ioda

Internet Outage Detection & Analysis

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

Alberto Dainotti, kc claffy, Alistair King

Vasco Asturiano, Karyn Benson, Marina Fomenkov, Brad Huffaker,
Young Hyun, Ken Keys, Ryan Koga, Alex Ma, Chiara Orsini, Josh Polterock

caida

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

NSF

U.S. DEPARTMENT OF HOMELAND SECURITY

COMCAST

SDSC
SAN DIEGO SUPERCOMPUTER CENTER

UC San Diego

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, in *near-realtime*, 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

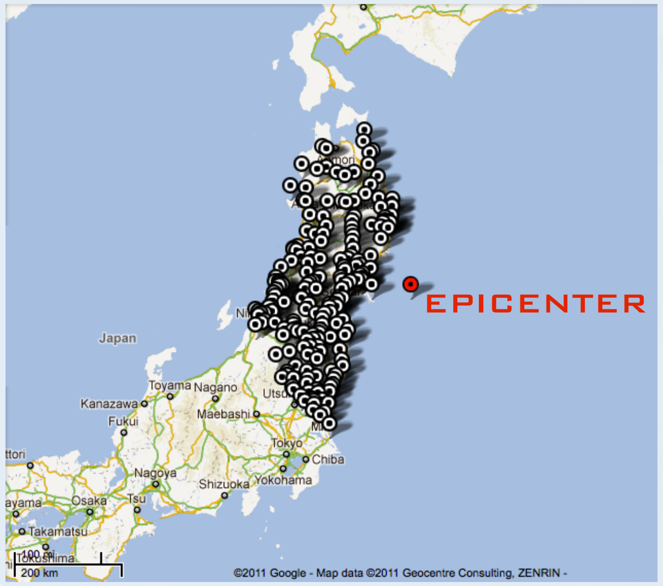
- Country-level Internet Blackouts during the Arab Spring

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

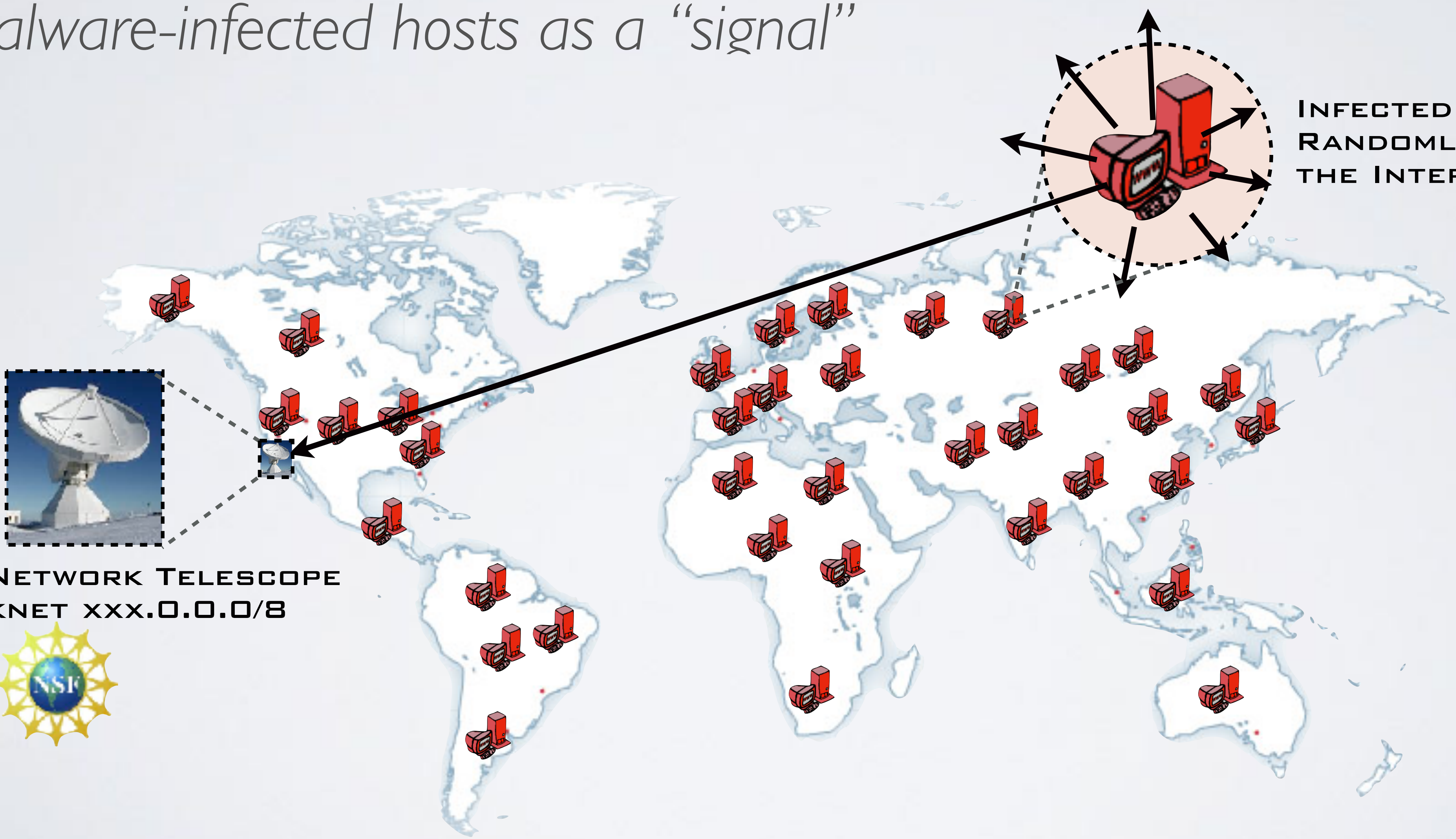
combining various types of measurements

- **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”*



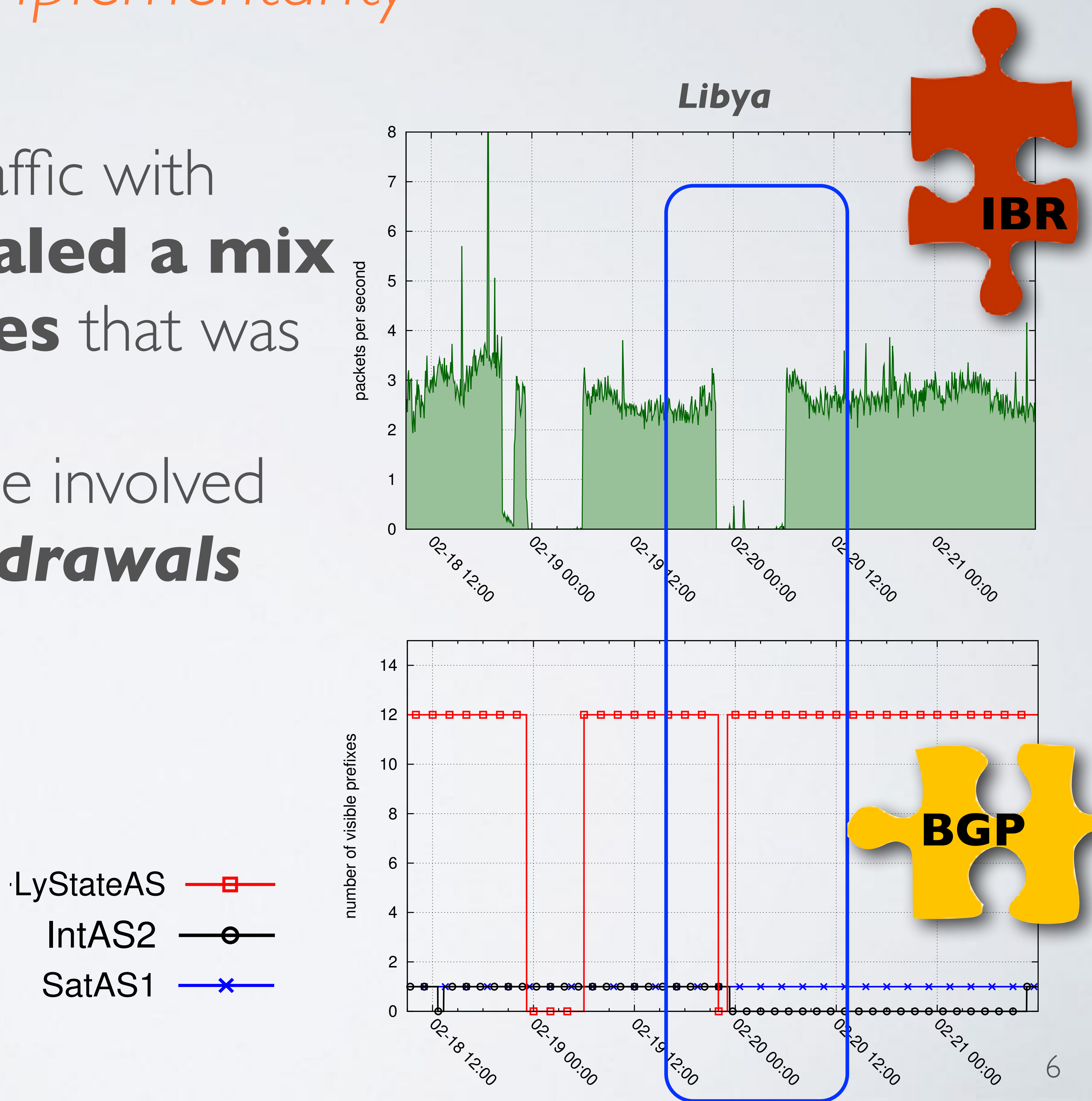
INFECTED HOST
RANDOMLY SCANNING
THE INTERNET

UCSD NETWORK TELESCOPE
DARKNET XXX.0.0.0/8

TELESCOPE + BGP

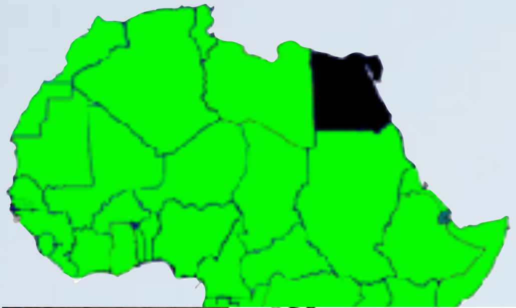
Complementarity

- 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***



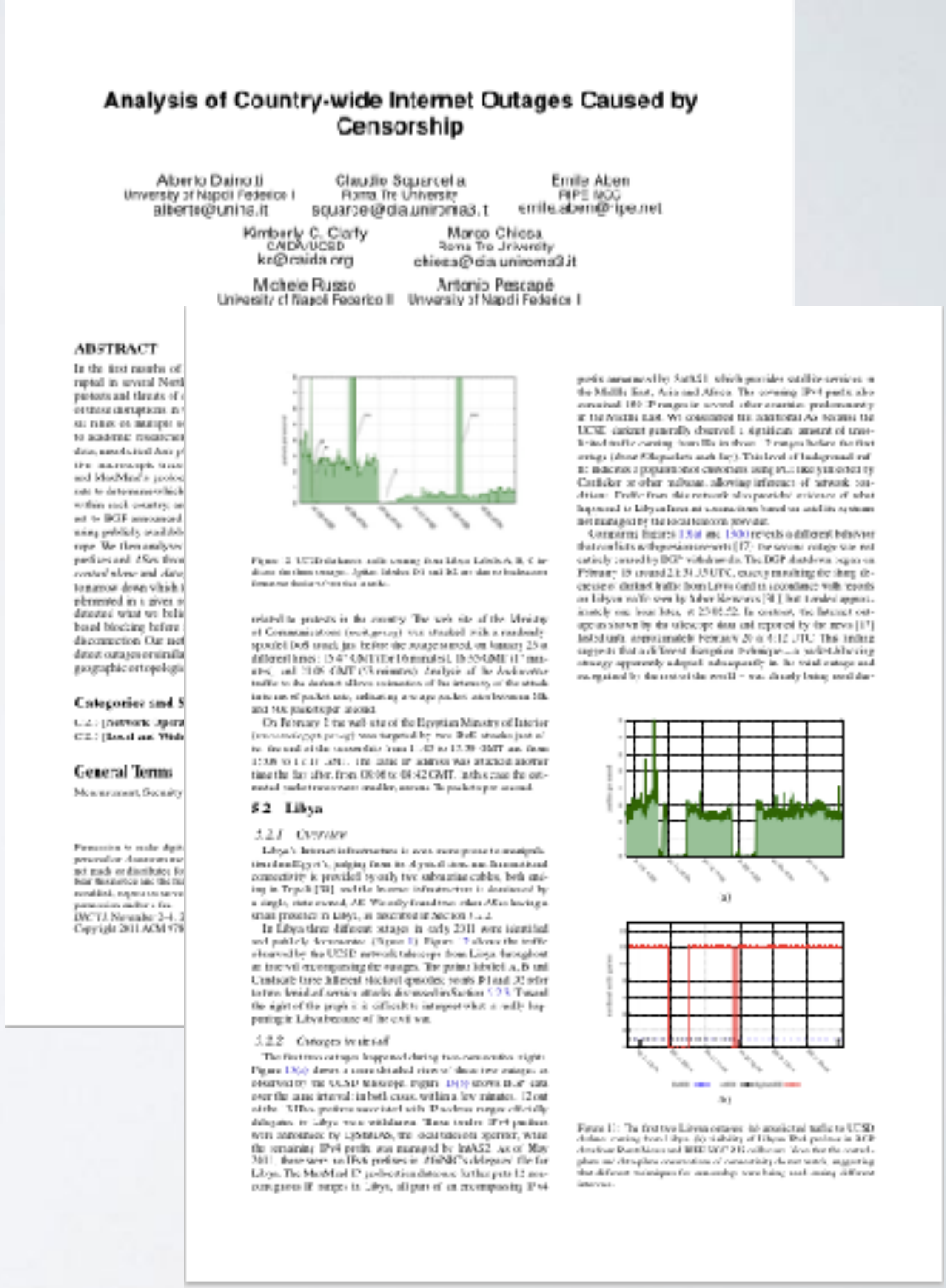
BEFORE IODA

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

Categories and S

General Terms

§2 Libya

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

ABSTRACT

[illegible]

Keywords

Outages, Connectivity Disruption, Censorship, Darknet, Network Telescope, Internet Background Radiation

1 INTRODUCTION

[illegible]

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

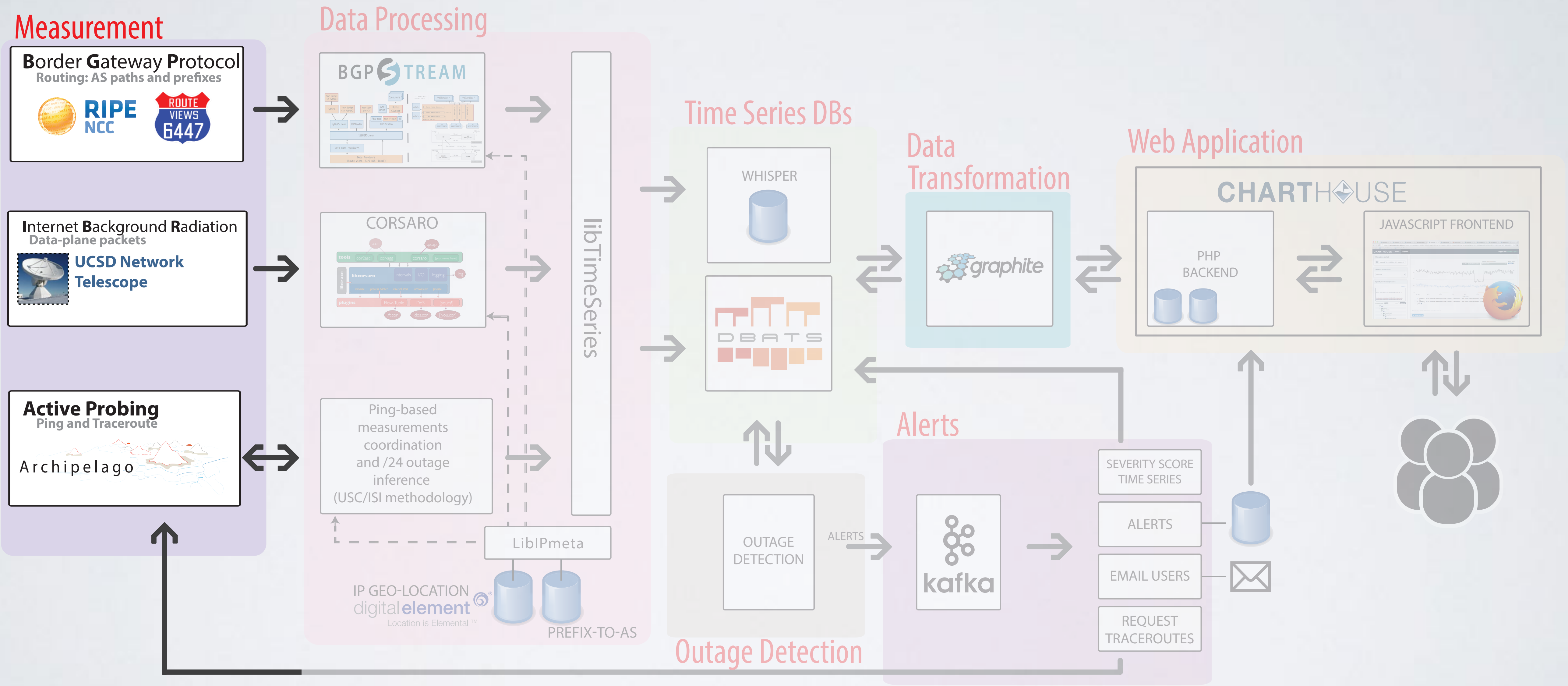
IODA CHALLENGES

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..

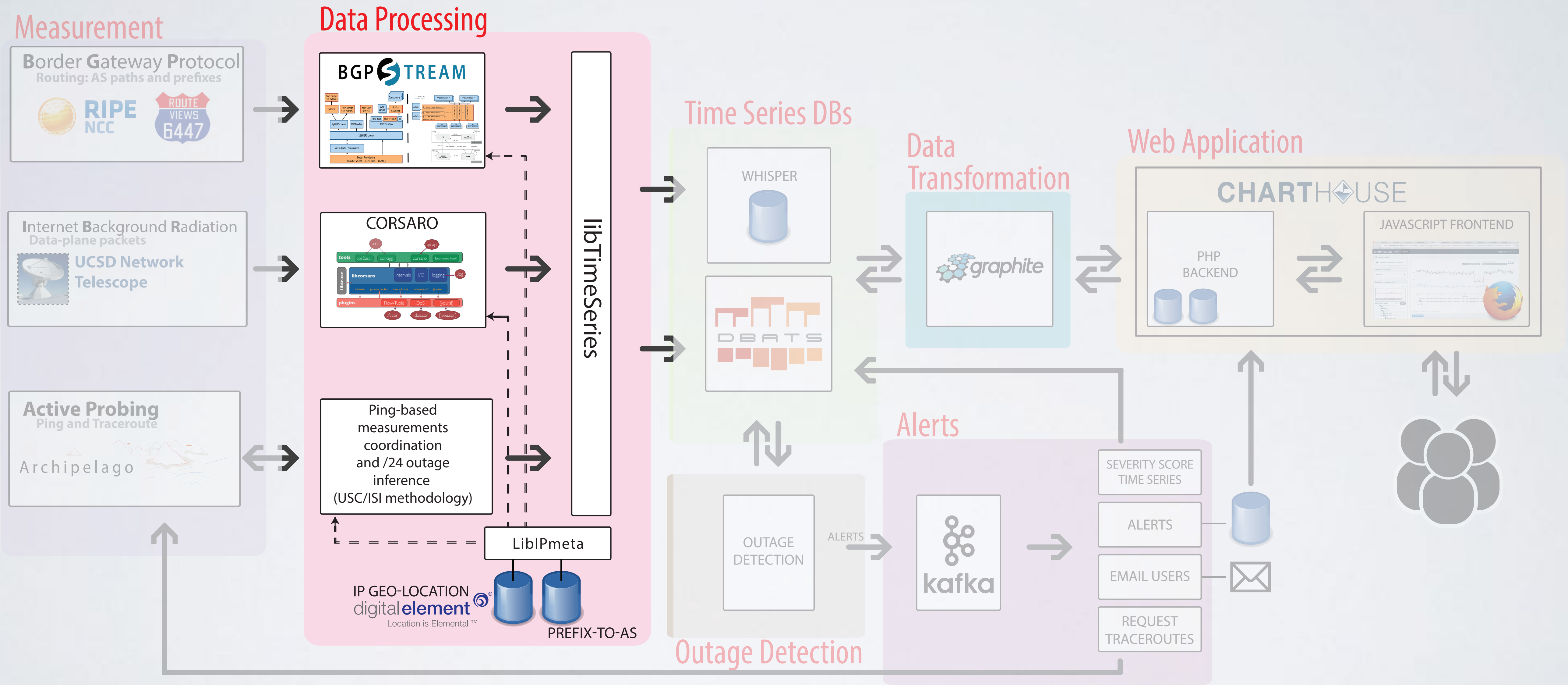
IODA'S CITY MAP

high-level system view



IODA'S CITY MAP

high-level system view



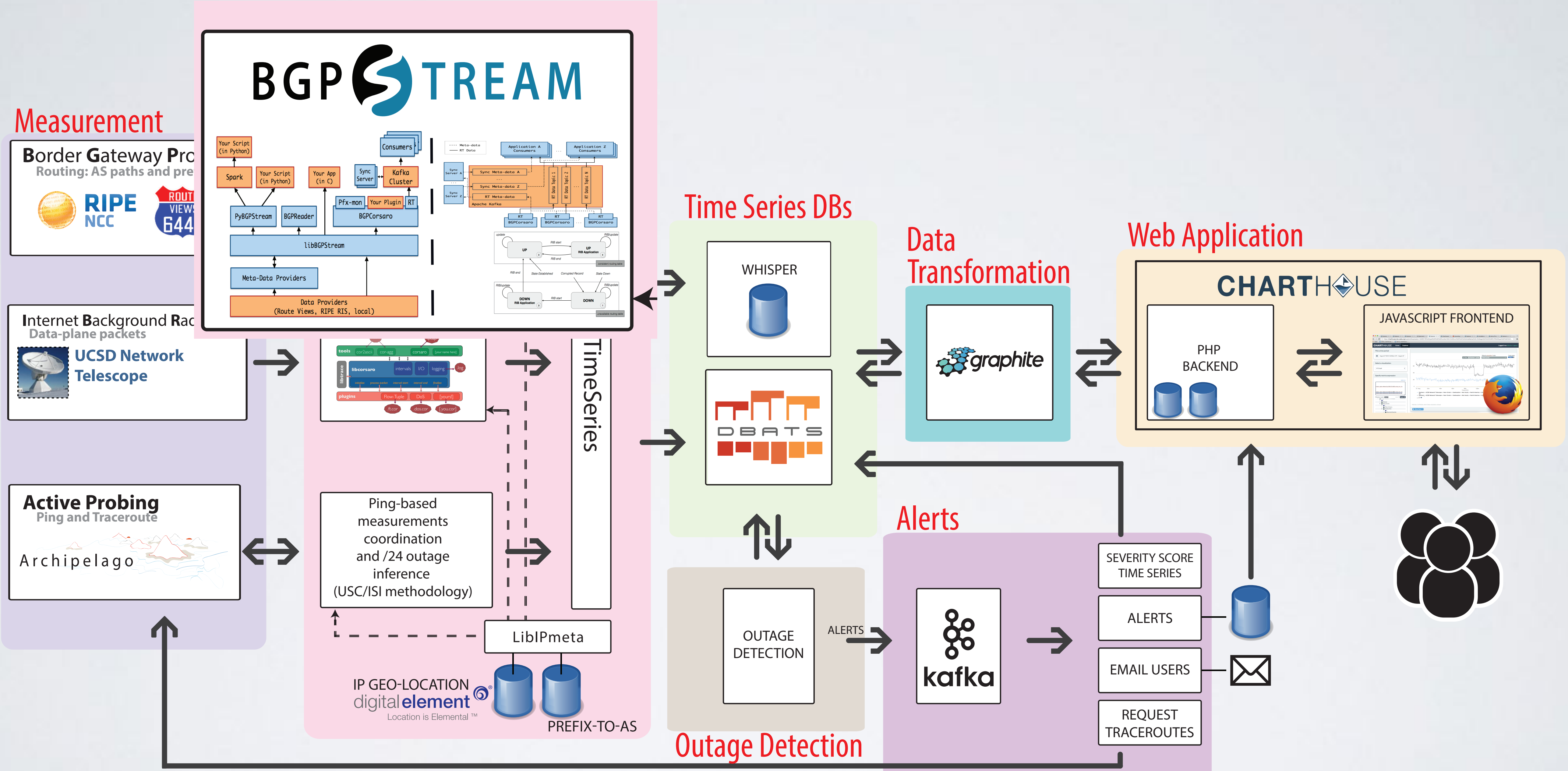
Center for Applied Internet Data Analysis
University of California San Diego

caida

UC San Diego
SDSC
SAN DIEGO SUPERCOMPUTER CENTER

BGPSTREAM

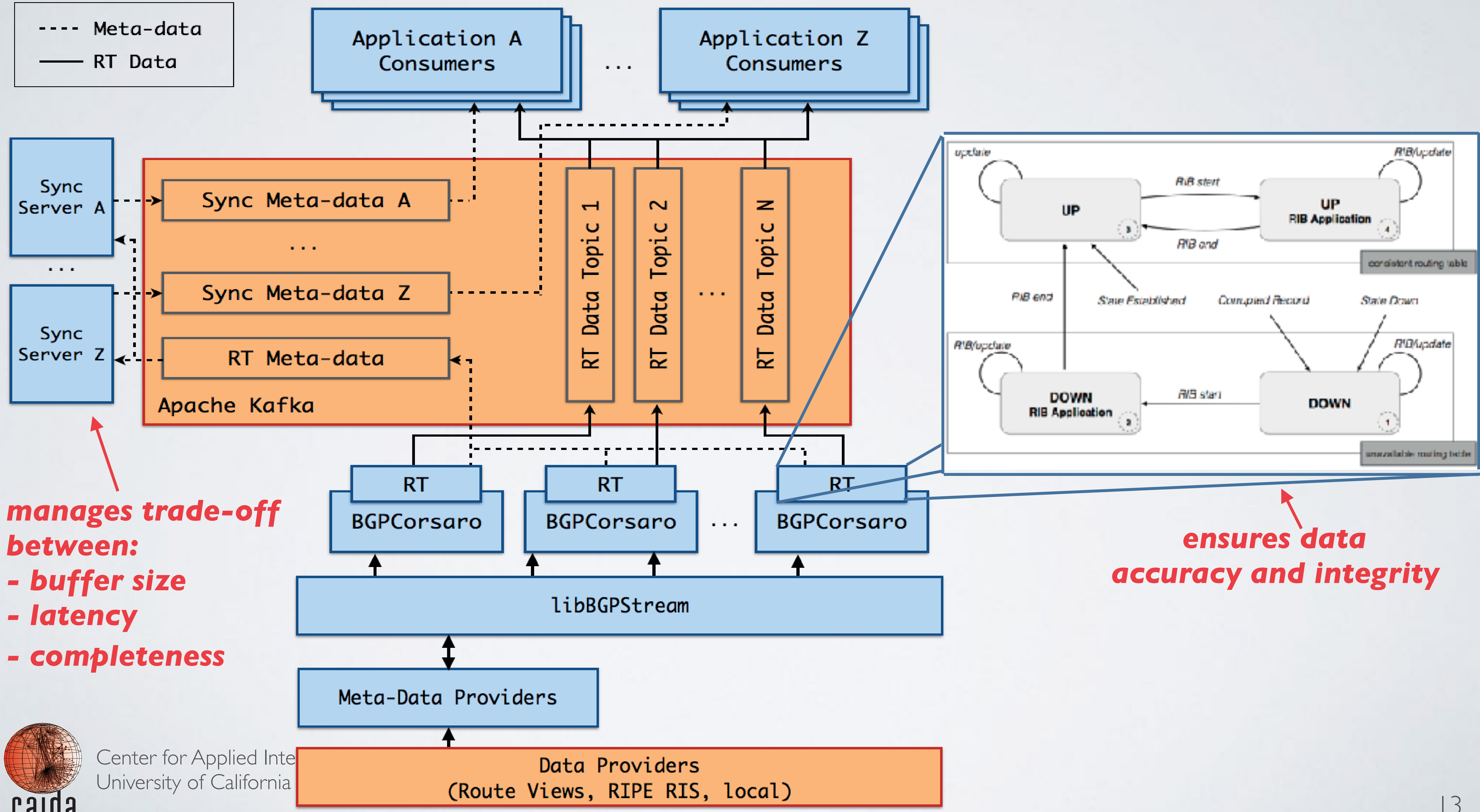
efficient scalable processing of Internet routing data



Center for Applied Internet Data Analysis
University of California San Diego

BGPSTREAM IN IODA

32 BGPCorsaro instances processing data from ~500 routers

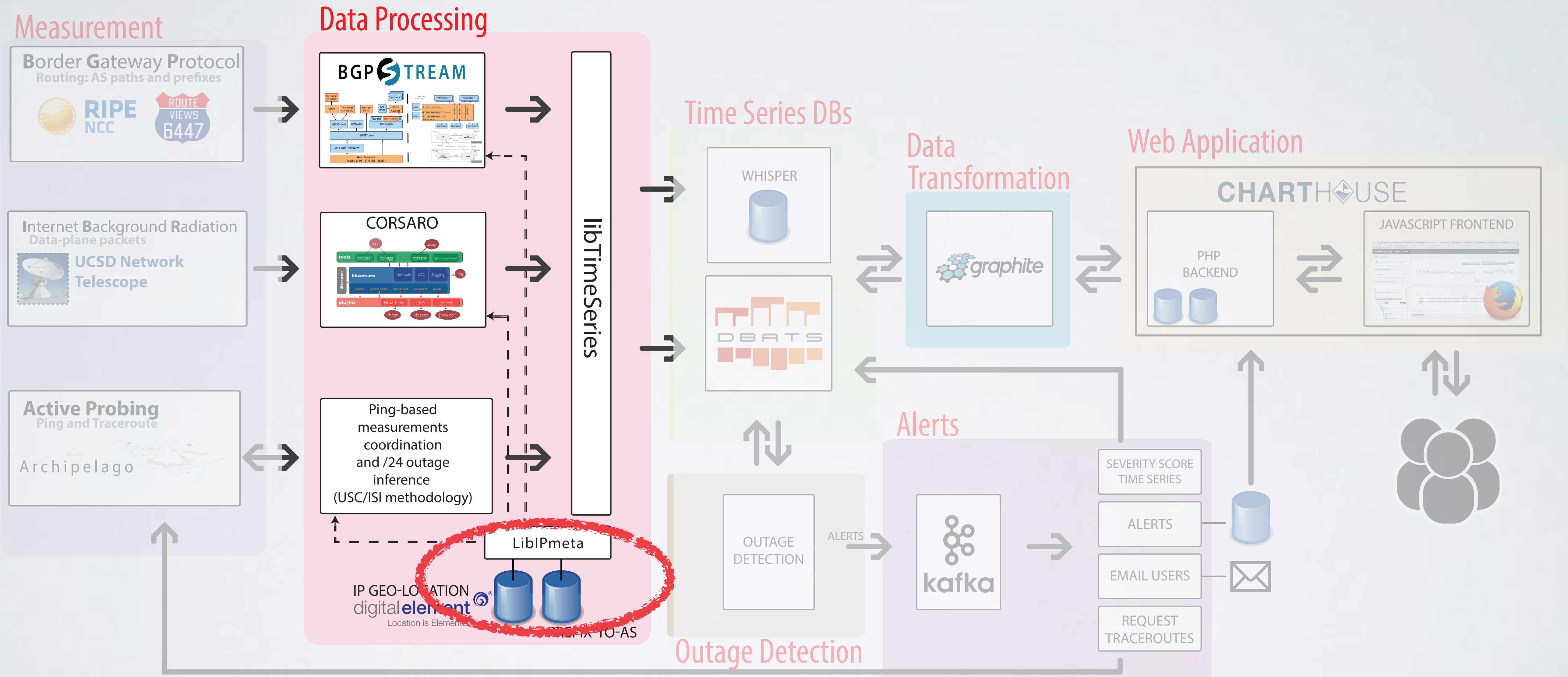


manages trade-off between:
- **buffer size**
- **latency**
- **completeness**

ensures data accuracy and integrity

IODA’S CITY MAP

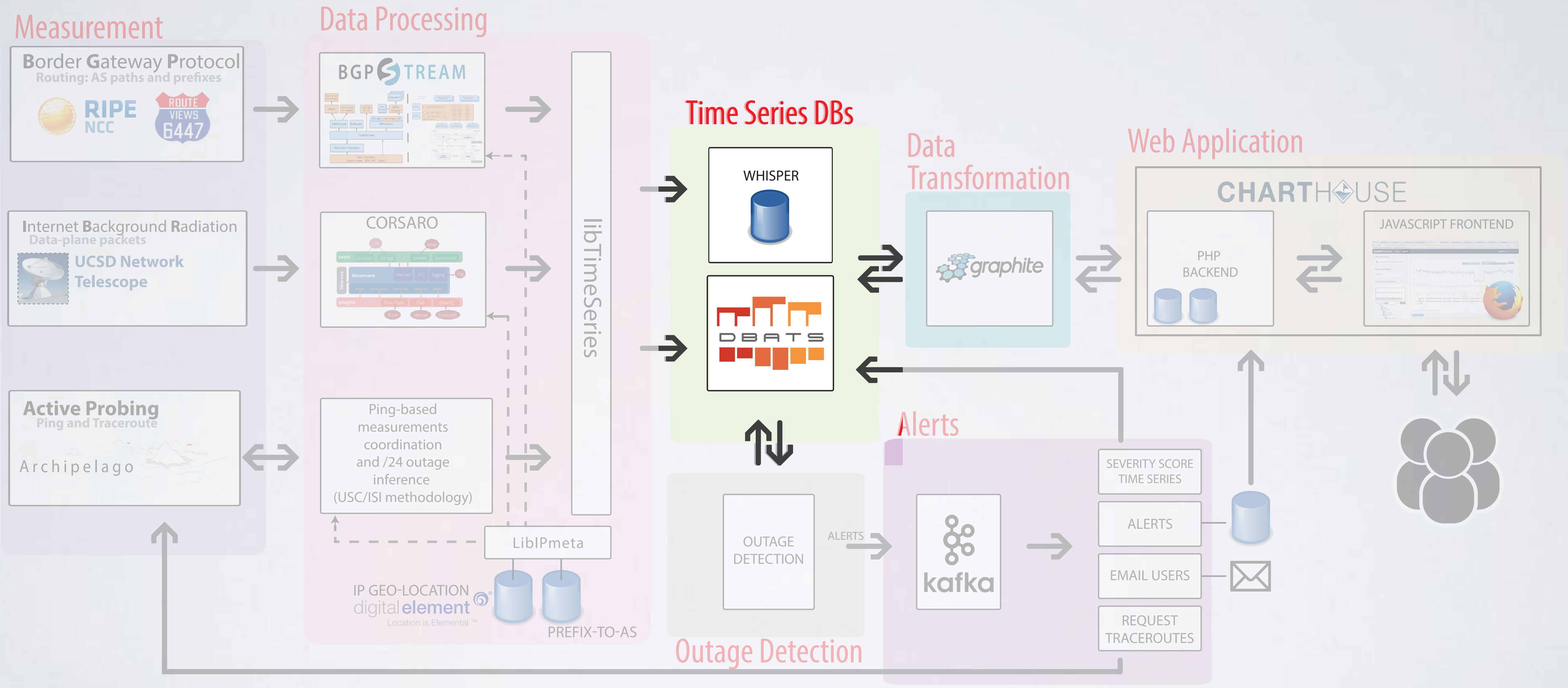
high-level system view



Center for Applied Internet Data Analysis
University of California San Diego

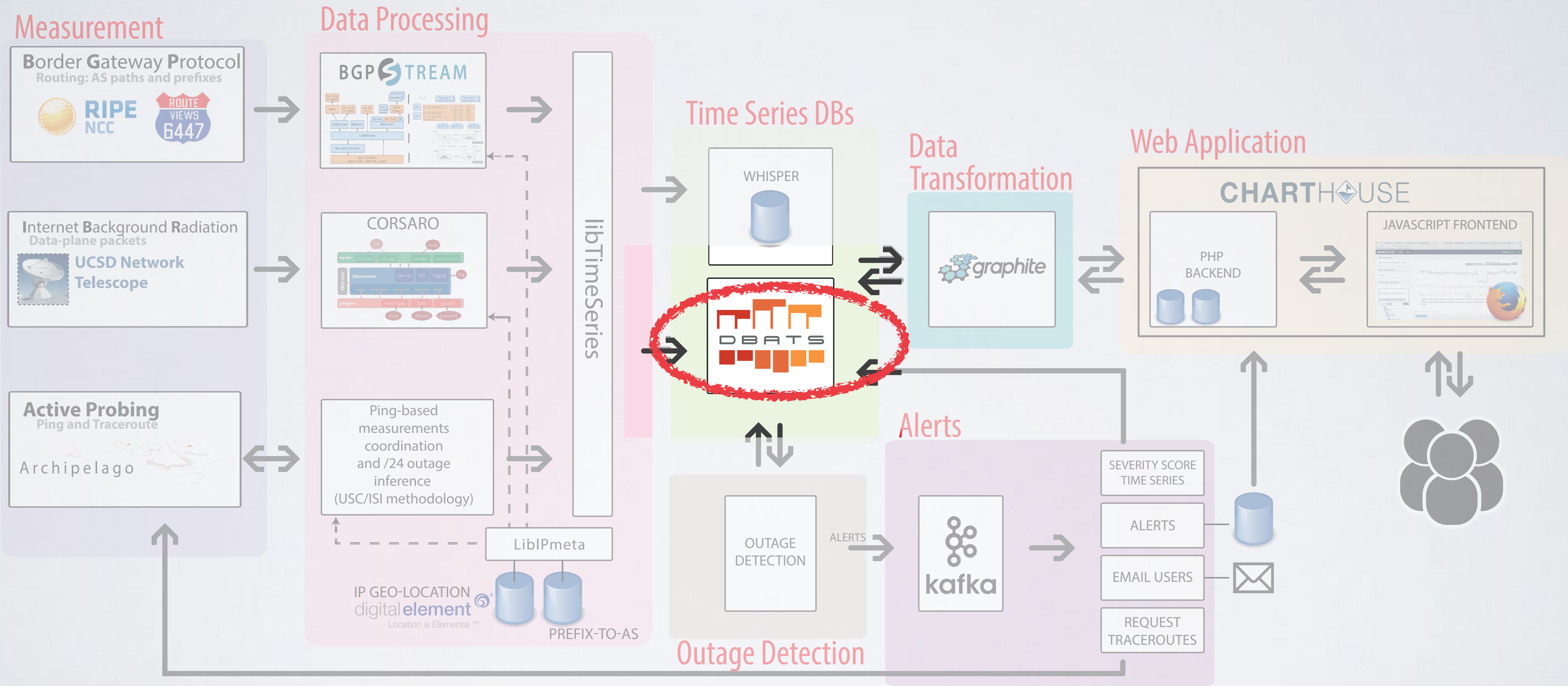
IODA'S CITY MAP

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
digital element
Location is Elemental ™

PREFIX-TO-AS

Time Series DBs

WHISPER

DBATS

Data Transformation

graphite

Web Application

CHARTHOUSE

PHP BACKEND

JAVASCRIPT FRONTEND

Outage Detection

OUTAGE DETECTION

ALERTS

Alerts

kafka

SEVERITY SCORE TIME SERIES

ALERTS

EMAIL USERS

REQUEST TRACEROUTES

Center for Applied Internet Data Analysis
University of California San Diego

caida

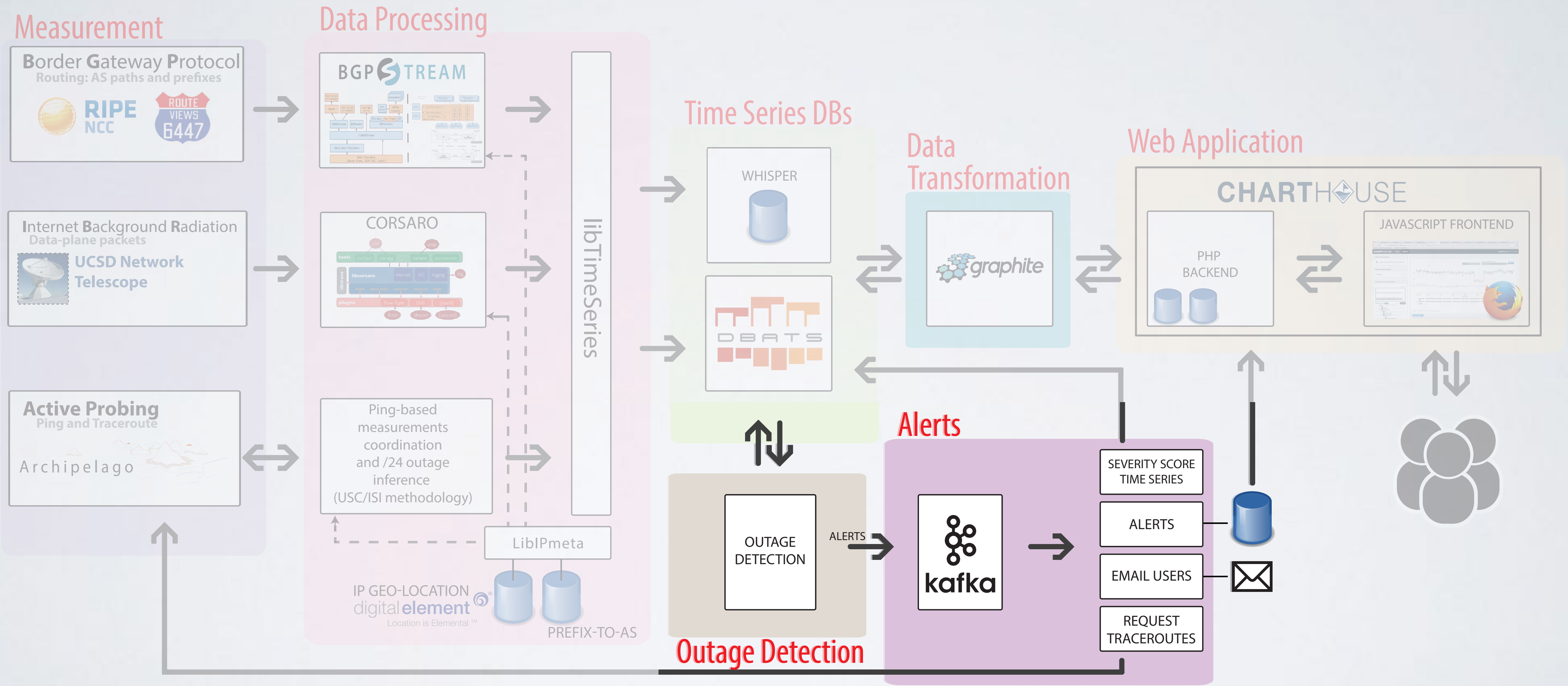
UC San Diego
SDSC
SAN DIEGO SUPERCOMPUTER CENTER

NSF

U.S. DEPARTMENT OF HOMELAND SECURITY

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

Outage Detection

OUTAGE DETECTION

ALERTS

Alerts

kafka

SEVERITY SCORE TIME SERIES

ALERTS

EMAIL USERS

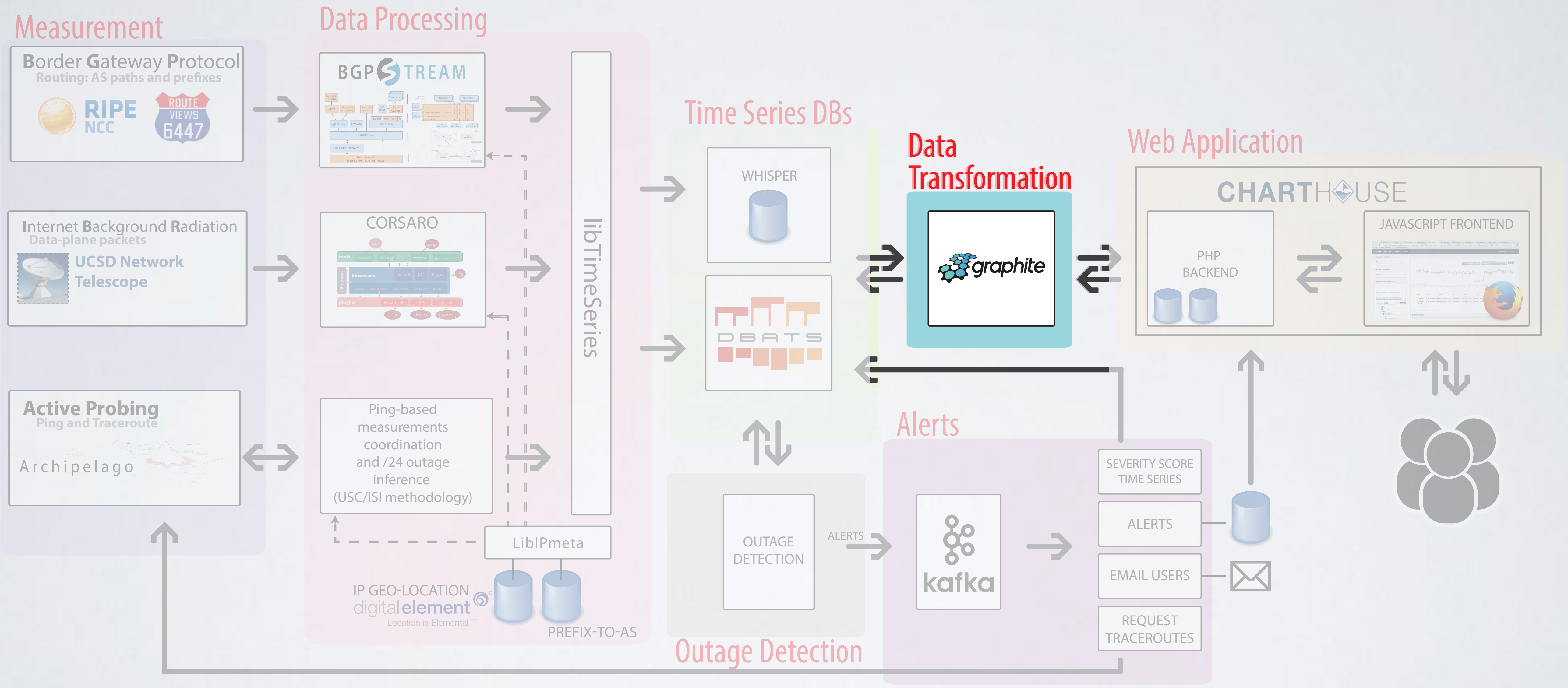
REQUEST TRACEROUTES

Center for Applied Internet Data Analysis
University of California San Diego

UC San Diego
SDSC
SAN DIEGO SUPERCOMPUTER CENTER

IODA'S CITY MAP

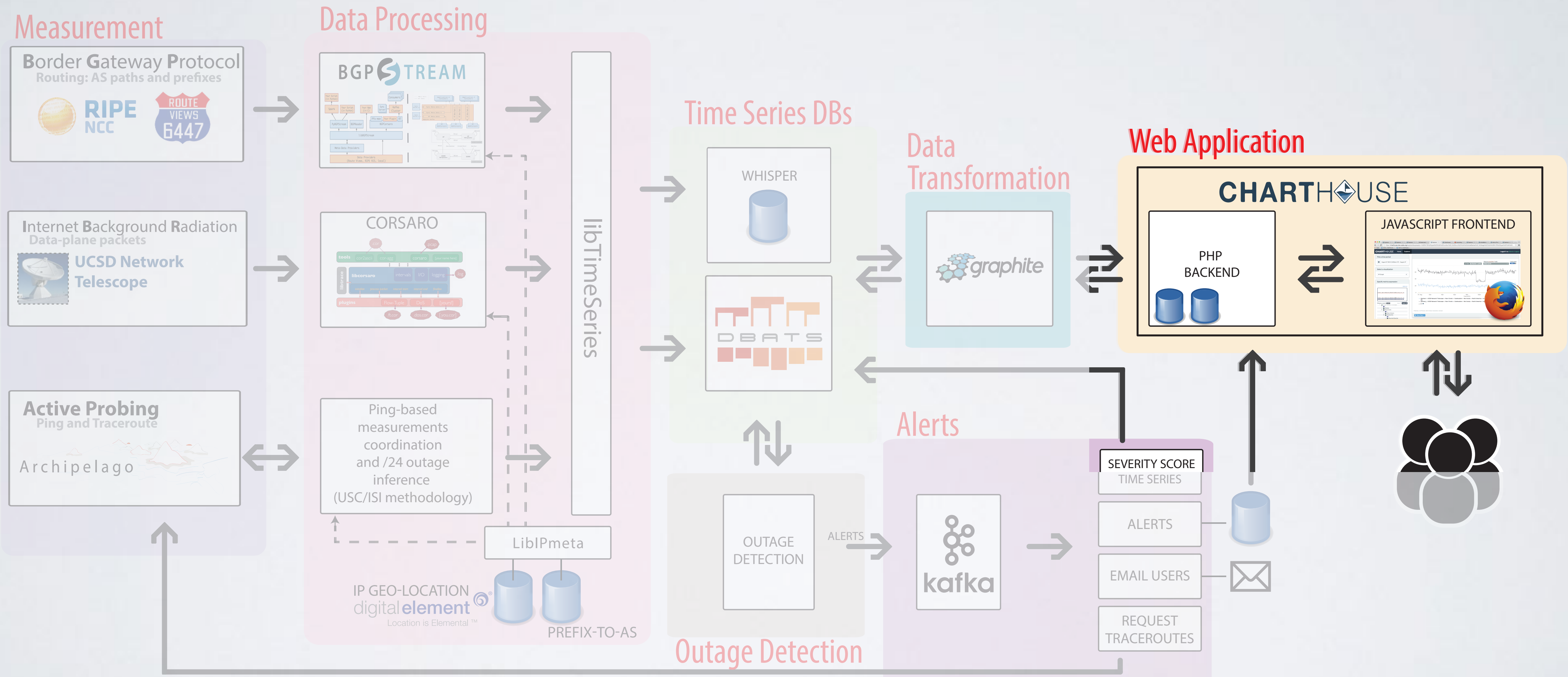
high-level system view



Center for Applied Internet Data Analysis
University of California San Diego

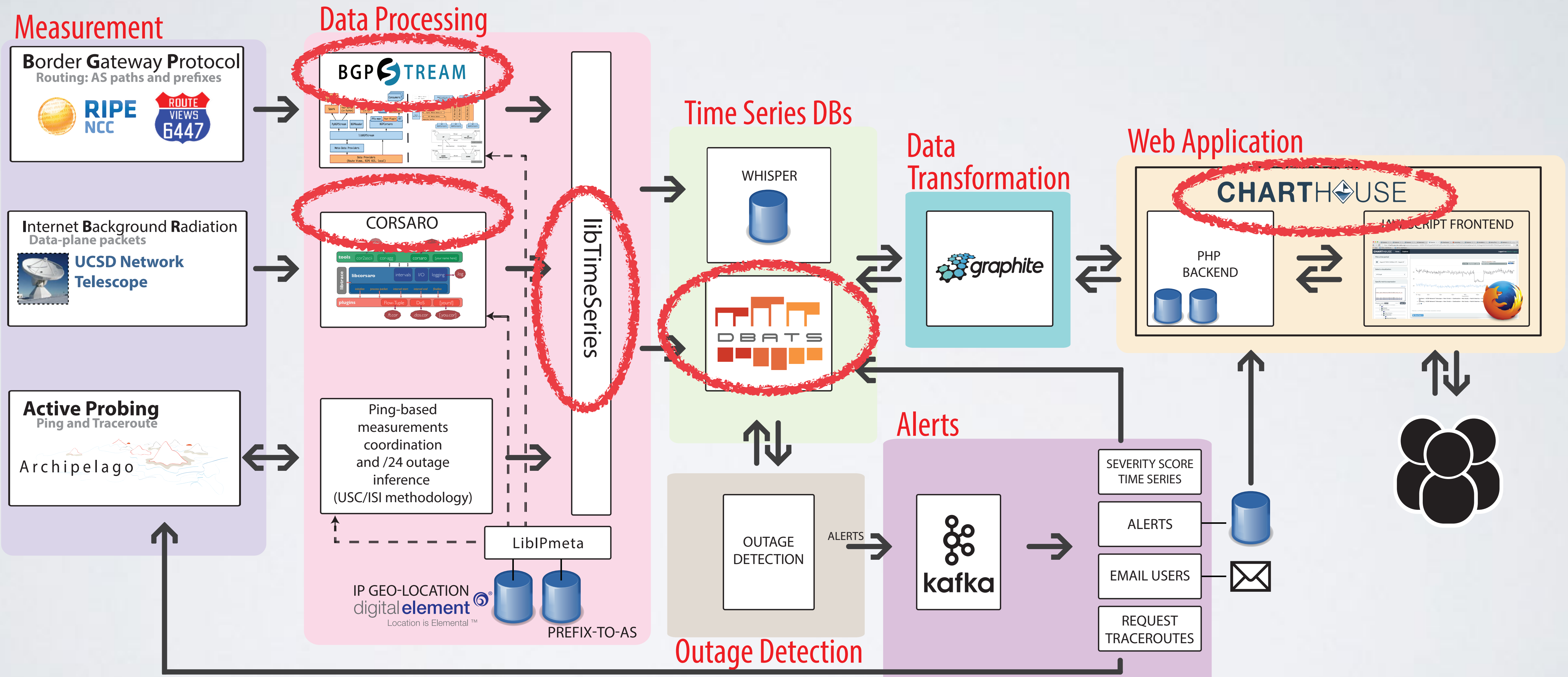
IODA'S CITY MAP

high-level system view

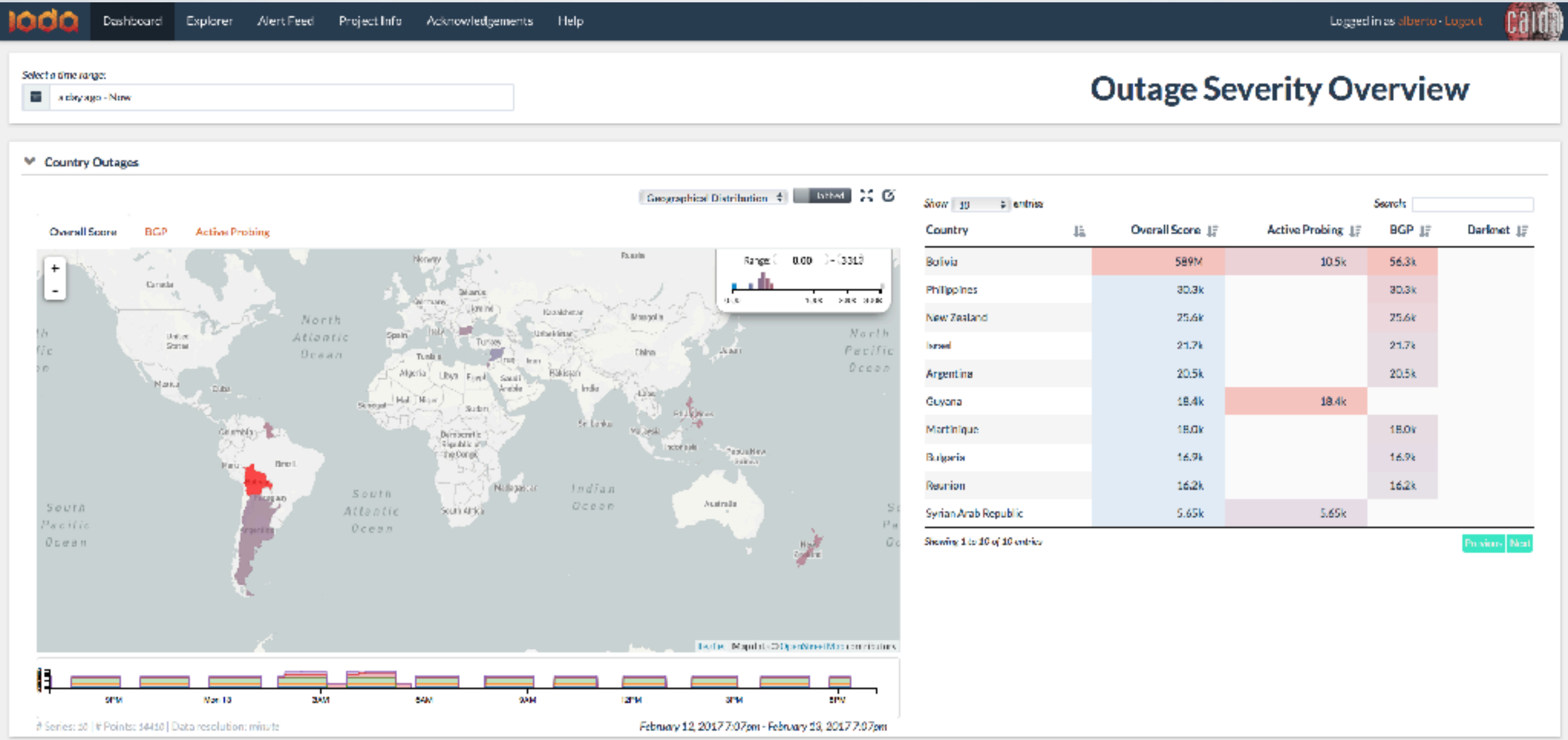


IODA SW SPIN OFFS

open-source frameworks of more general utility



IODA DEMO



Outage Severity Overview

Select a time range: a day ago - Now

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

Series: 10 | # Points: 14410 | Data resolution: minute

February 12, 2017 7:07pm - February 13, 2017 7:07pm

TALK/DEMO PURPOSE

feedback/interest

- Pre-release: use it!
- Collect feedback
- Add other data sources

IODA FUTURE

Ongoing work

- day-to-day maintenance to keep it online
- backfill of historical data
- sw/hw infrastructure updates
- more documentation

- make a kafka stream (we already have it. if you're interested) publicly available and share historical datasets through DHS IMPACT

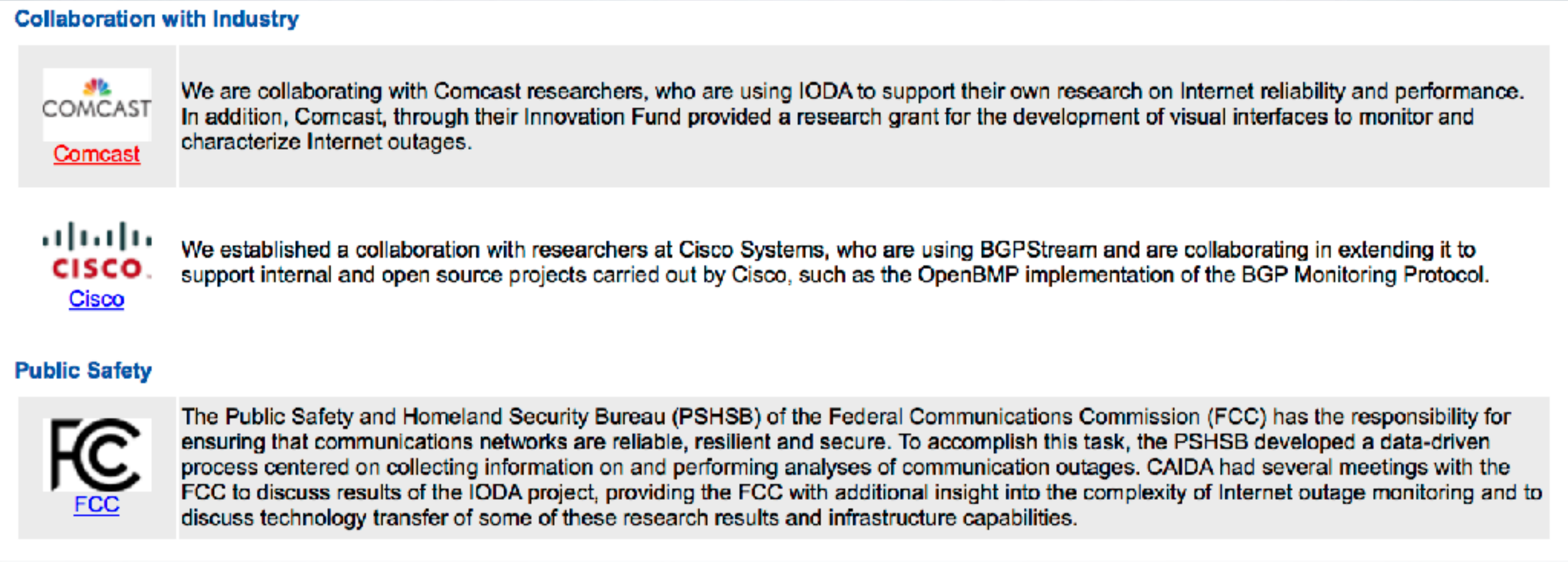
IODA FUTURE

Improvements

- More functionalities in web interface (e.g., add menu selectors of AS/ Country/region)
- Finer geo granularity
  - Engineering + Research (e.g., improve prefix geolocation)
- Reduce latency (IBR, BGP, active probing)
- Improvements to IBR signals
  - clean up
  - detection
  - systematically validate / evaluate IBR detection (we started at country level)
- IPv6 support

ONGOING COLLABS

Academia, Industry, Government



Collaboration with Industry

COMCAST Comcast	We are collaborating with Comcast researchers, who are using IODA to support their own research on Internet reliability and performance. In addition, Comcast, through their Innovation Fund provided a research grant for the development of visual interfaces to monitor and characterize Internet outages.
CISCO Cisco	We established a collaboration with researchers at Cisco Systems, who are using BGPStream and are collaborating in extending it to support internal and open source projects carried out by Cisco, such as the OpenBMP implementation of the BGP Monitoring Protocol.

Public Safety

FC FCC	The Public Safety and Homeland Security Bureau (PSHSB) of the Federal Communications Commission (FCC) has the responsibility for ensuring that communications networks are reliable, resilient and secure. To accomplish this task, the PSHSB developed a data-driven process centered on collecting information on and performing analyses of communication outages. CAIDA had several meetings with the FCC to discuss results of the IODA project, providing the FCC with additional insight into the complexity of Internet outage monitoring and to discuss technology transfer of some of these research results and infrastructure capabilities.

- Also, research collaborations with networking and poli-sci researchers

IODA FUTURE

Collabs

- Work with John to validate our ``Trinocular" implementation and maybe integrate his data source
- Work with Neil + Rama on combining the *micro* view with the *macro* view
- Add other data sources (Merit, VNG, …)

THANKS

ioda.caida.org

www.caida.org/projects/ioda