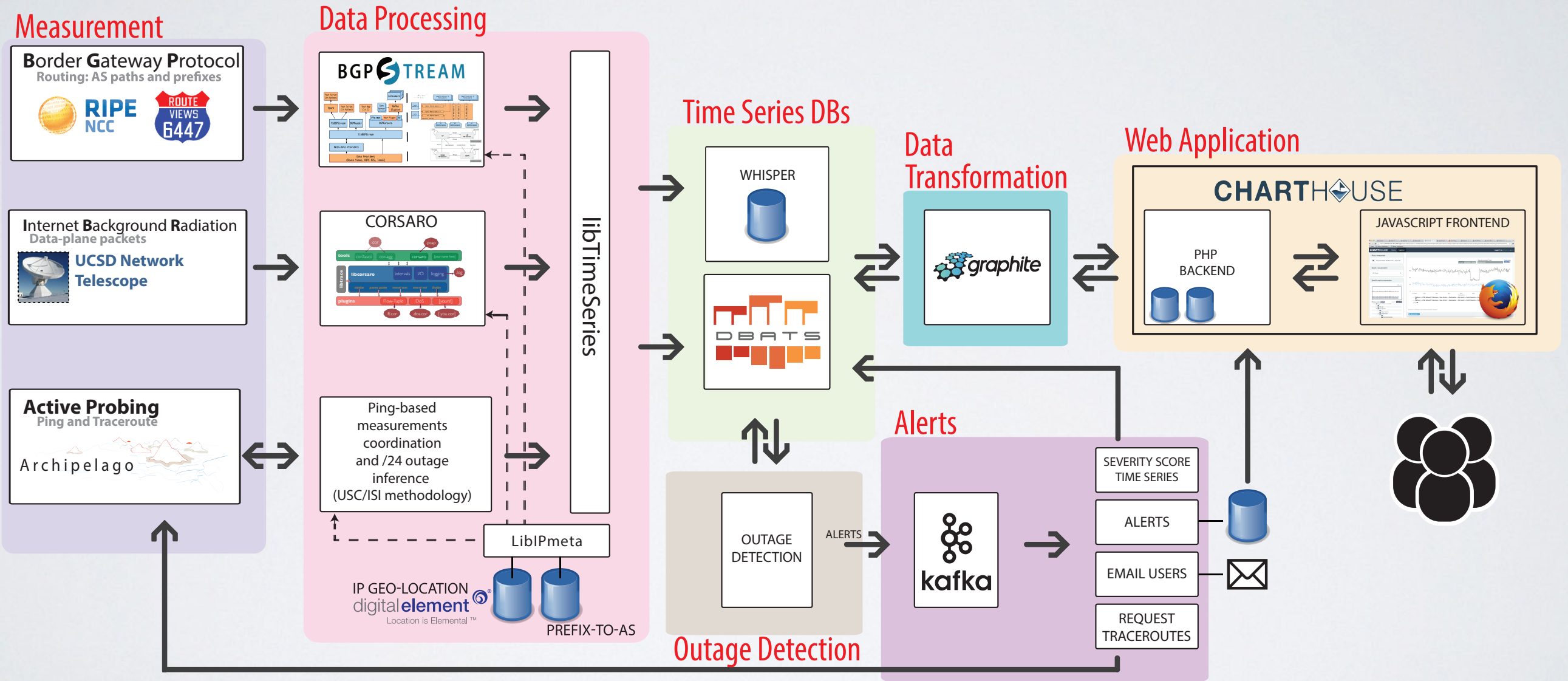
Showing 1 to 10 of 10 entries

Previous Next



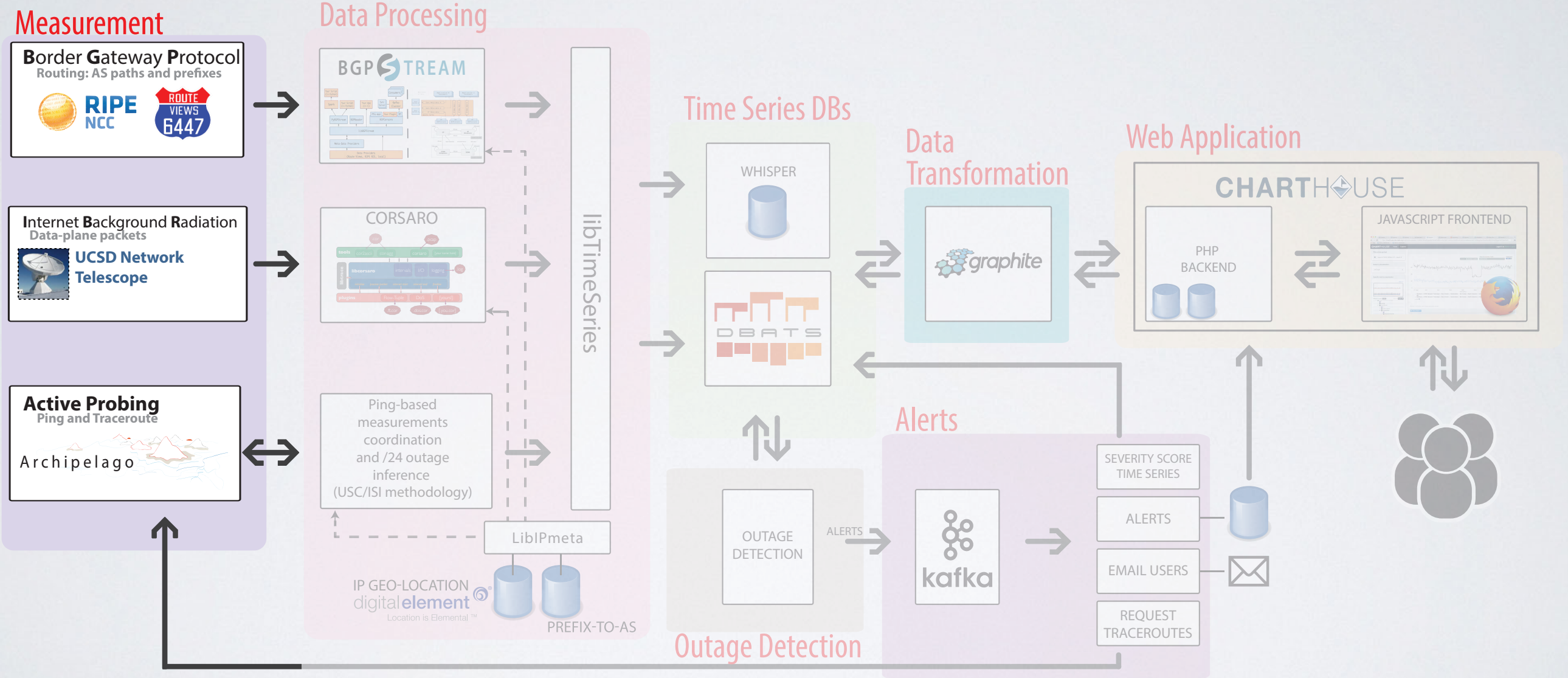
# IODA'S CITY MAP

*high-level system view*



# IODA'S CITY MAP

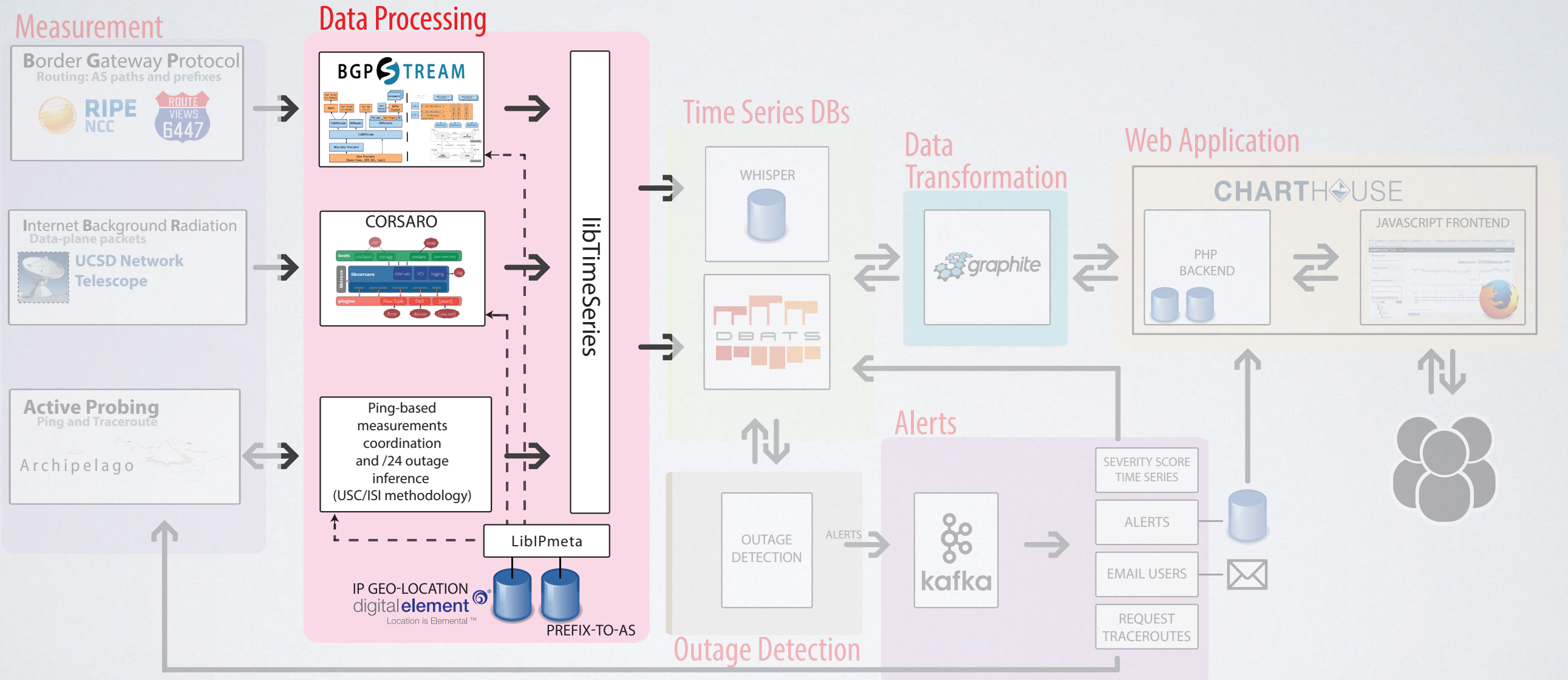
*high-level system view*





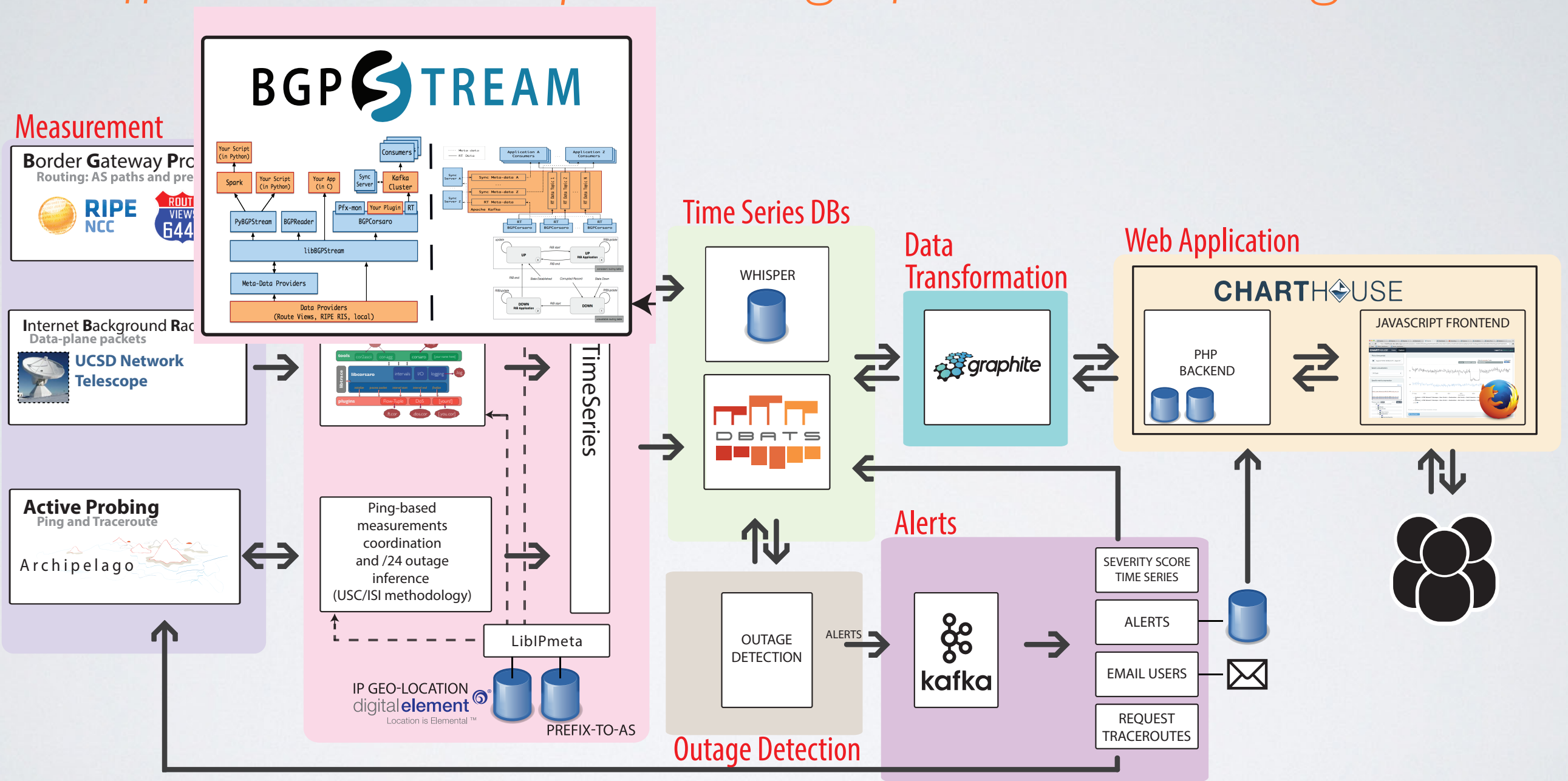
# IODA'S CITY MAP

*high-level system view*



# BGPSTREAM

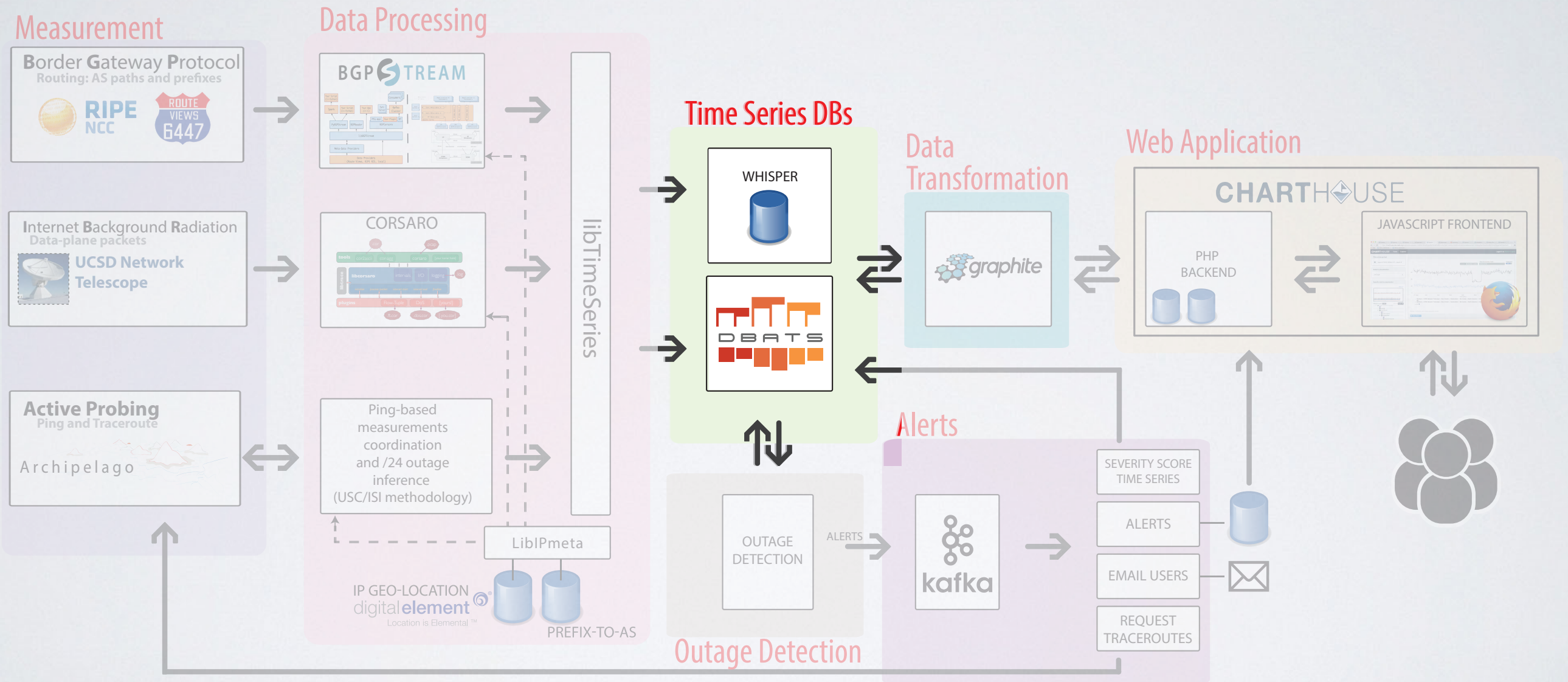
*efficient scalable processing of Internet routing data*





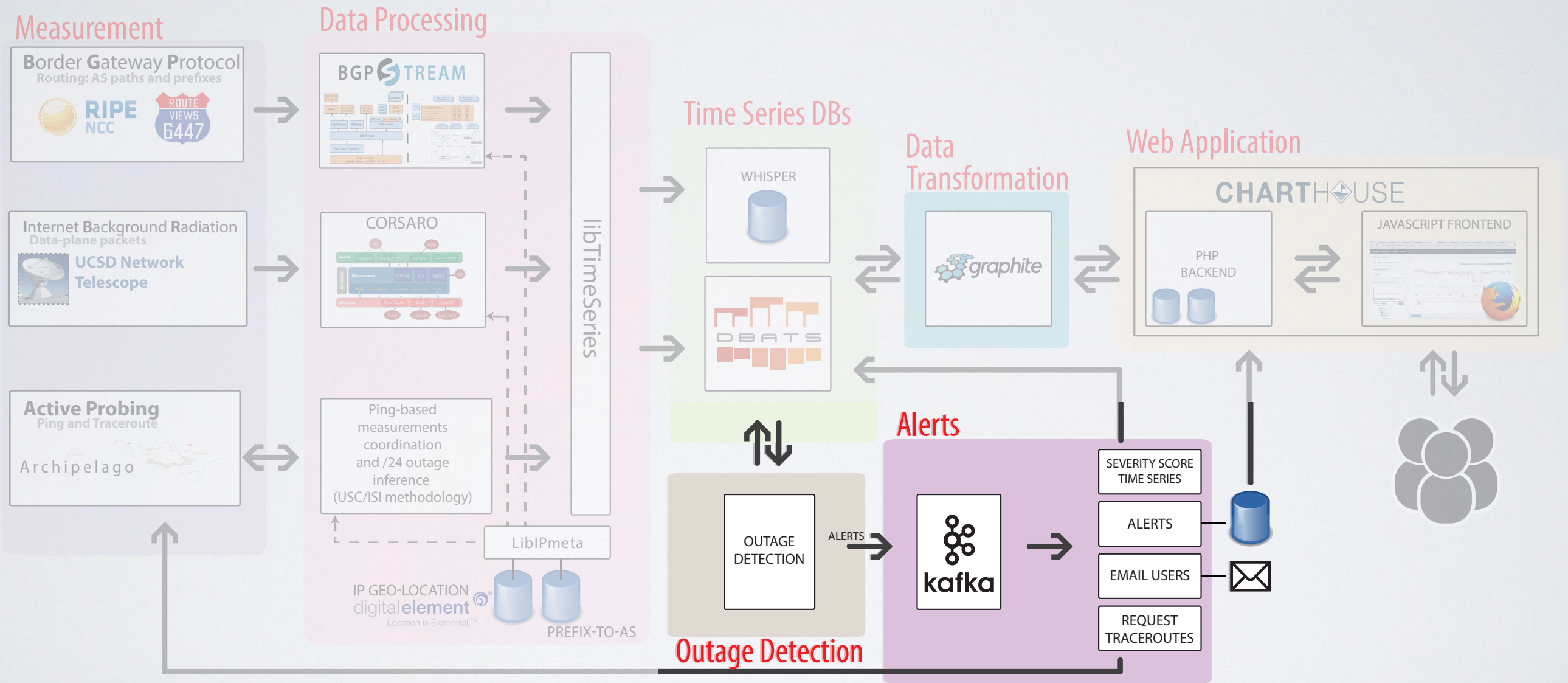
# IODA'S CITY MAP

*high-level system view*



# IODA'S CITY MAP

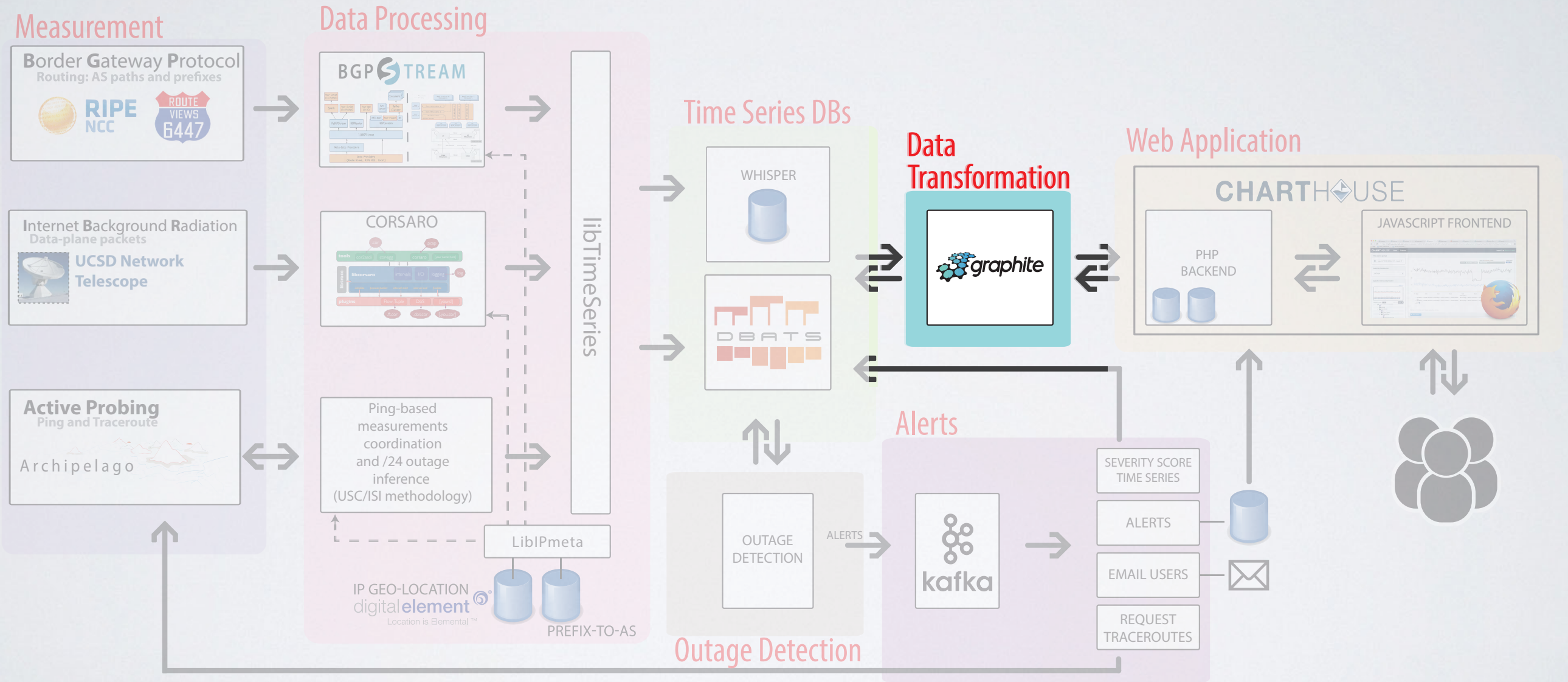
*high-level system view*





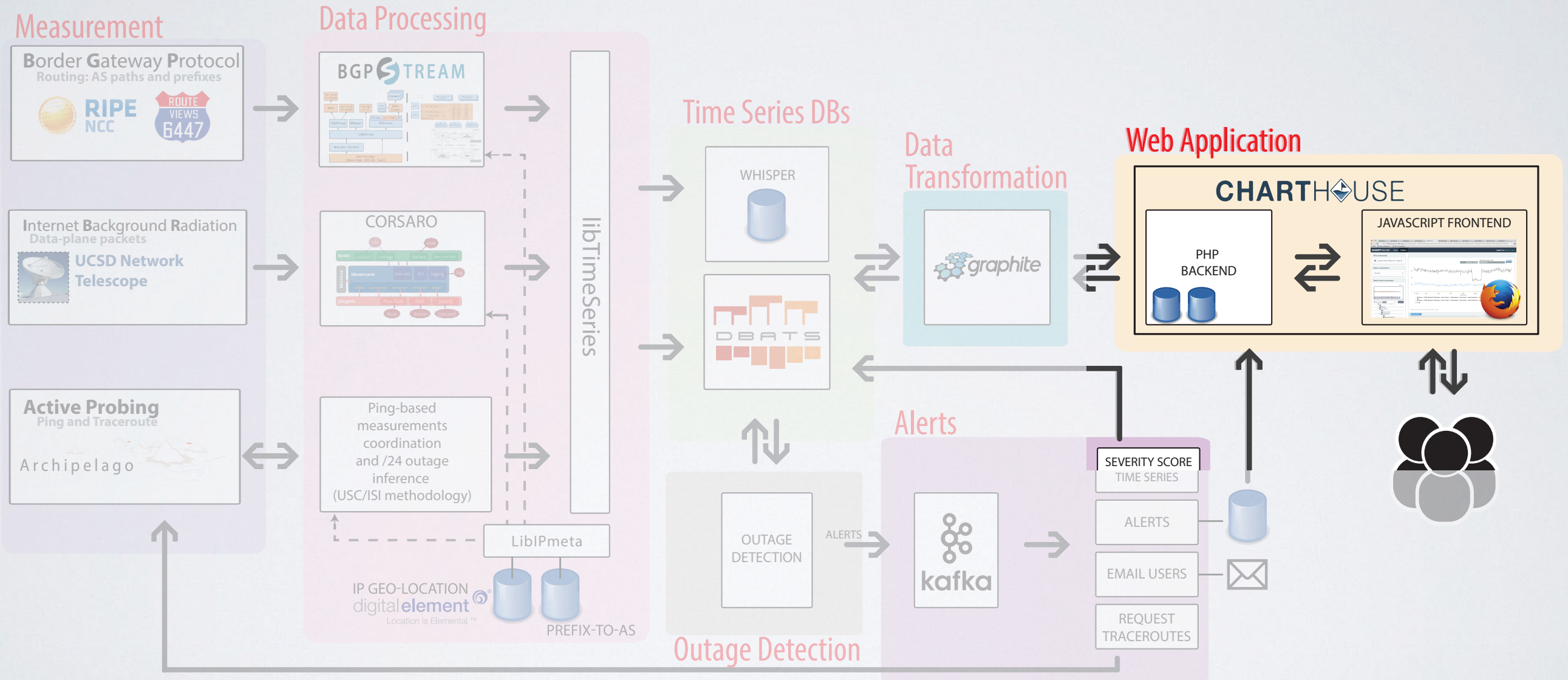
# IODA'S CITY MAP

*high-level system view*



# IODA'S CITY MAP

*high-level system view*





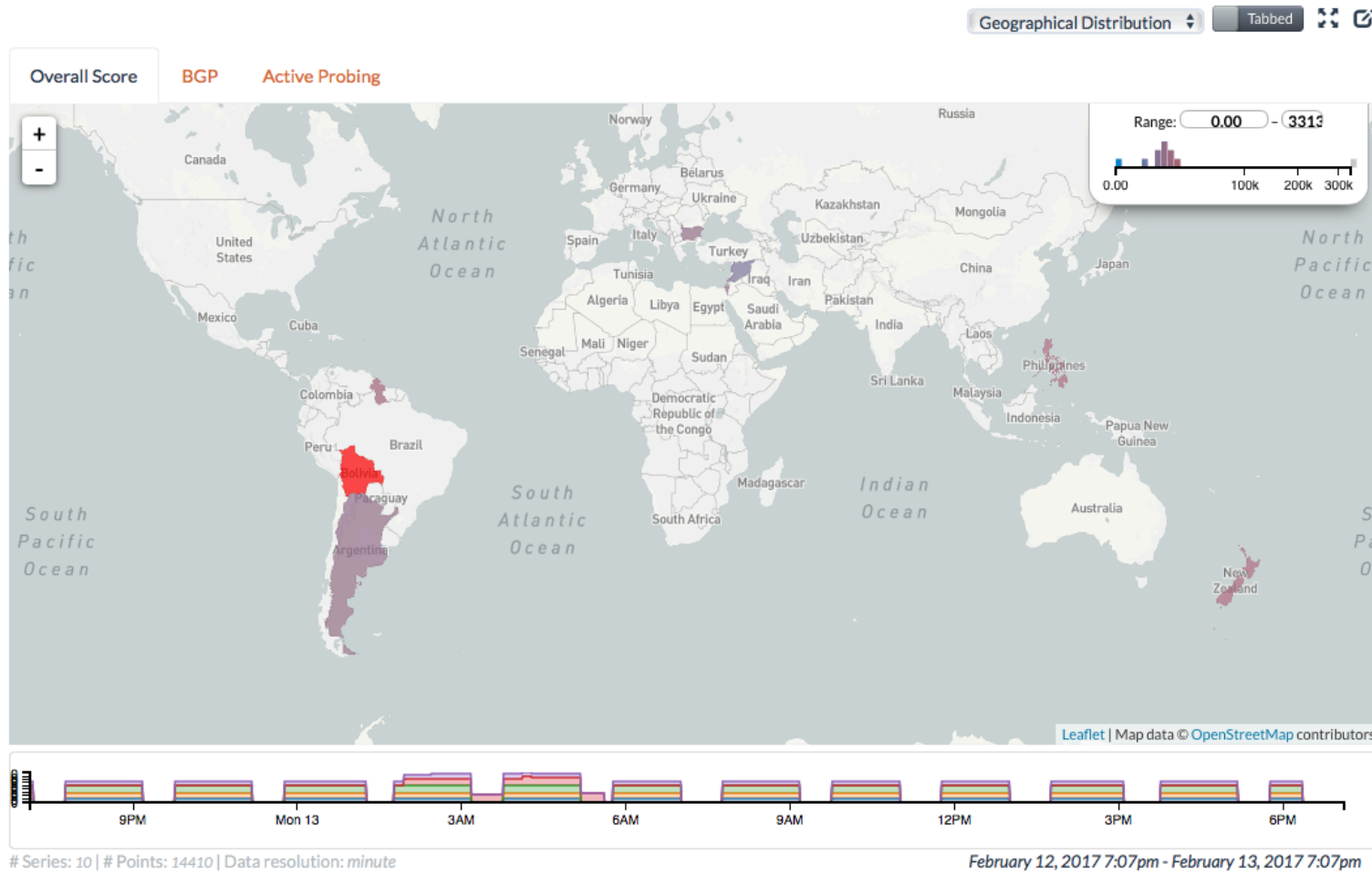
# IODA DEMO

Select a time range:

a day ago - Now

## Outage Severity Overview

### Country Outages



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](http://ioda.caida.org)*

