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*

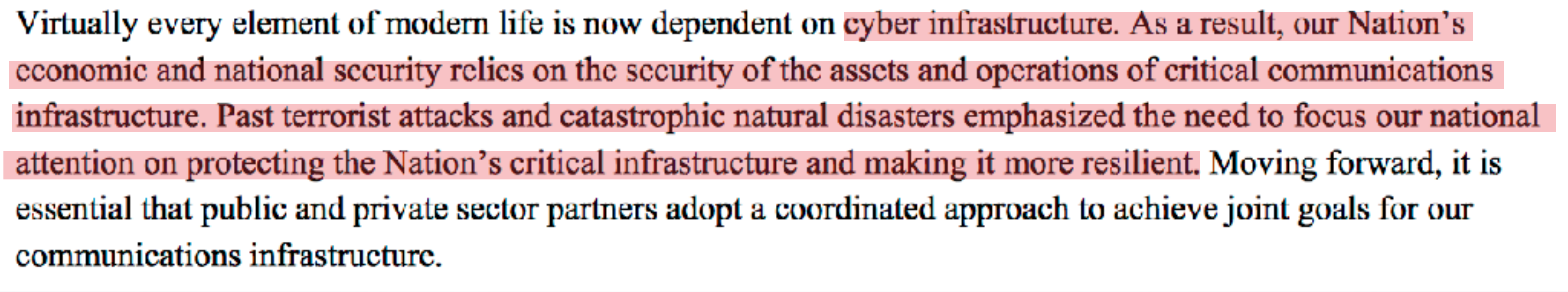
- Potential causes: *natural disasters, cyber attacks, physical attacks (terrorism, war, …), bugs and misconfigurations, government orders, …*

INTERNET OUTAGES

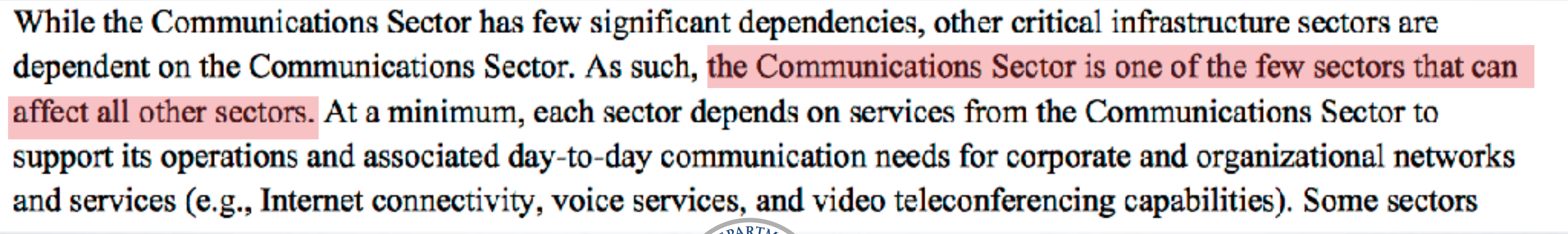
why so relevant?

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 essential that public and private sector partners adopt a coordinated approach to achieve joint goals for our communications infrastructure.



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

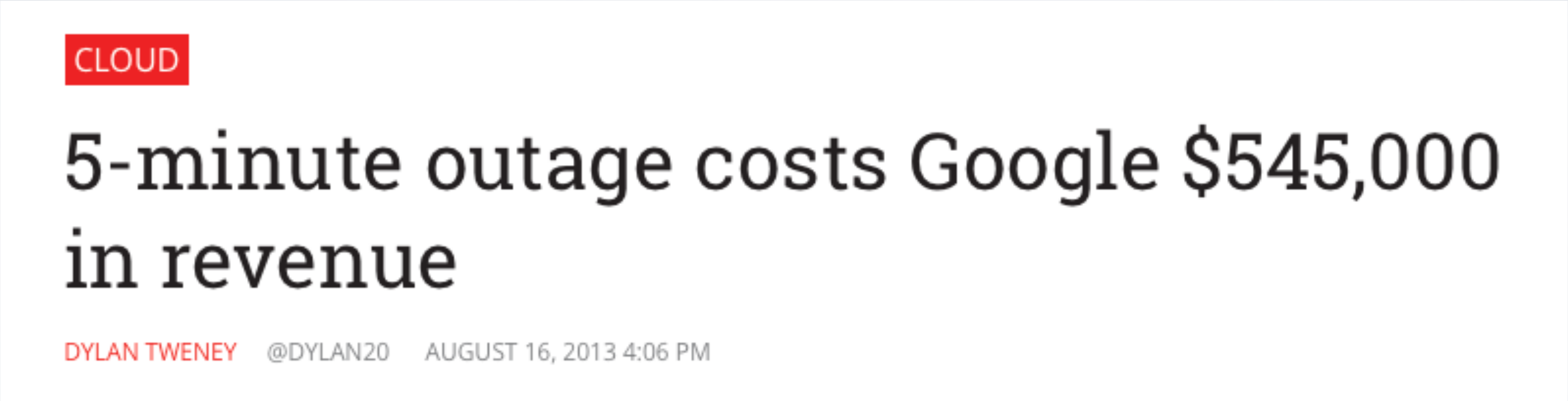
US Department of Homeland Security,
National Infrastructure Protection Plan (NIPP) 2013

INTERNET OUTAGES

why so relevant?

Financial and reputational costs

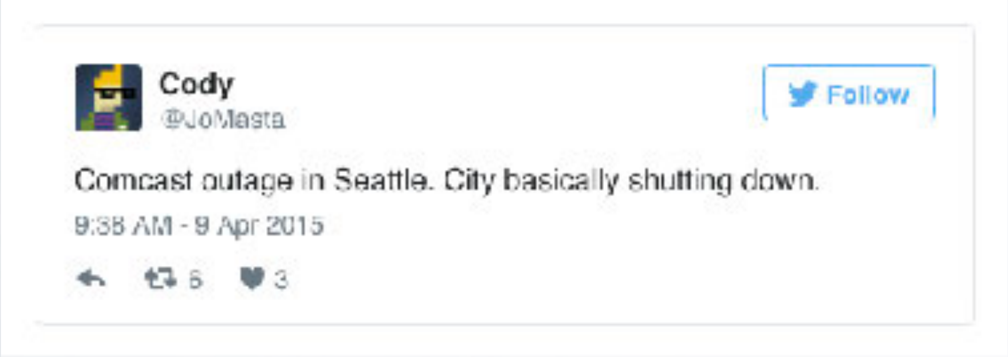
Services are meant to be always on



CLOUD

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

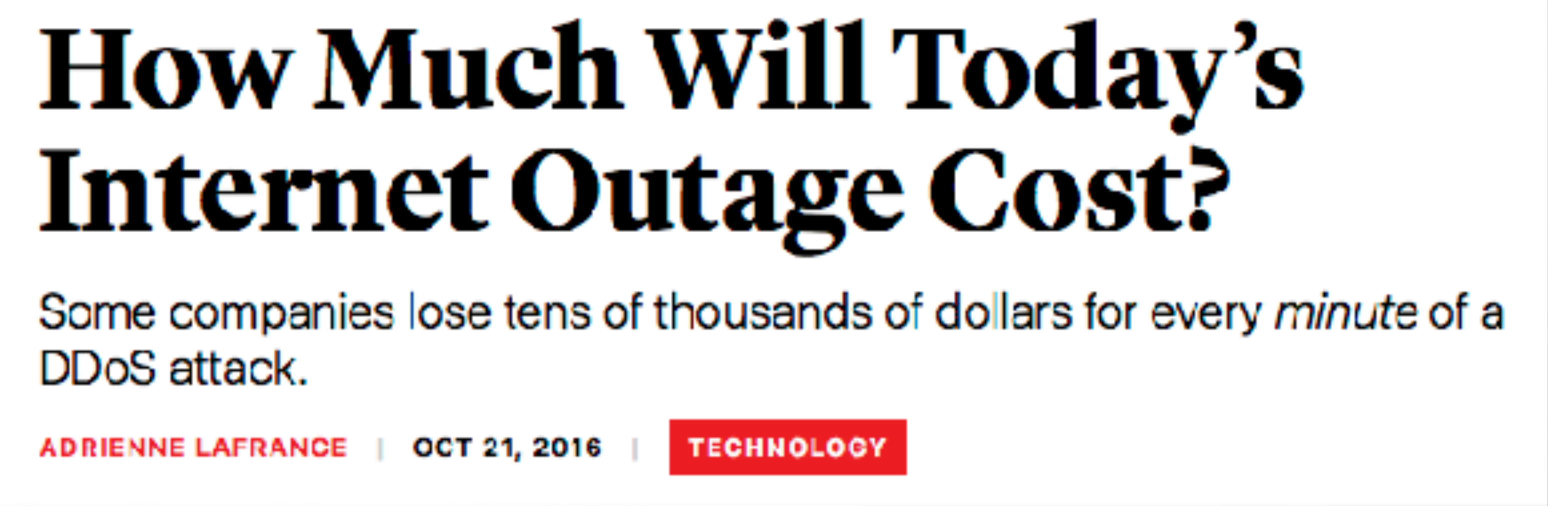
DYLAN TWENEY @DYLAN20 AUGUST 16, 2013 4:06 PM



Cody
@JoMasta

Comcast outage in Seattle. City basically shutting down.

9:38 AM - 9 Apr 2015



How Much Will Today's Internet Outage Cost?

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

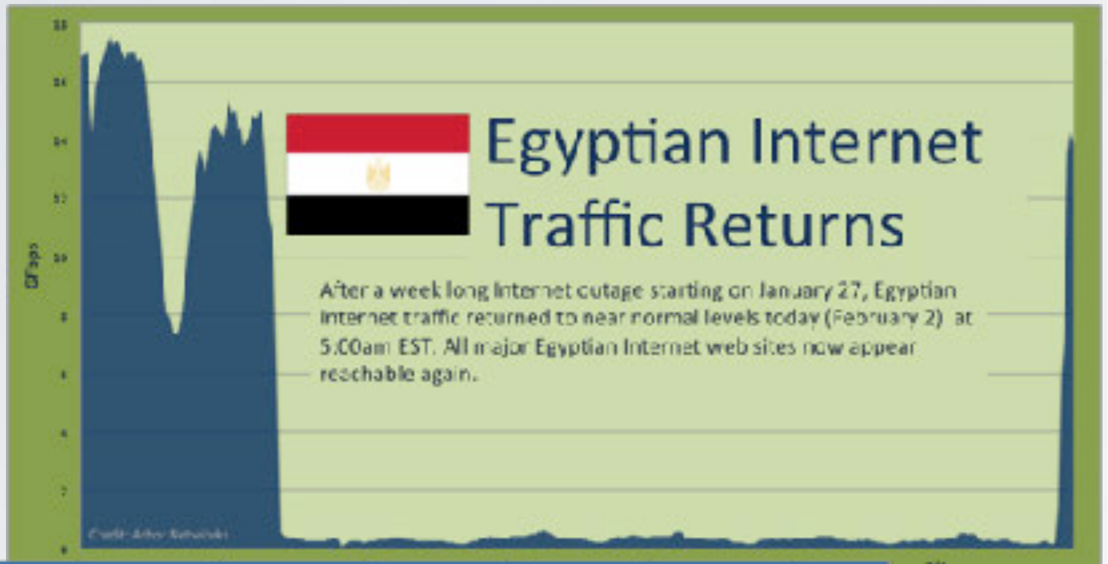
ADRIENNE LAFRANCE | OCT 21, 2016 | TECHNOLOGY

INTERNET OUTAGES

why so relevant?

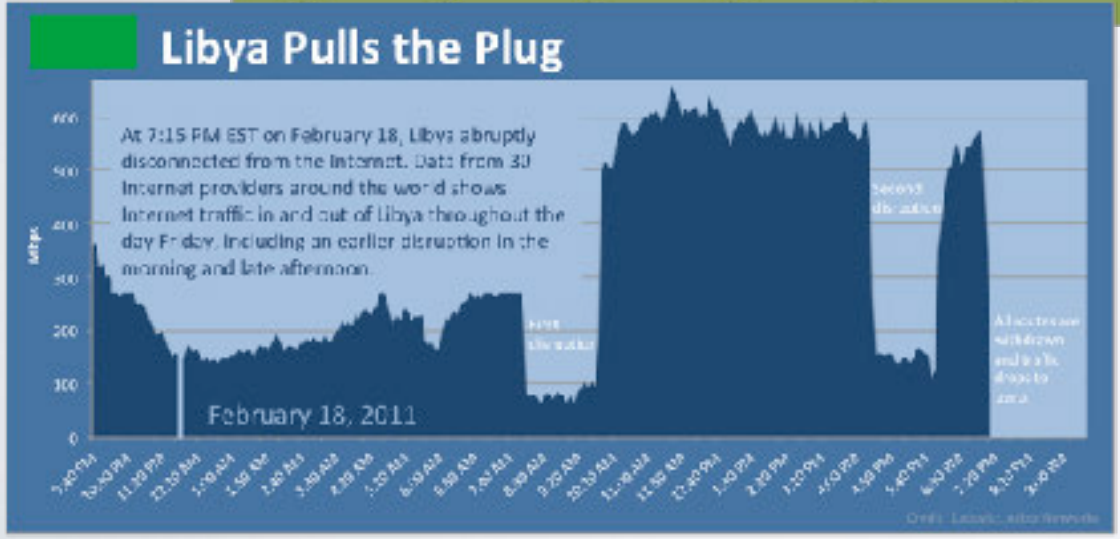
Human Rights

censorship and political violence



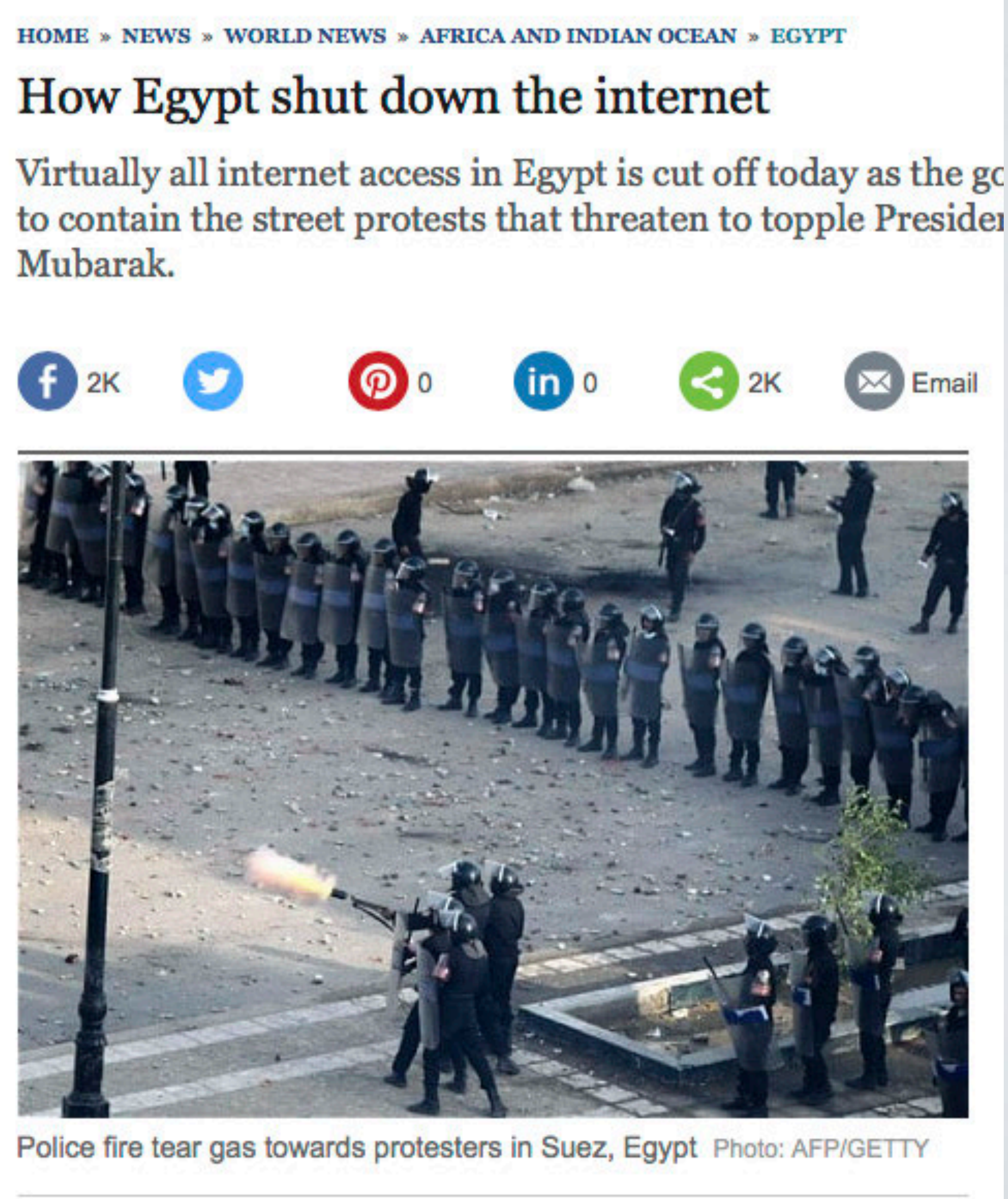
Egyptian Internet Traffic Returns

After a week long Internet outage starting on January 27, Egyptian Internet traffic returned to near normal levels today (February 2) at 5:00am EST. All major Egyptian Internet web sites now appear reachable again.



Libya Pulls the Plug

At 7:15 PM EST on February 18, Libya abruptly disconnected from the Internet. Data from 30 Internet providers around the world shows Internet traffic in and out of Libya throughout the day Friday, including an earlier disruption in the morning and late afternoon.



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 Presiden
Mubarak.

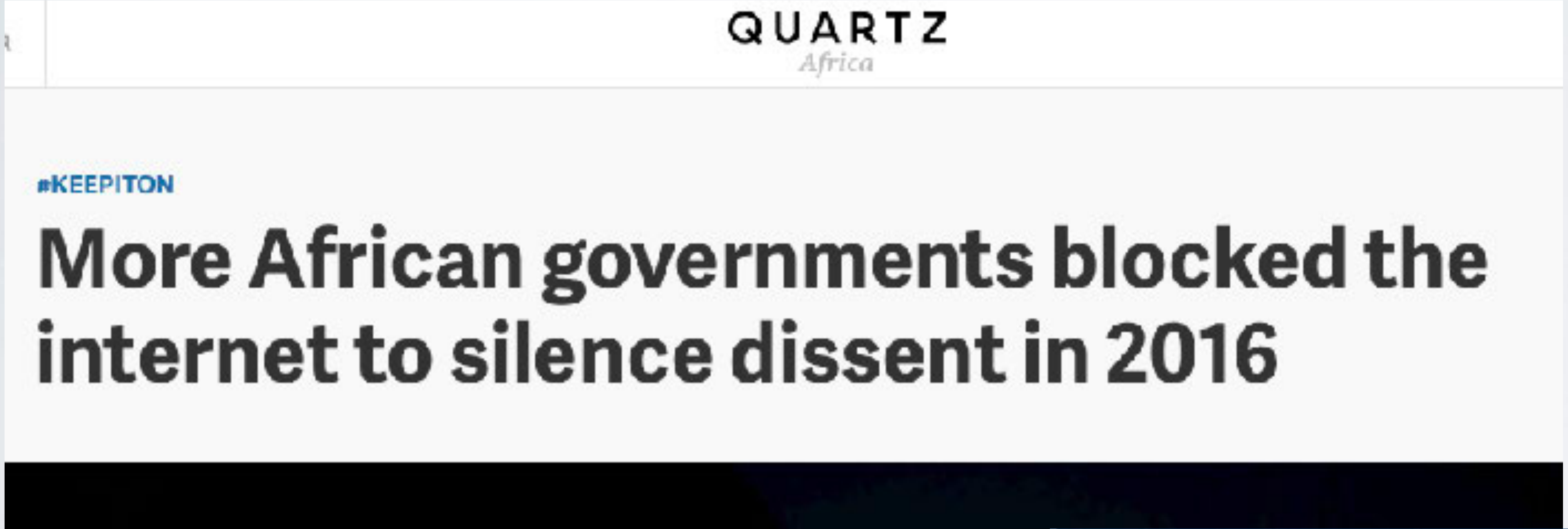
Police fire tear gas towards protesters in Suez, Egypt Photo: AFP/GETTY

INTERNET OUTAGES

why so relevant?

Human Rights

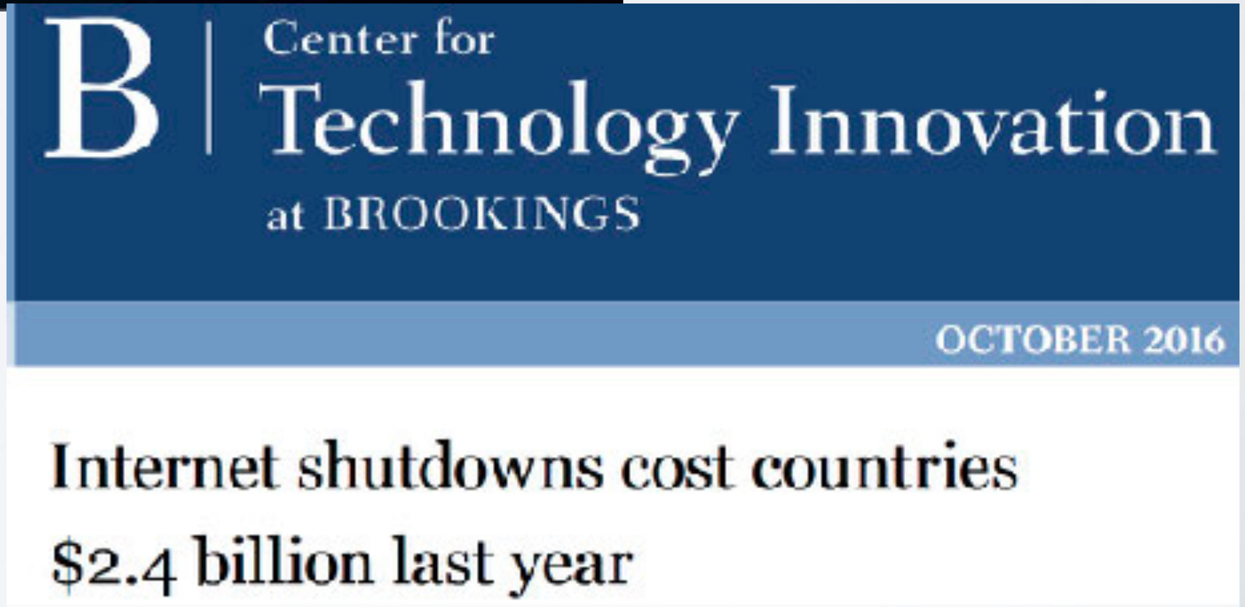
censorship and political violence



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

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

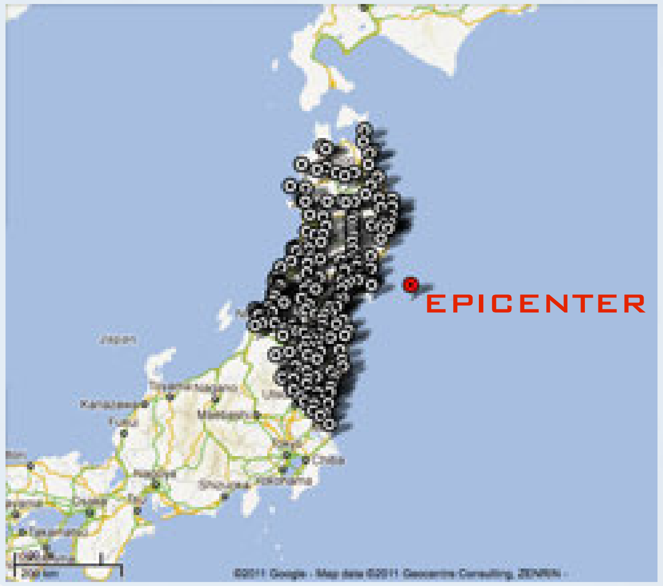
- Country-level Internet Blackouts during the Arab Spring

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

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

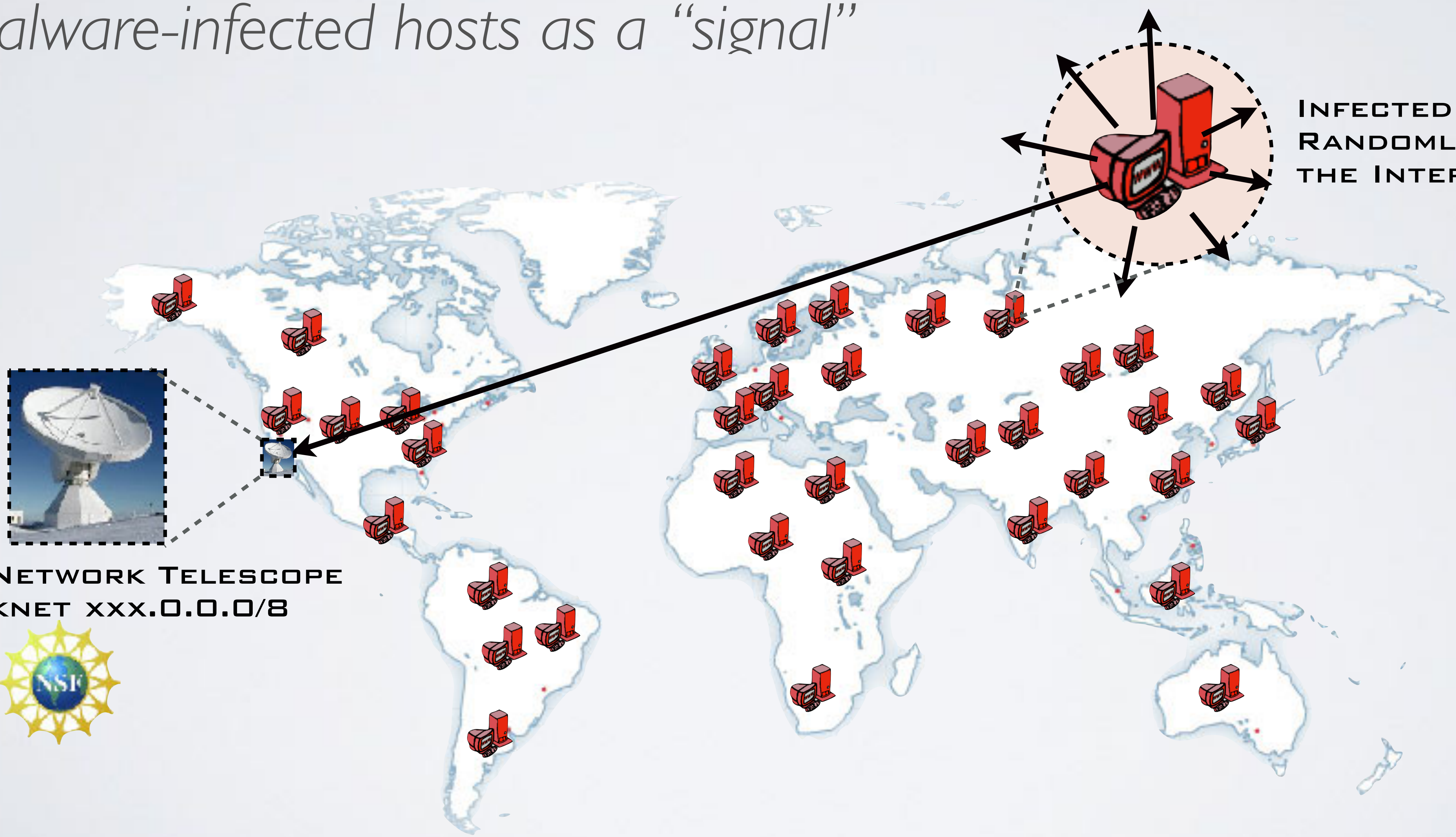
...
BGP
IBR
ACTIVE PROBING

- **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"*



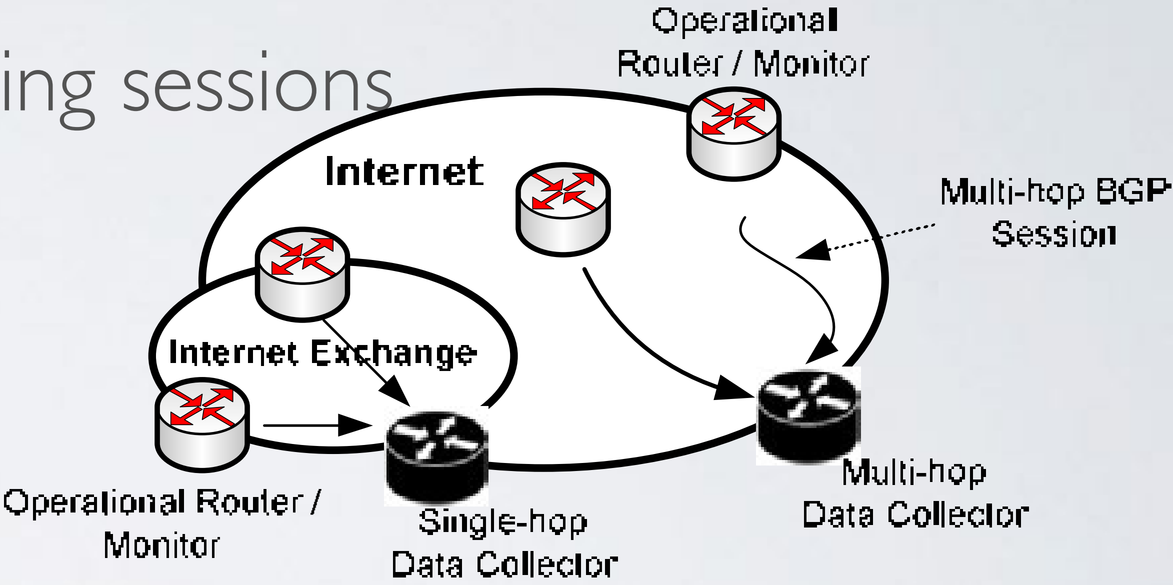
INFECTED HOST RANDOMLY SCANNING THE INTERNET

UCSD NETWORK TELESCOPE
DARKNET xxx.0.0.0/8

BGP

*Monitoring Global Internet **Routing***

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


Operational Router / Monitor
Internet
Multi-hop BGP Session
Internet Exchange
Operational Router / Monitor
Single-hop Data Collector
Multi-hop Data Collector

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

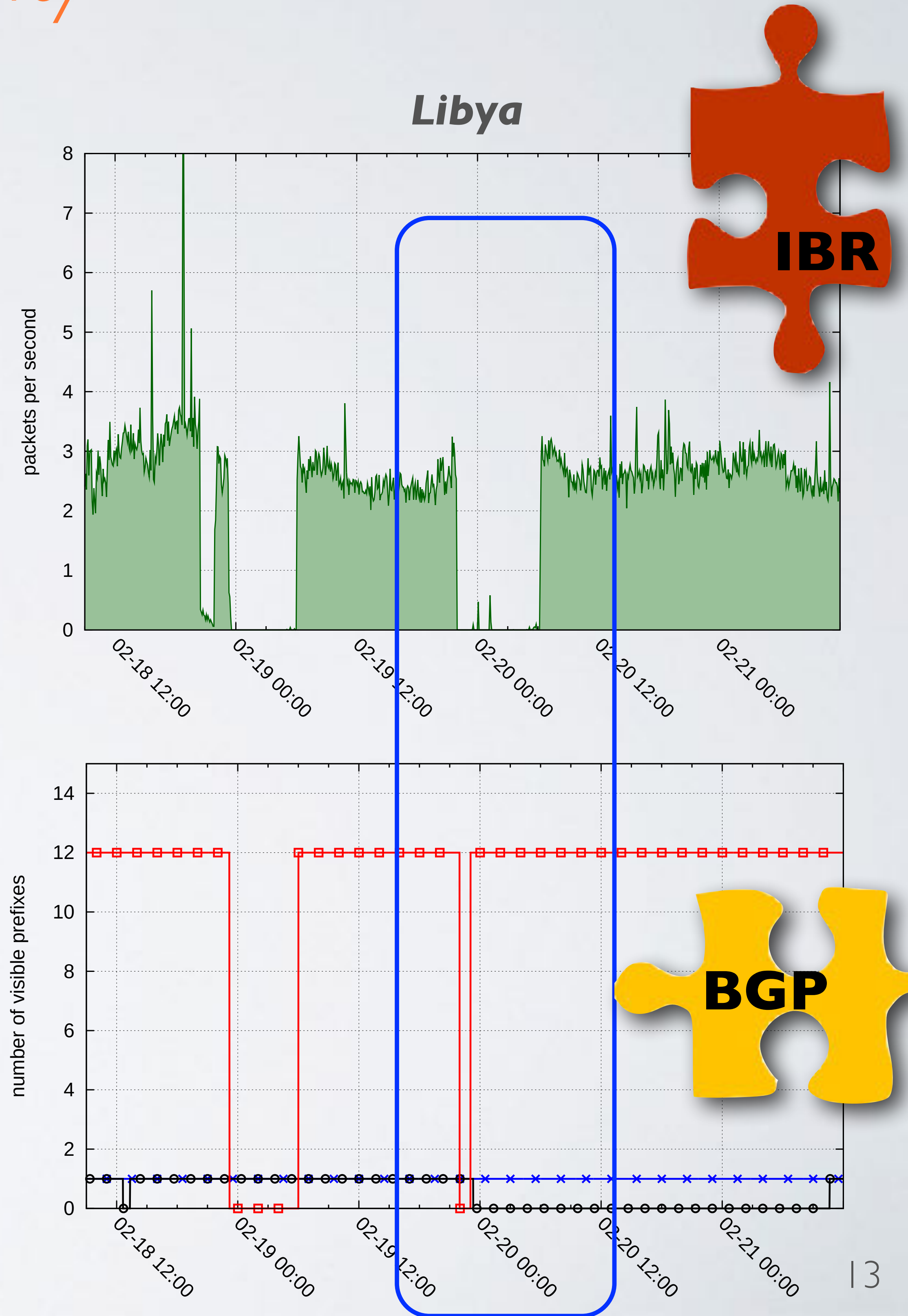
http://www.routeviews.org

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

TELESCOPE + BGP

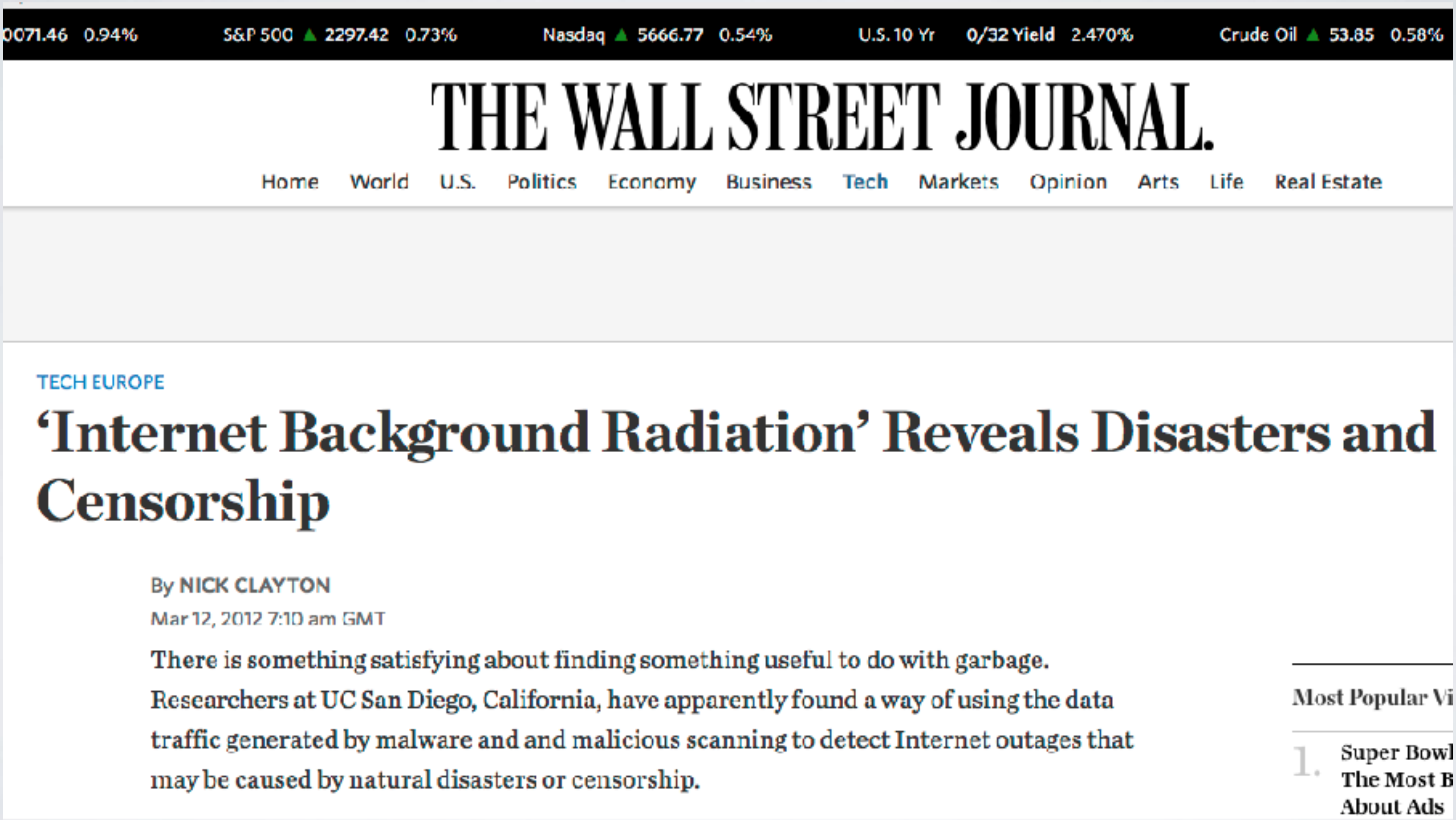
Complementarity

- 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

hitting the news



THE WALL STREET JOURNAL.

TECH EUROPE

‘Internet Background Radiation’ Reveals Disasters and Censorship

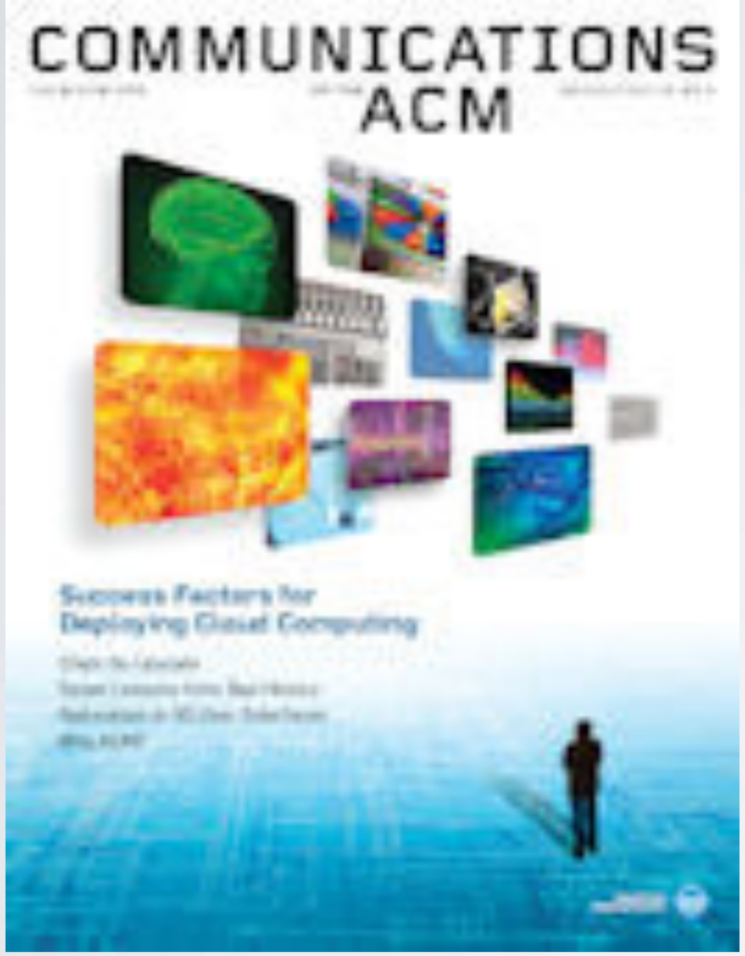
By NICK CLAYTON

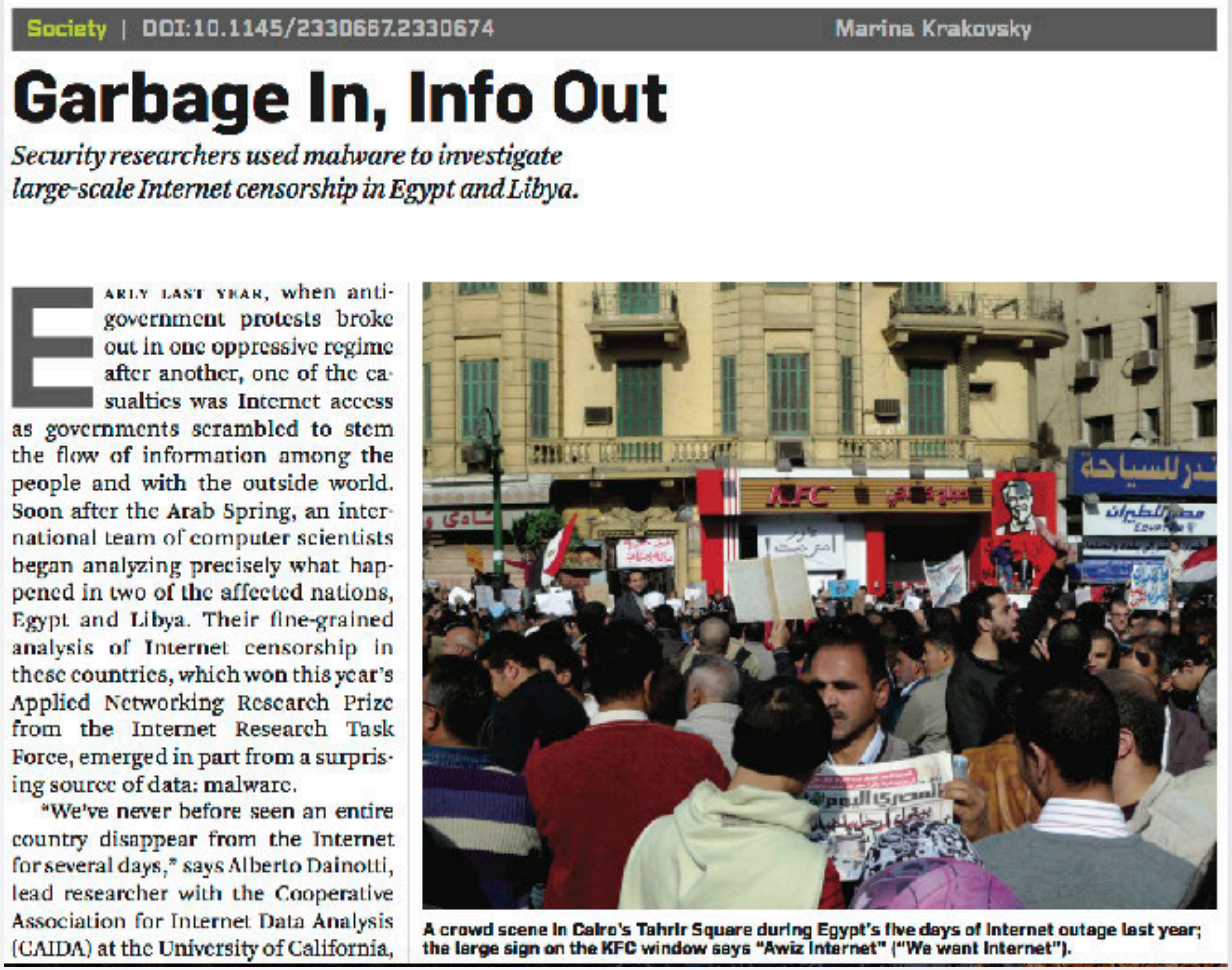
Mar 12, 2012 7:10 am GMT

There is something satisfying about finding something useful to do with garbage. Researchers at UC San Diego, California, have apparently found a way of using the data traffic generated by malware and and malicious scanning to detect Internet outages that may be caused by natural disasters or censorship.

BEFORE IODA

hitting the news





Society | DOI:10.1145/2330667.2330674

Marina Krakovsky

Garbage In, Info Out

Security researchers used malware to investigate large-scale Internet censorship in Egypt and Libya.

EARLY LAST YEAR, when anti-government protests broke out in one oppressive regime after another, one of the casualties was Internet access as governments scrambled to stem the flow of information among the people and with the outside world. Soon after the Arab Spring, an international team of computer scientists began analyzing precisely what happened in two of the affected nations, Egypt and Libya. Their fine-grained analysis of Internet censorship in these countries, which won this year's Applied Networking Research Prize from the Internet Research Task Force, emerged in part from a surprising source of data: malware.

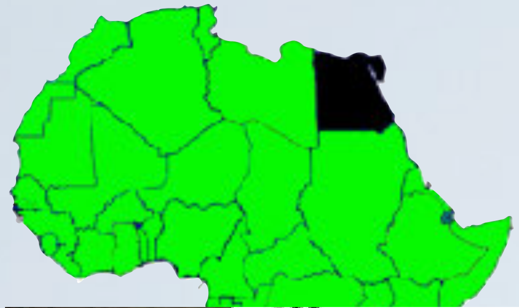
"We've never before seen an entire country disappear from the Internet for several days," says Alberto Dainotti, lead researcher with the Cooperative Association for Internet Data Analysis (CAIDA) at the University of California,

A crowd scene in Cairo's Tahrir Square during Egypt's five days of Internet outage last year; the large sign on the KFC window says "Awiz Internet" ("We want Internet").

Center for Applied Internet Data Analysis
University of California San Diego

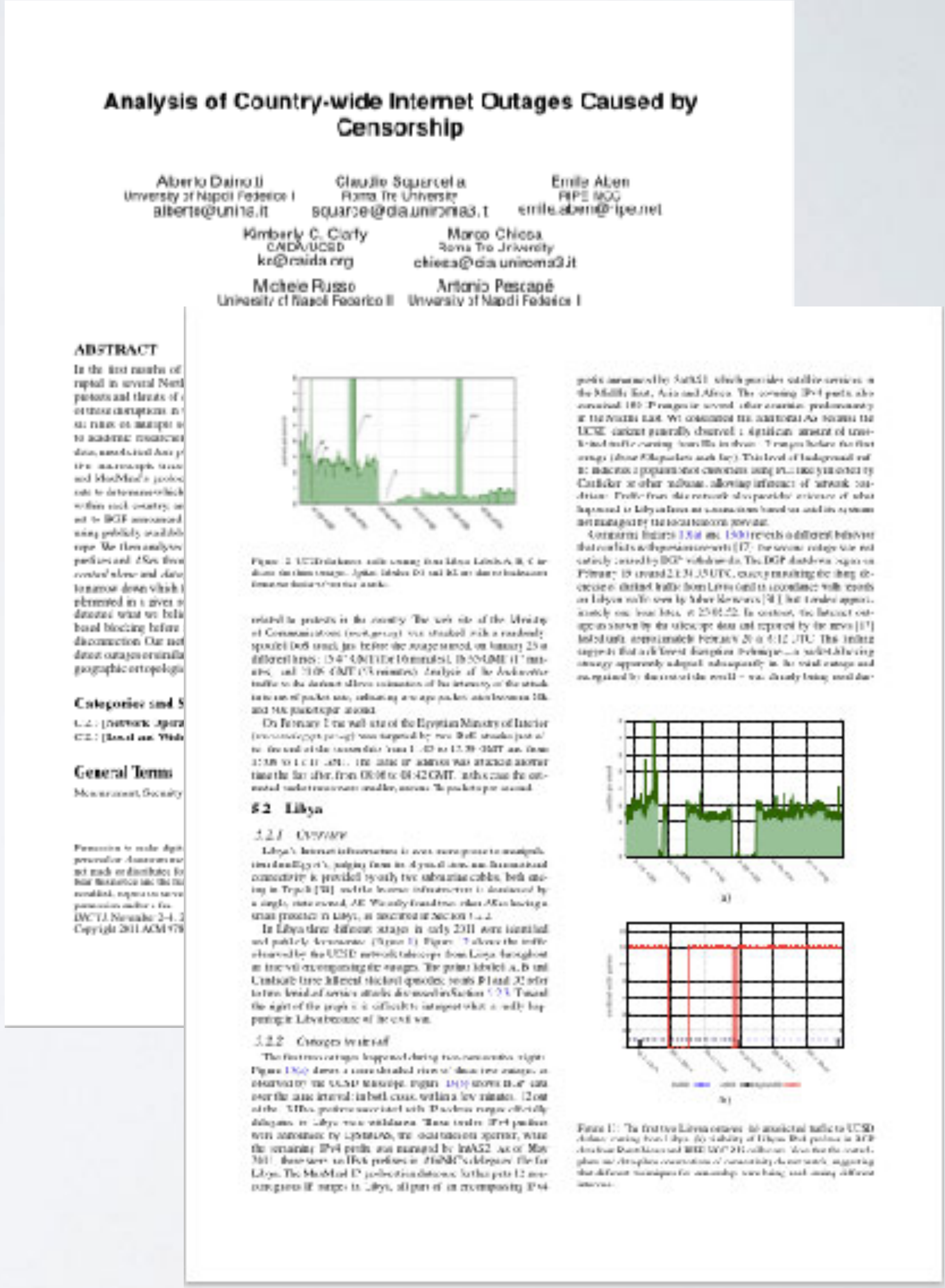
BEFORE IODA

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 Subject Descriptors

General Terms

3.2 Libya

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

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**

Center for Applied Internet Data Analysis
University of California San Diego

caida
www.caida.org

IODA CHALLENGES

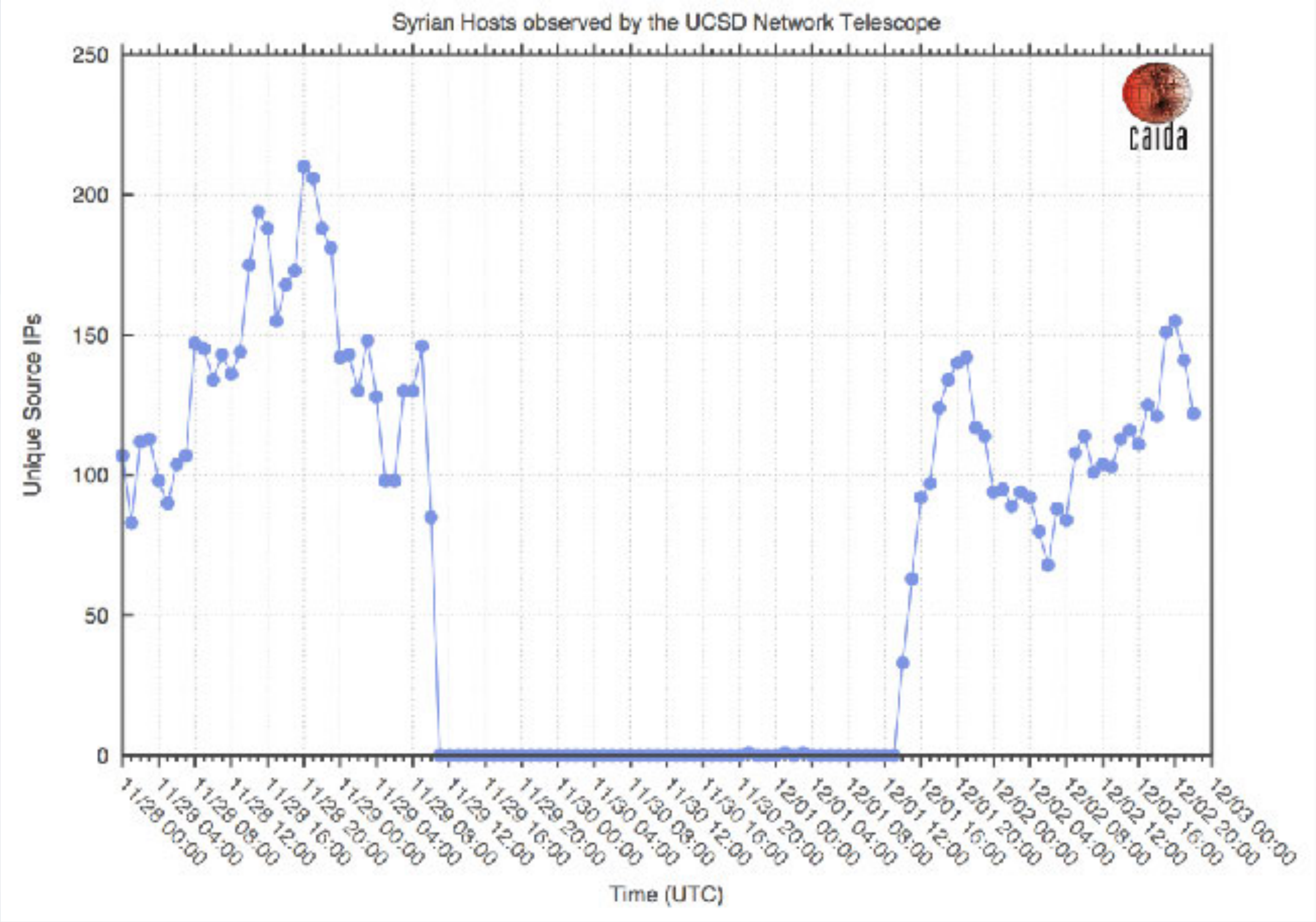
Why this is a tough problem

- 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

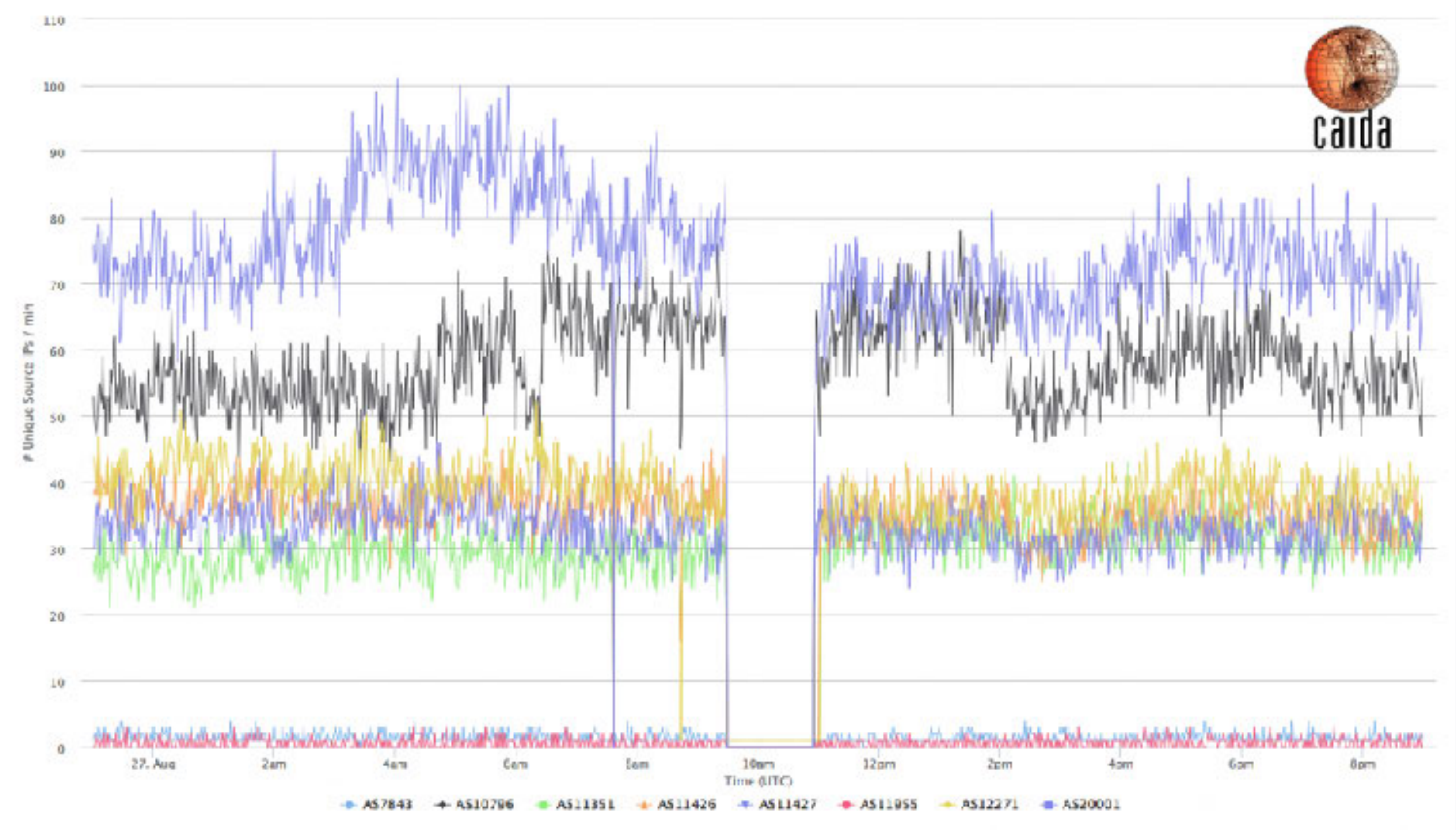
Syria disappears from the Internet — Nov 2012



IODA FIRST YEARS

documenting events on our blog

Time Warner Cable outage 27th August 2014

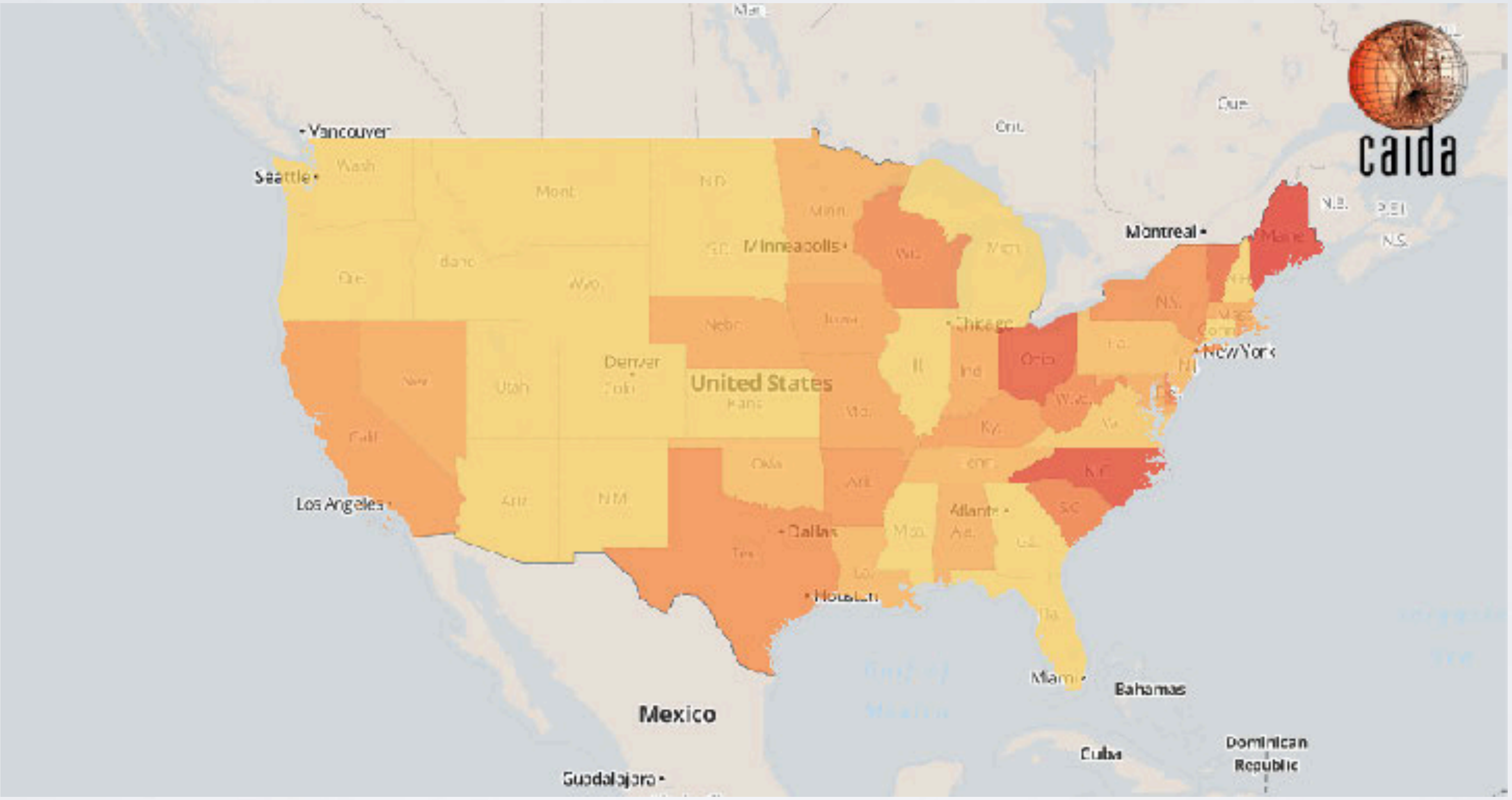


Center for Applied Internet Data Analysis
University of California San Diego

IODA FIRST YEARS

documenting events on our blog

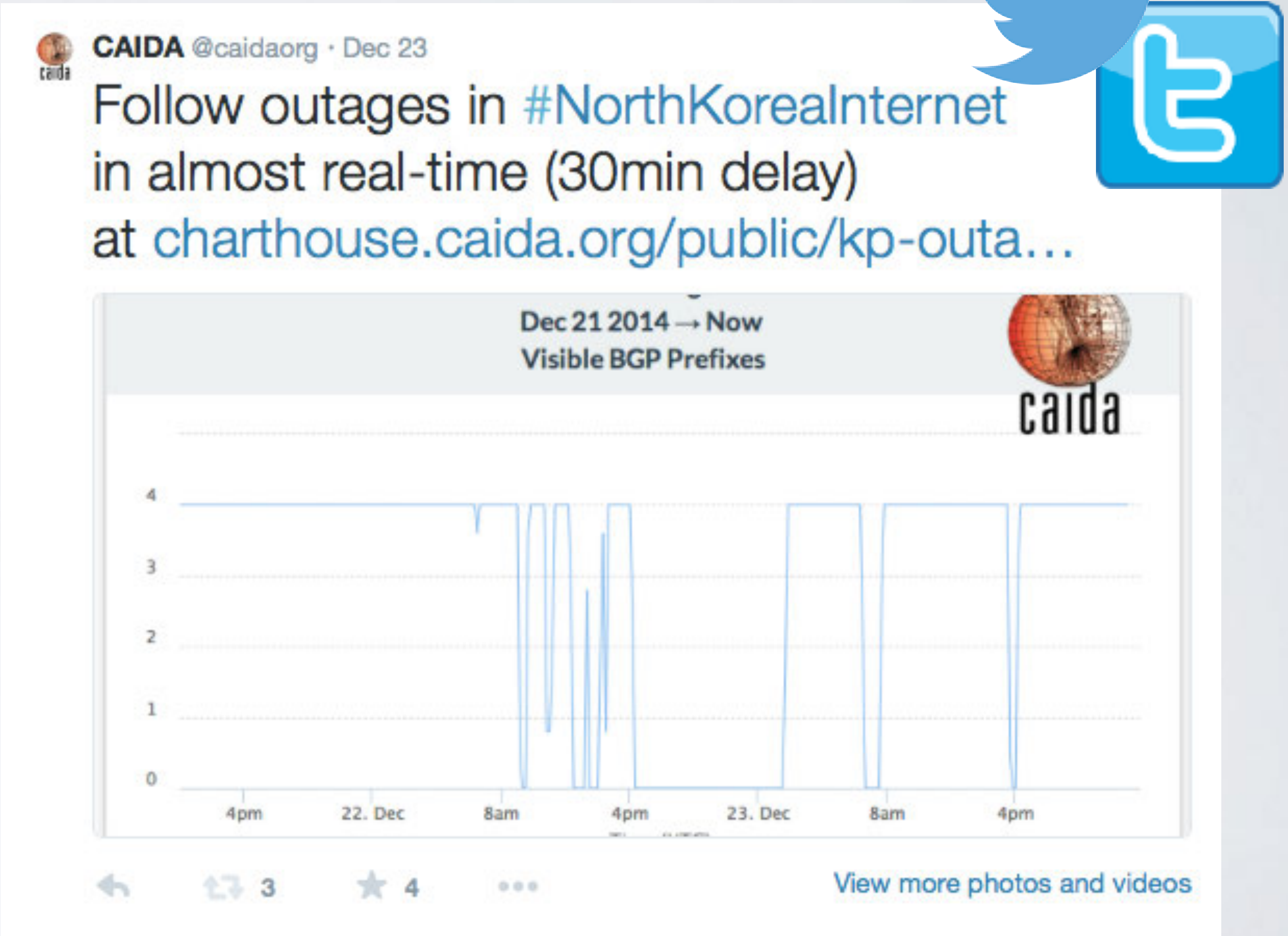
Time Warner Cable outage 27th August 2014



IODA AFTER 2 YEARS

live Internet monitoring

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



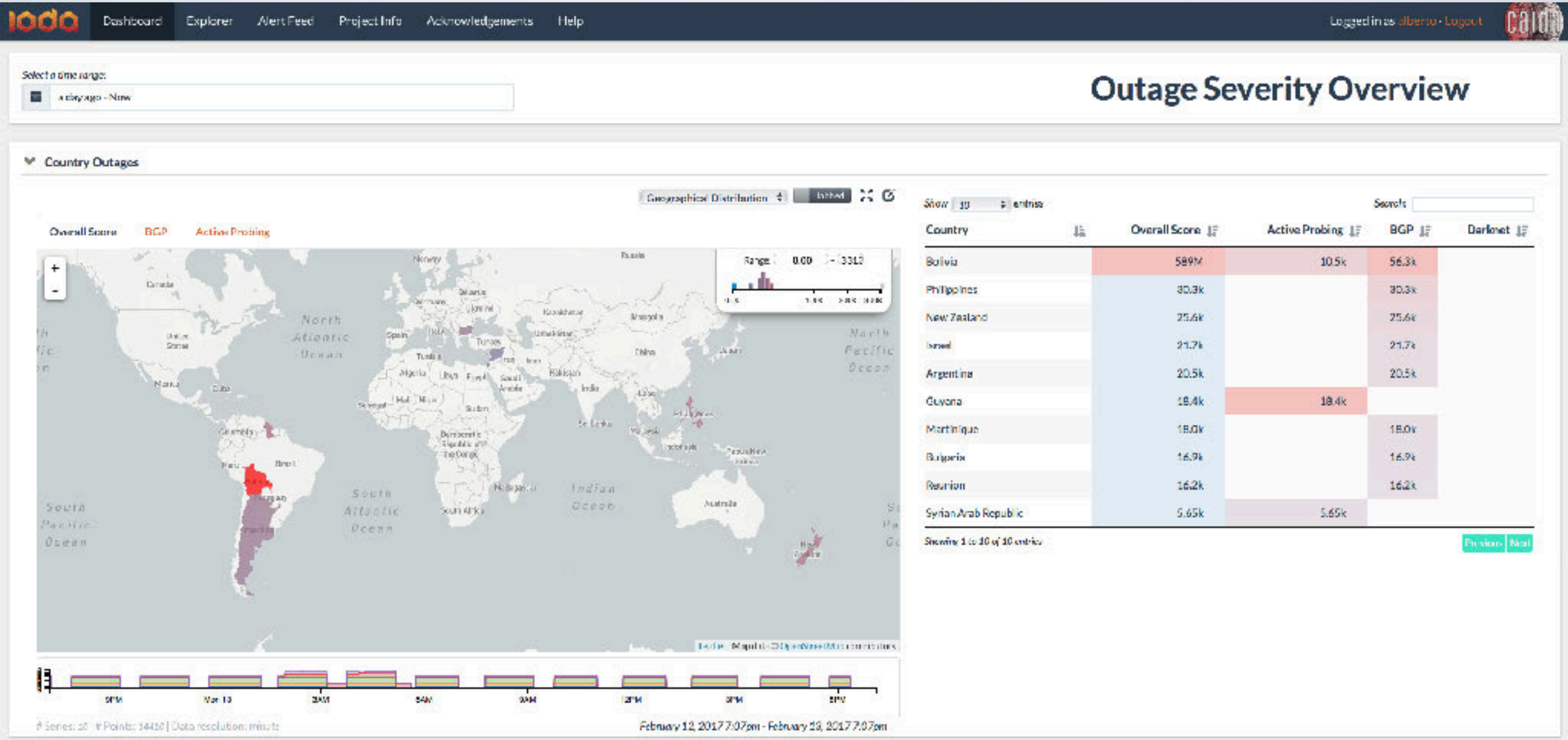
CAIDA @caidaorg · Dec 23

Follow outages in #NorthKoreaInternet in almost real-time (30min delay) at charthouse.caida.org/public/kp-outa…

https://ioda.caida.org/public/kp-outage

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

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

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

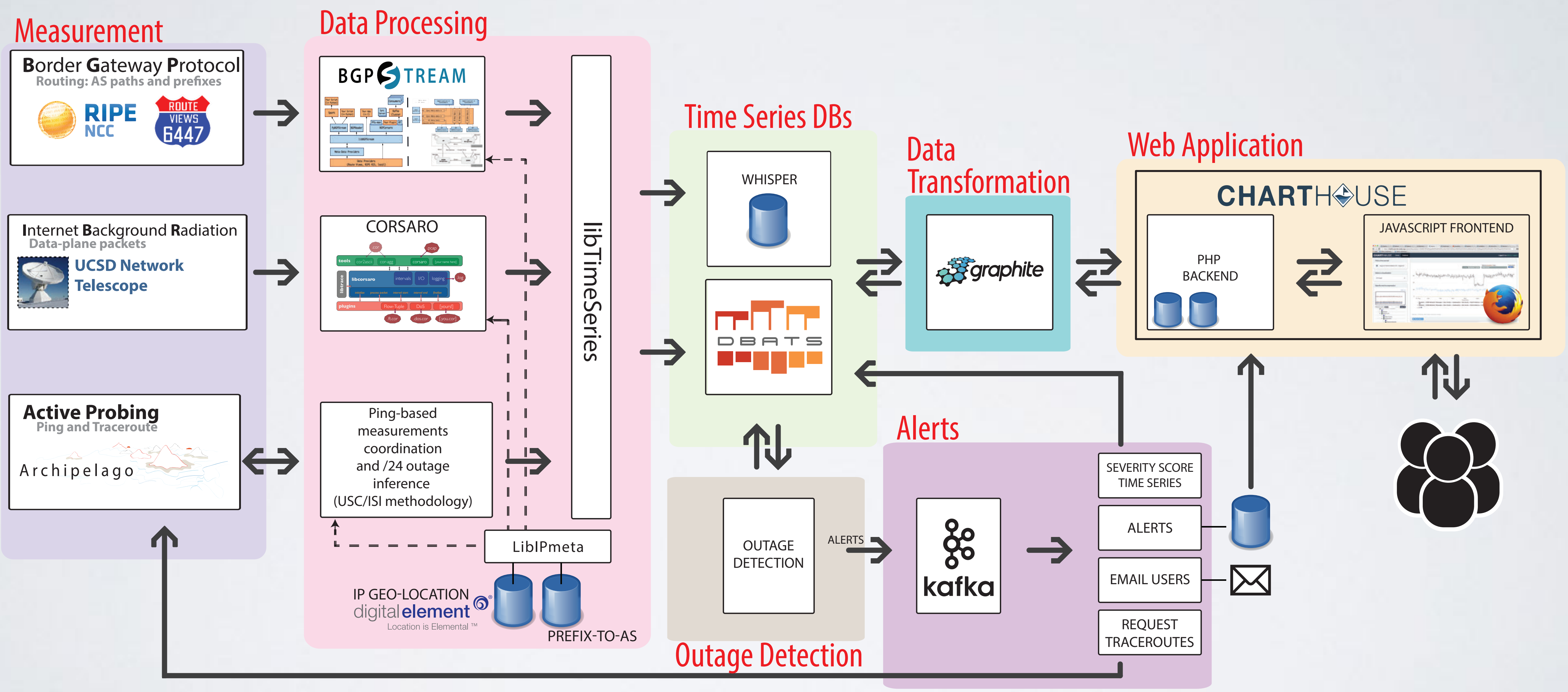
Center for Applied Internet Data Analysis
University of California San Diego

caida
www.caida.org

https://ioda.caida.org

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

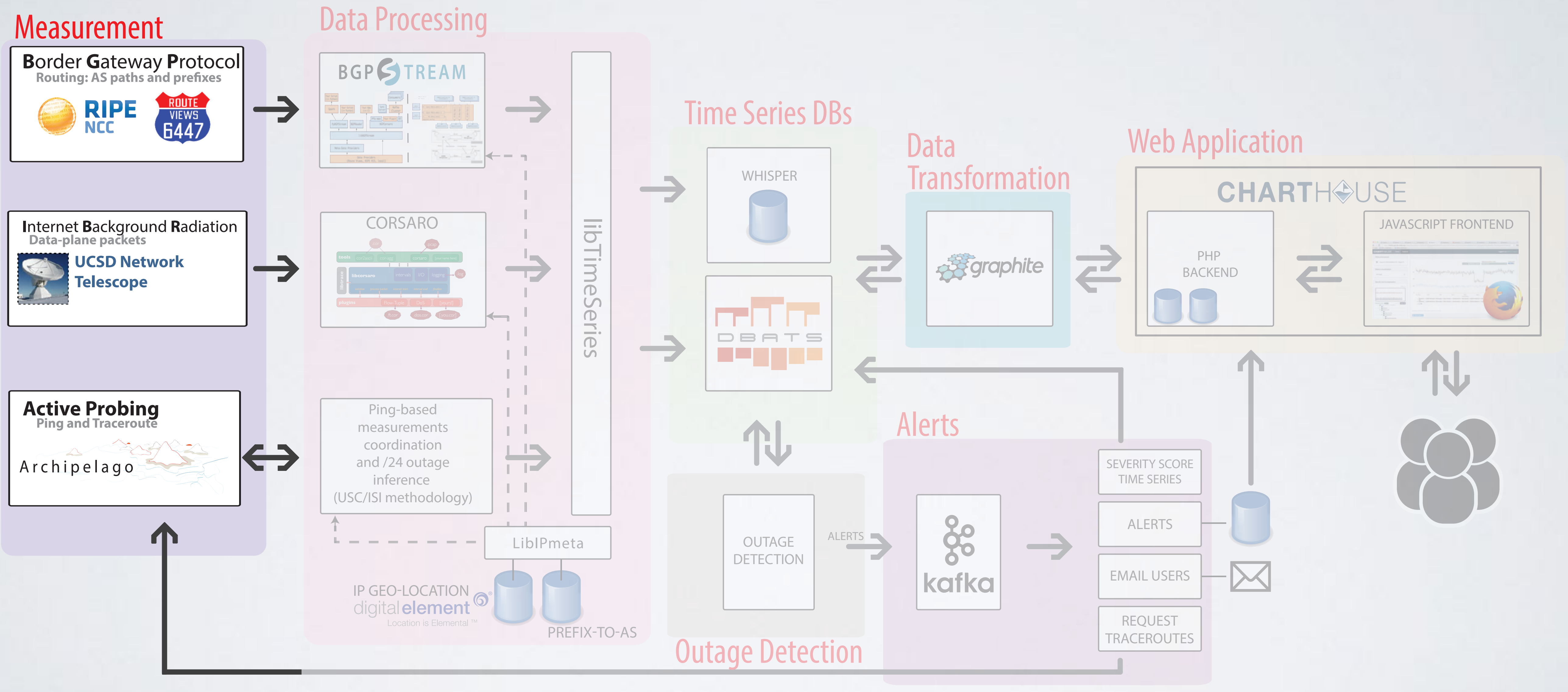
ALERTS

EMAIL USERS

REQUEST TRACEROUTES

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

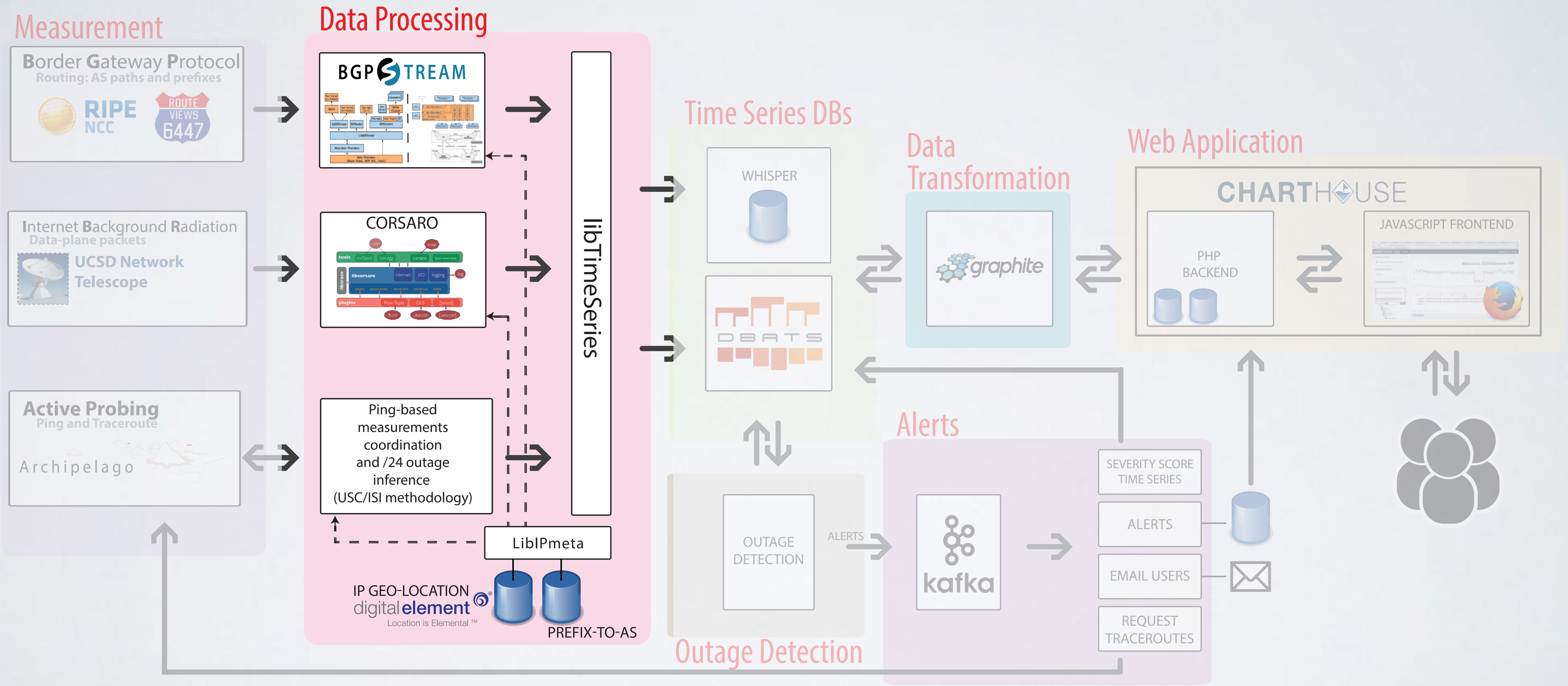
ALERTS

EMAIL USERS

REQUEST TRACEROUTES

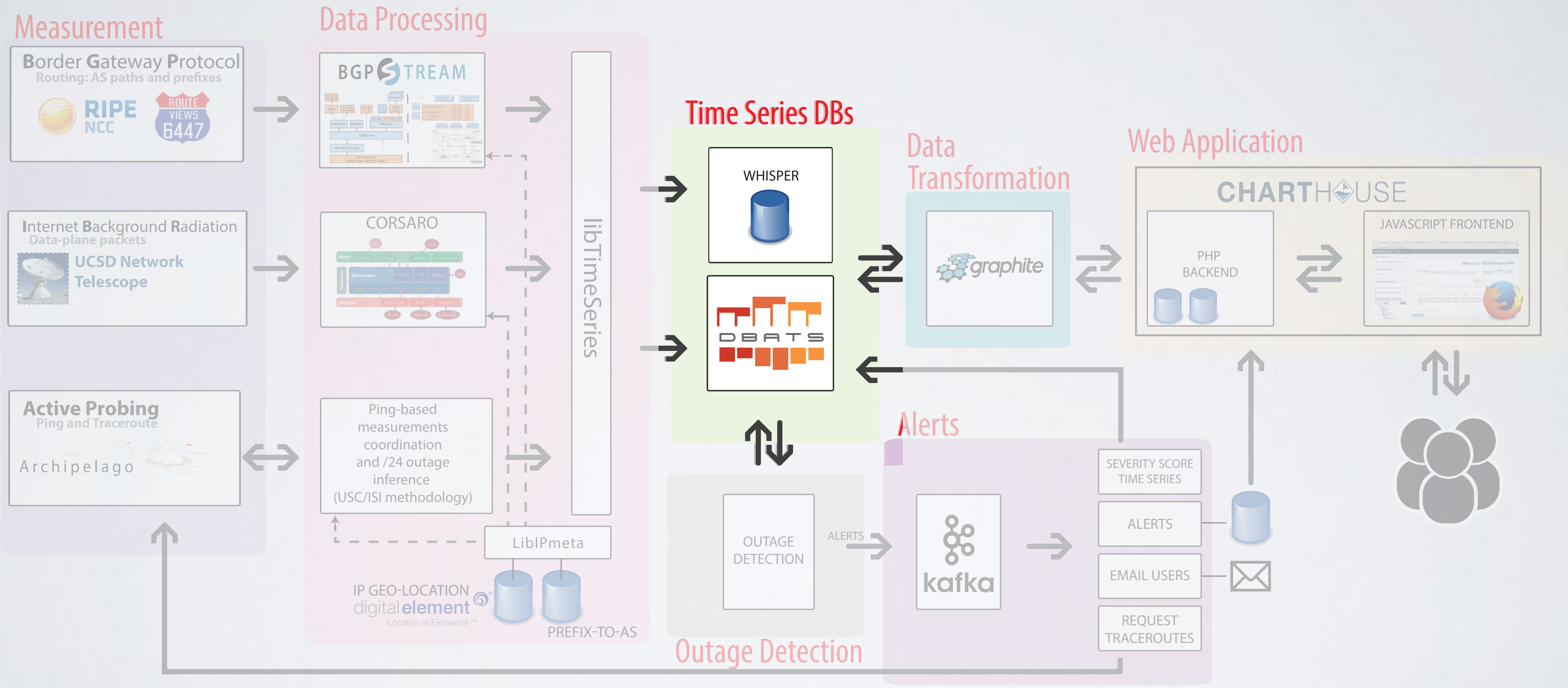
IODA'S CITY MAP

high-level system view



IODA'S CITY MAP

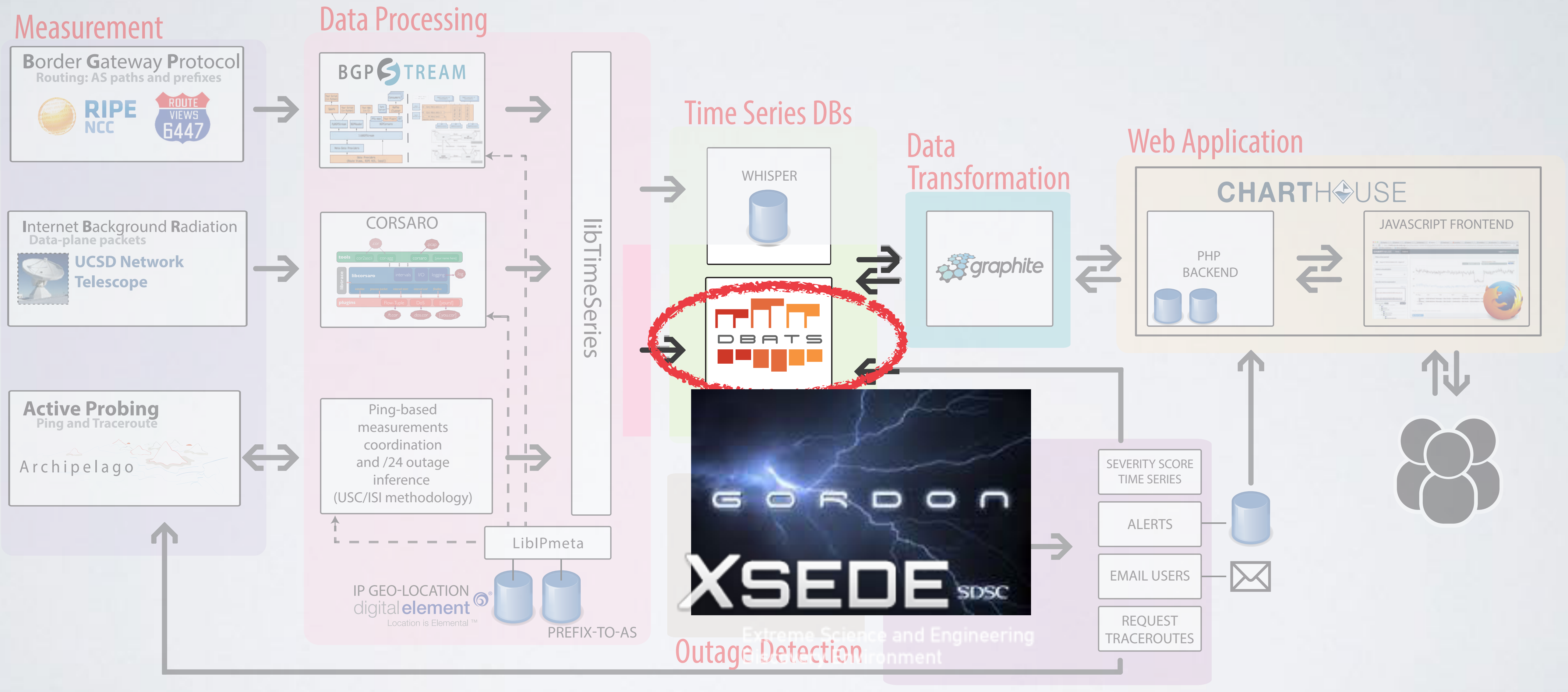
high-level system view



Center for Applied Internet Data Analysis
University of California San Diego

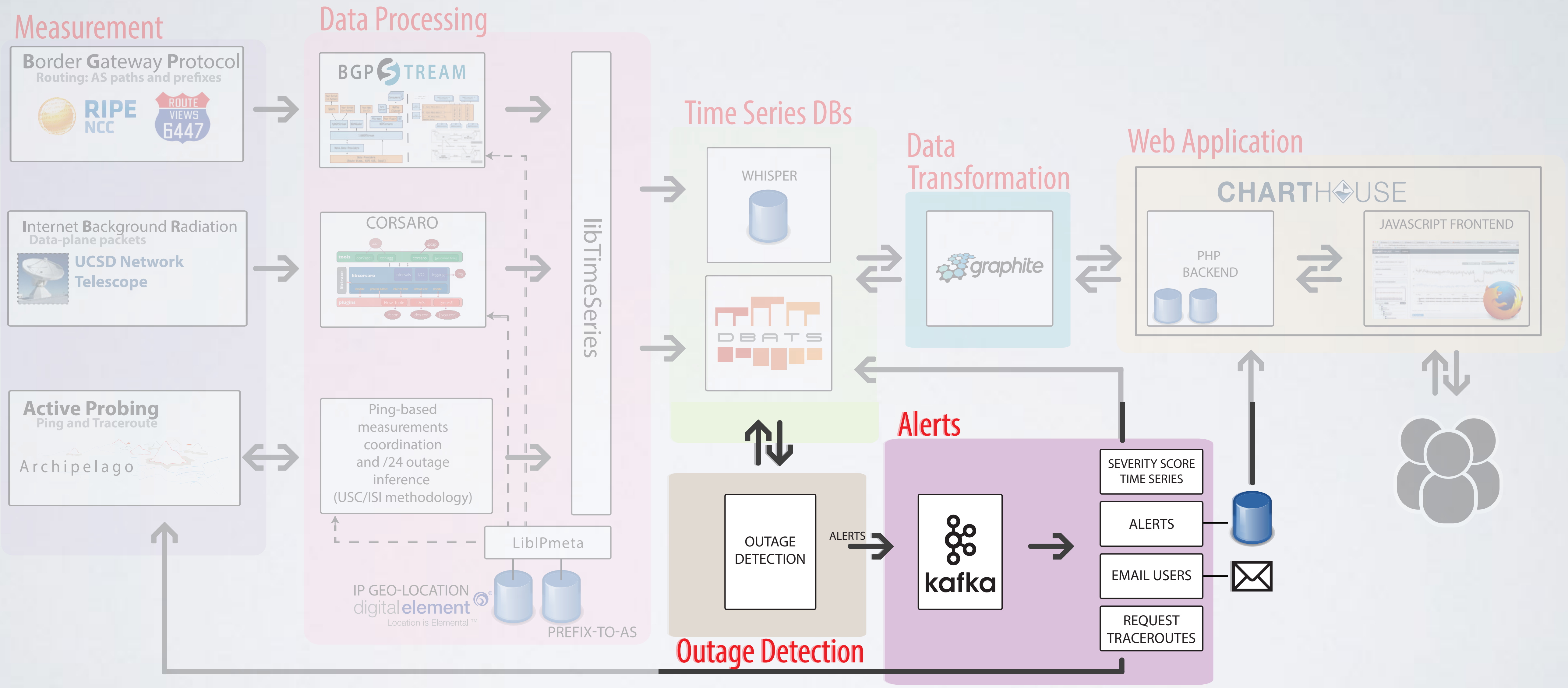
PART RUNS ON GORDON!

NSF XSEDE allocation



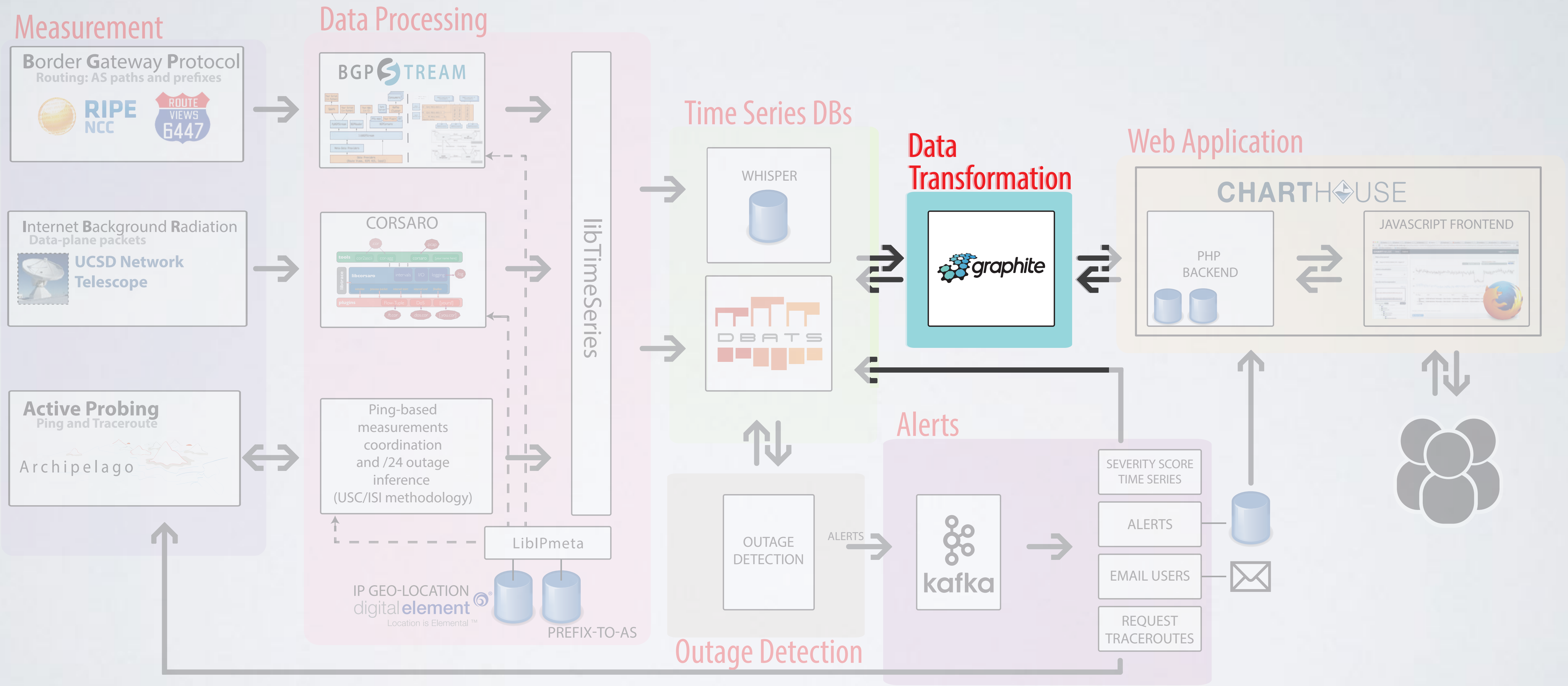
IODA'S CITY MAP

high-level system view



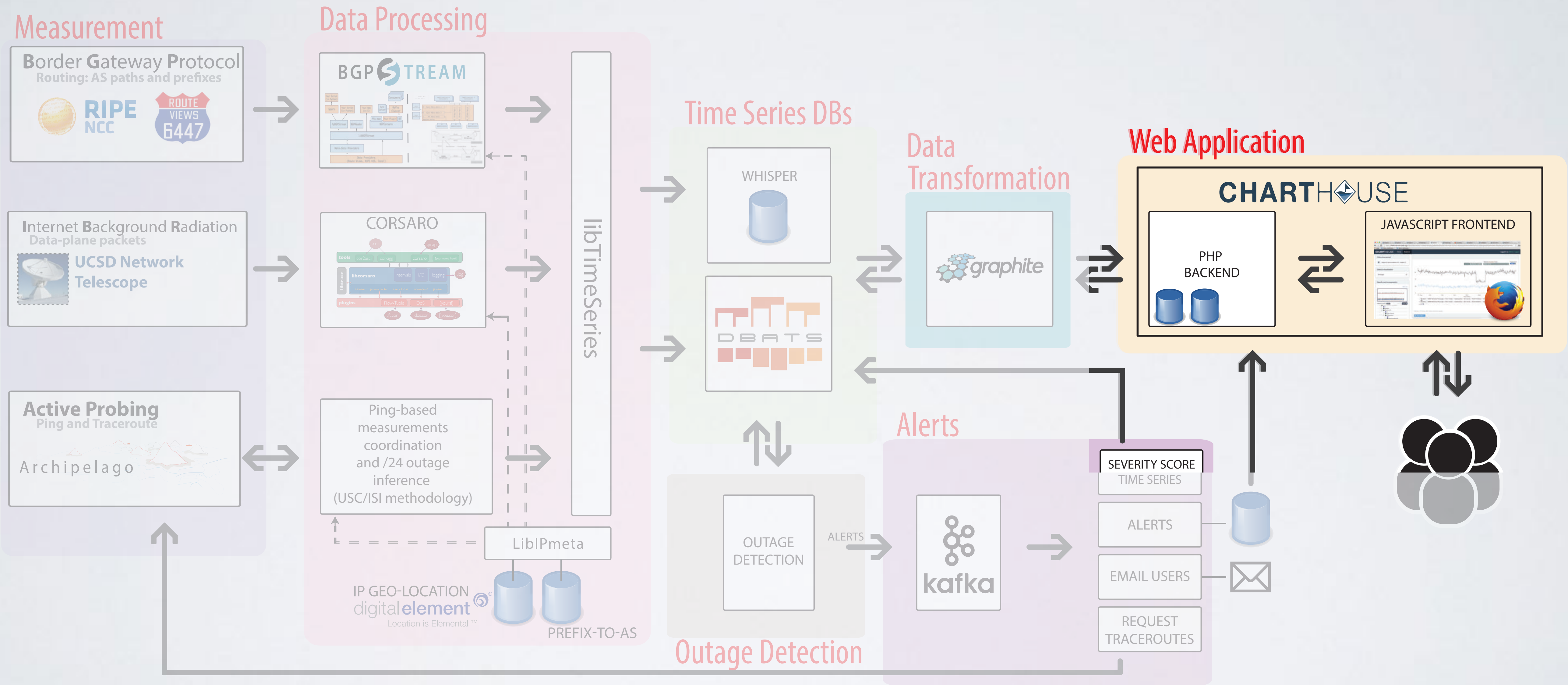
IODA'S CITY MAP

high-level system view



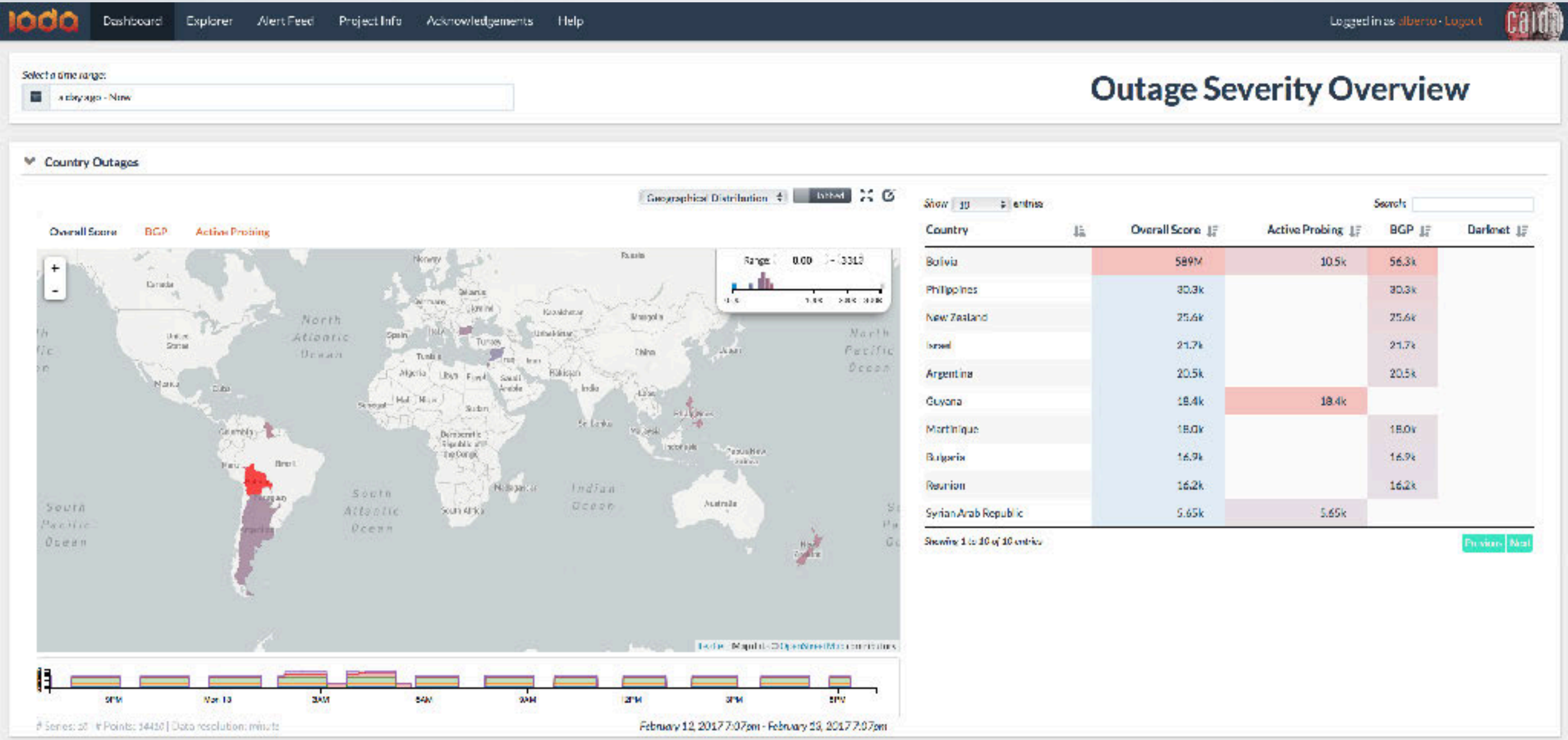
IODA'S CITY MAP

high-level system view



Center for Applied Internet Data Analysis
University of California San Diego

IODA DEMO



Select a time range:

a day ago - Now

Outage Severity Overview

Country Outages

Series: 38 | # Points: 14410 | Data resolution: minute

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

Show 10 entries

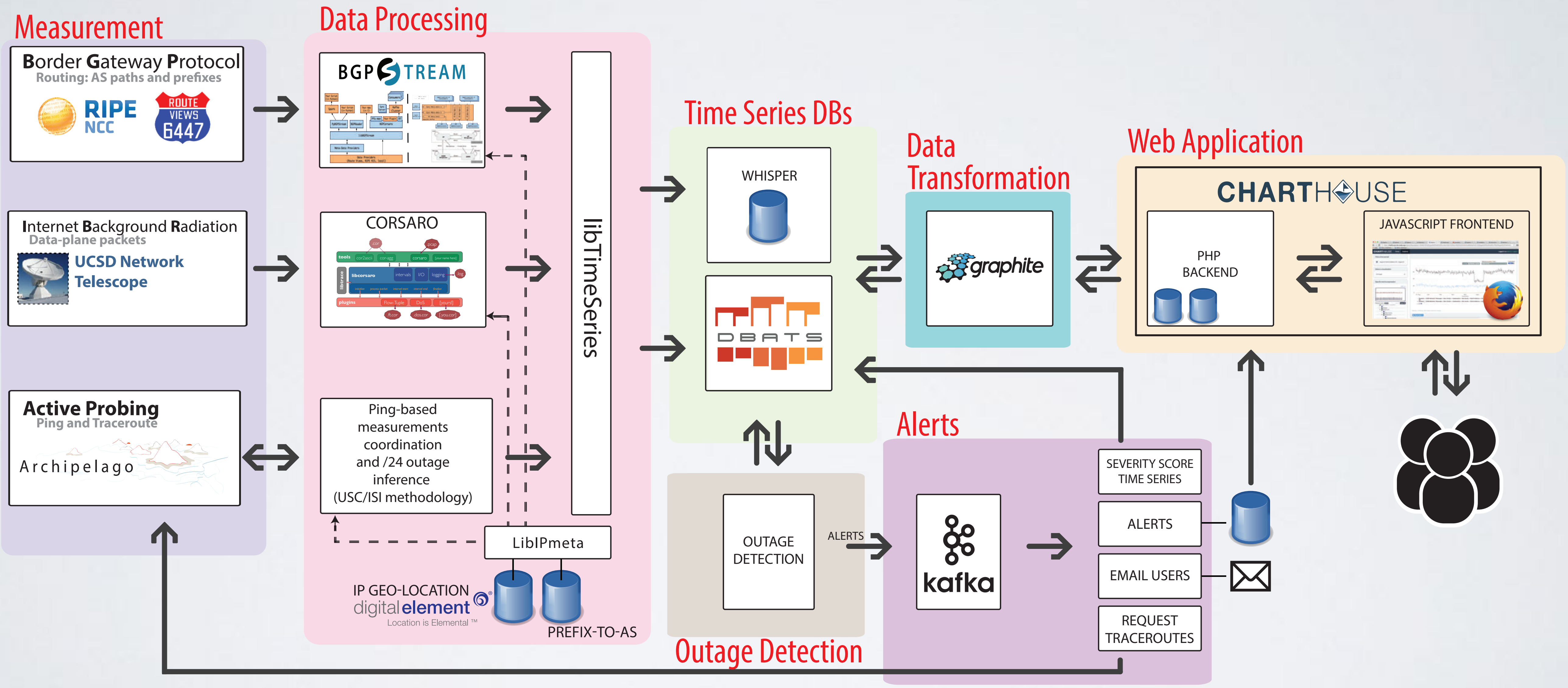
Search:

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

MANY SUB-SYSTEMS

each with its own challenges



Measurement

Border **G**ateway **P**rotocol
Routing: AS paths and prefixes
RIPE NCC
ROUTE VIEWS 6447

Internet **B**ackground **R**adiation
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

ALERTS

Outage Detection

Alerts

kafka

SEVERITY SCORE TIME SERIES

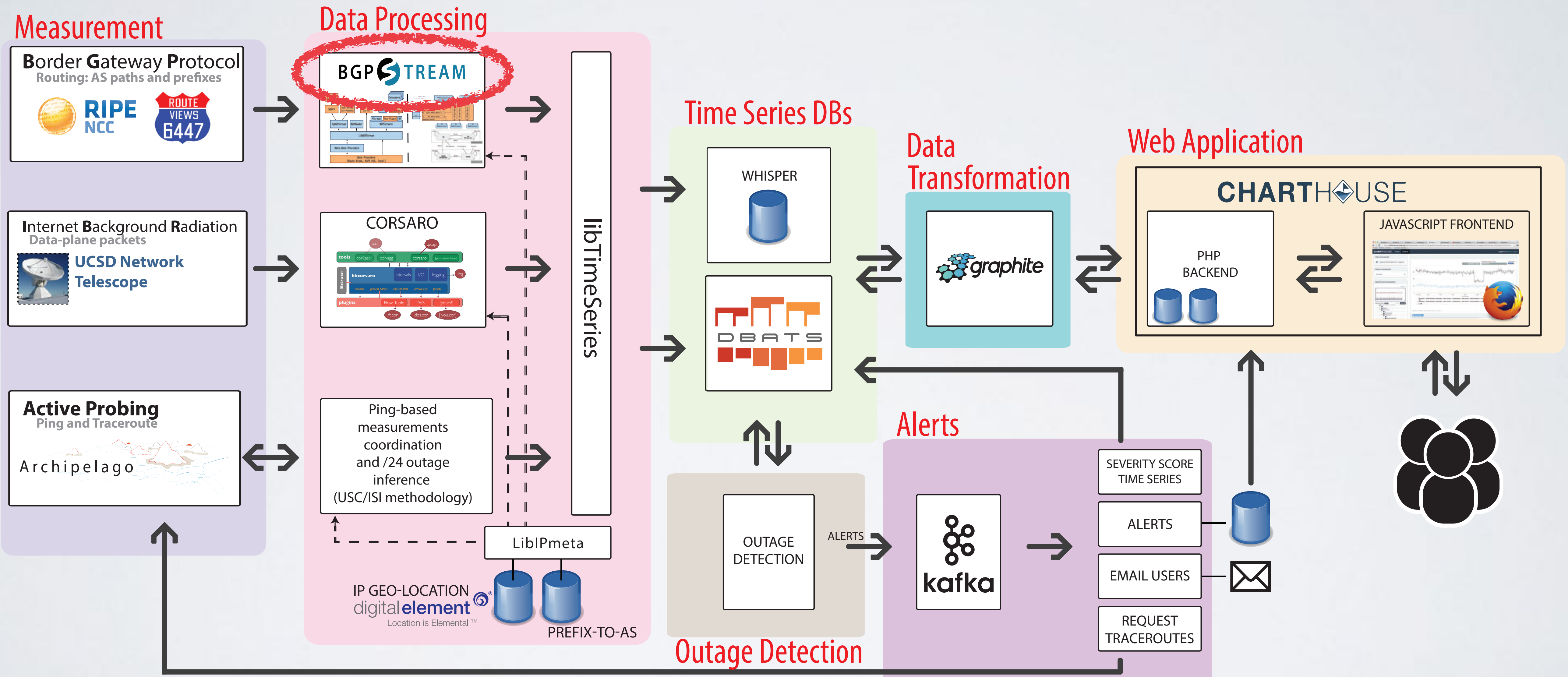
ALERTS

EMAIL USERS

REQUEST TRACEROUTES

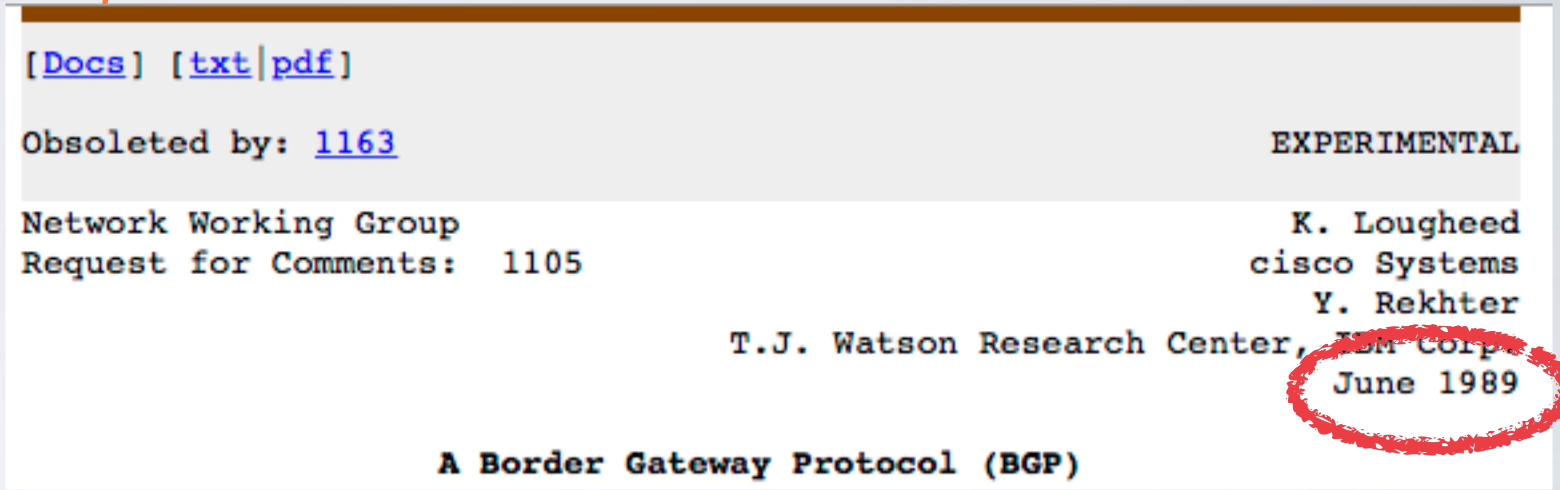
AN EXAMPLE: BGPSTREAM

efficient scalable processing of Internet routing data



BGPSTREAM

the paradox

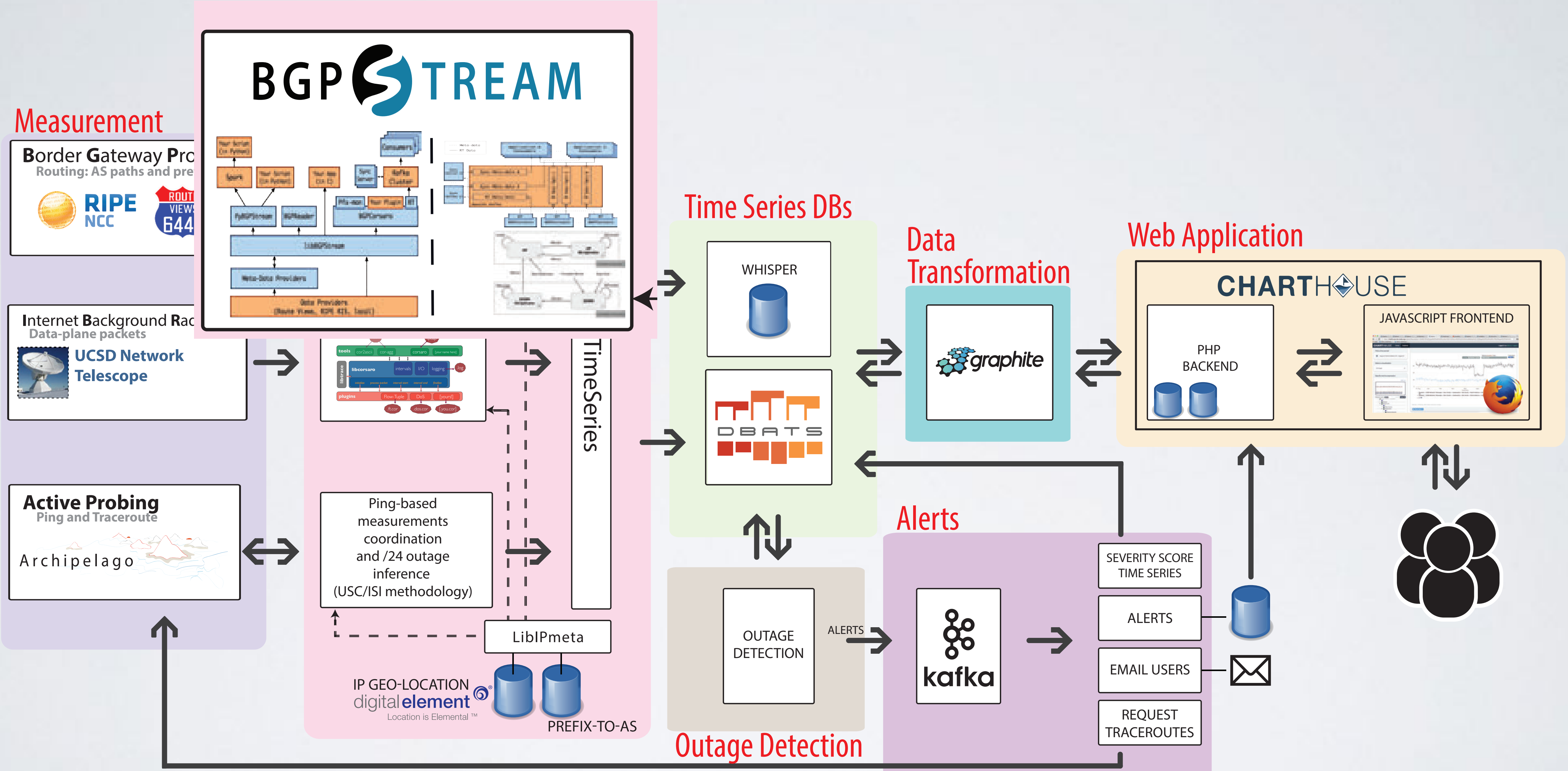


```
[Docs] [txt|pdf]

Obsoleted by: 1163                                       EXPERIMENTAL

Network Working Group                                     K. Lougheed
Request for Comments:  1105                             cisco Systems
                                                           Y. Rekhter
                              T.J. Watson Research Center, IBM Corp.
                                                            June 1989

                     A Border Gateway Protocol (BGP)
```

- **BGP is the central nervous system of the Internet!**
- There is almost 40 years of highly relevant research on BGP (*and still going..*)
- Operators collect, analyze and monitor BGP data to learn about and solve Internet routing problems
- **There *was* no efficient way of processing large amounts of distributed and/or live BGP measurement data**

BGPSTREAM

efficient scalable processing of Internet routing data



Measurement

Border Gateway Pro
Routing: AS paths and pre

Internet Background Rad
Data-plane packets
UCSD Network Telescope

Active Probing
Ping and Traceroute
Archipelago

BGPSTREAM

TimeSeries

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

LibIPmeta

IP GEO-LOCATION

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

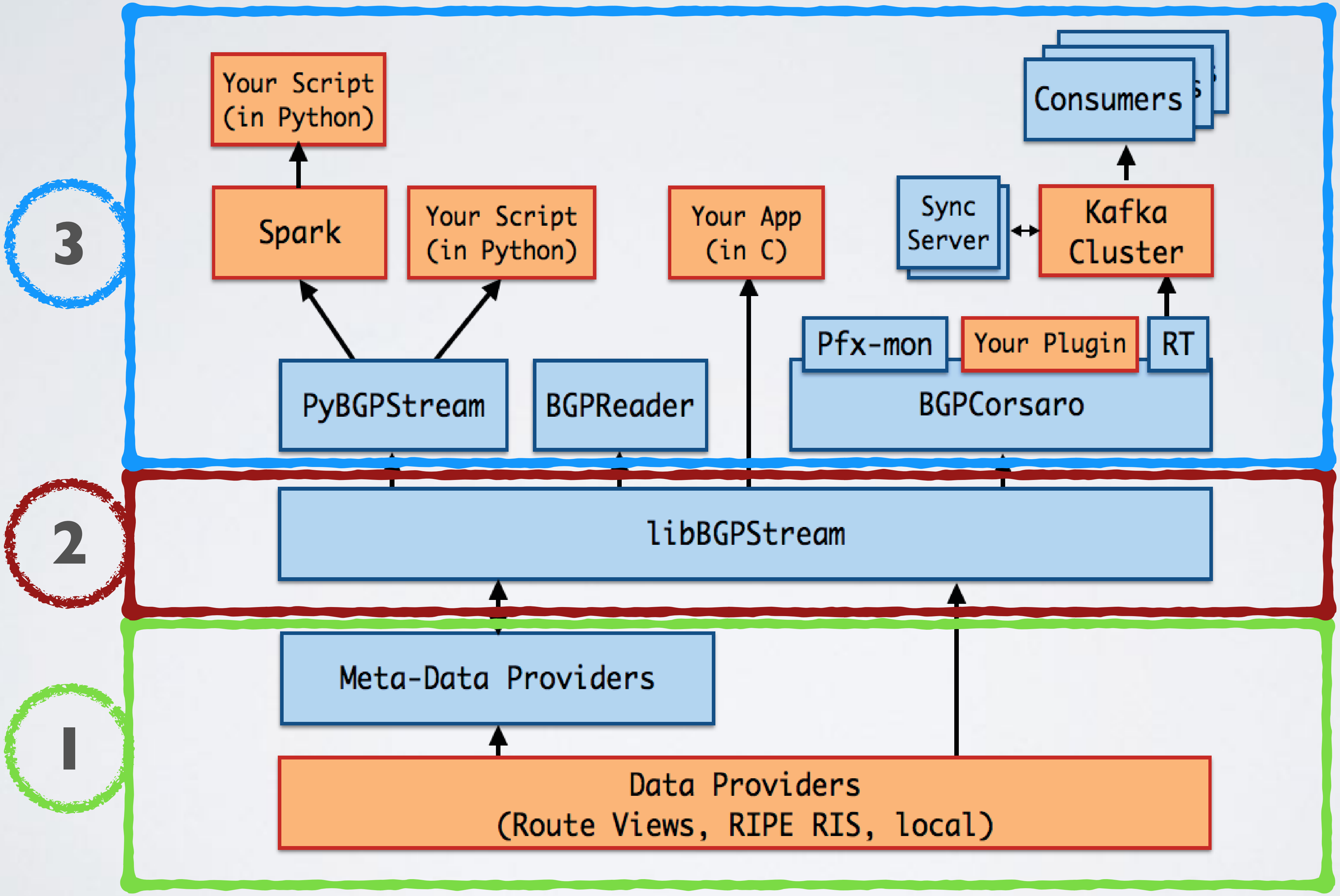
ALERTS

EMAIL USERS

REQUEST TRACEROUTES

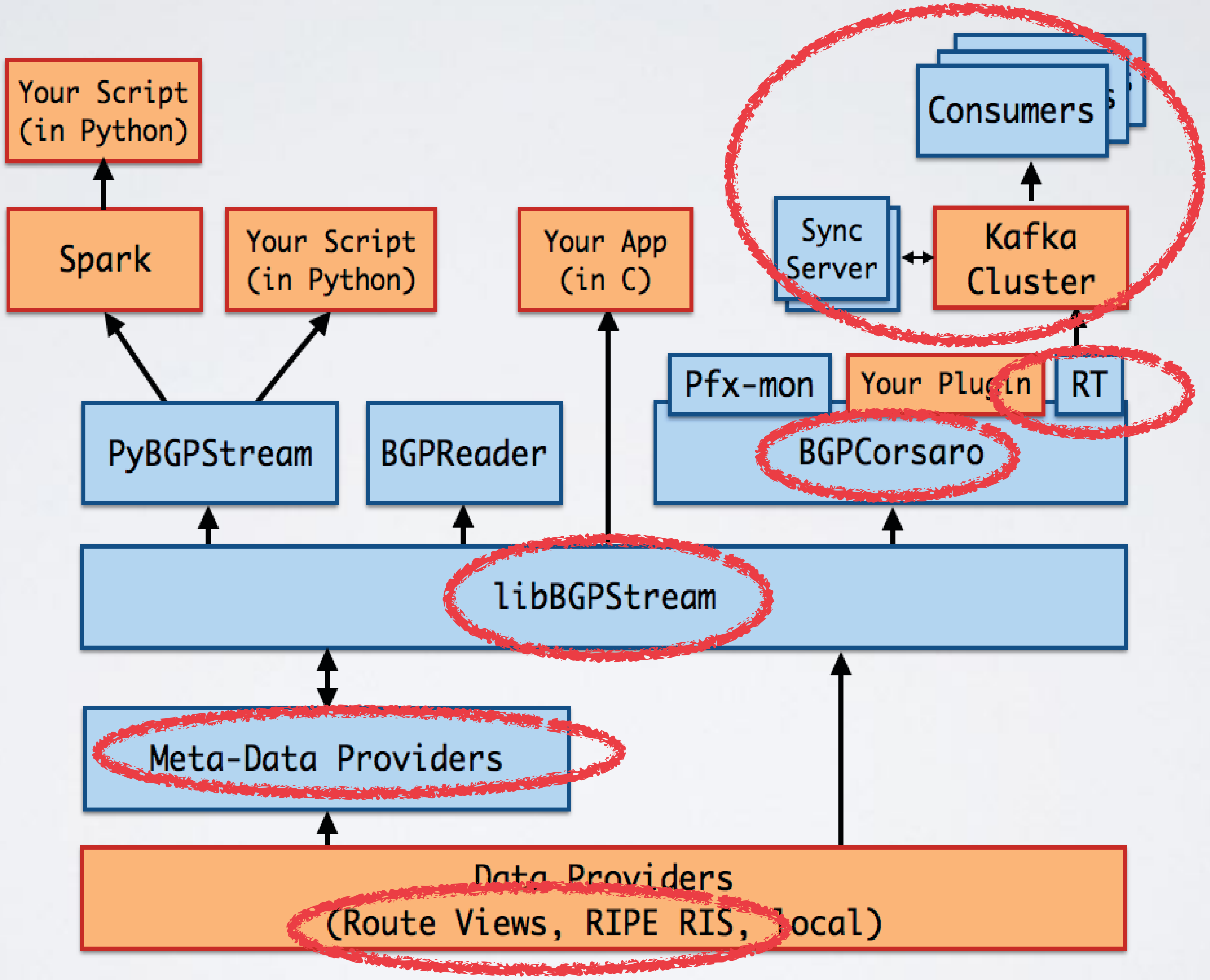
BGPSTREAM

efficient scalable processing of Internet routing data



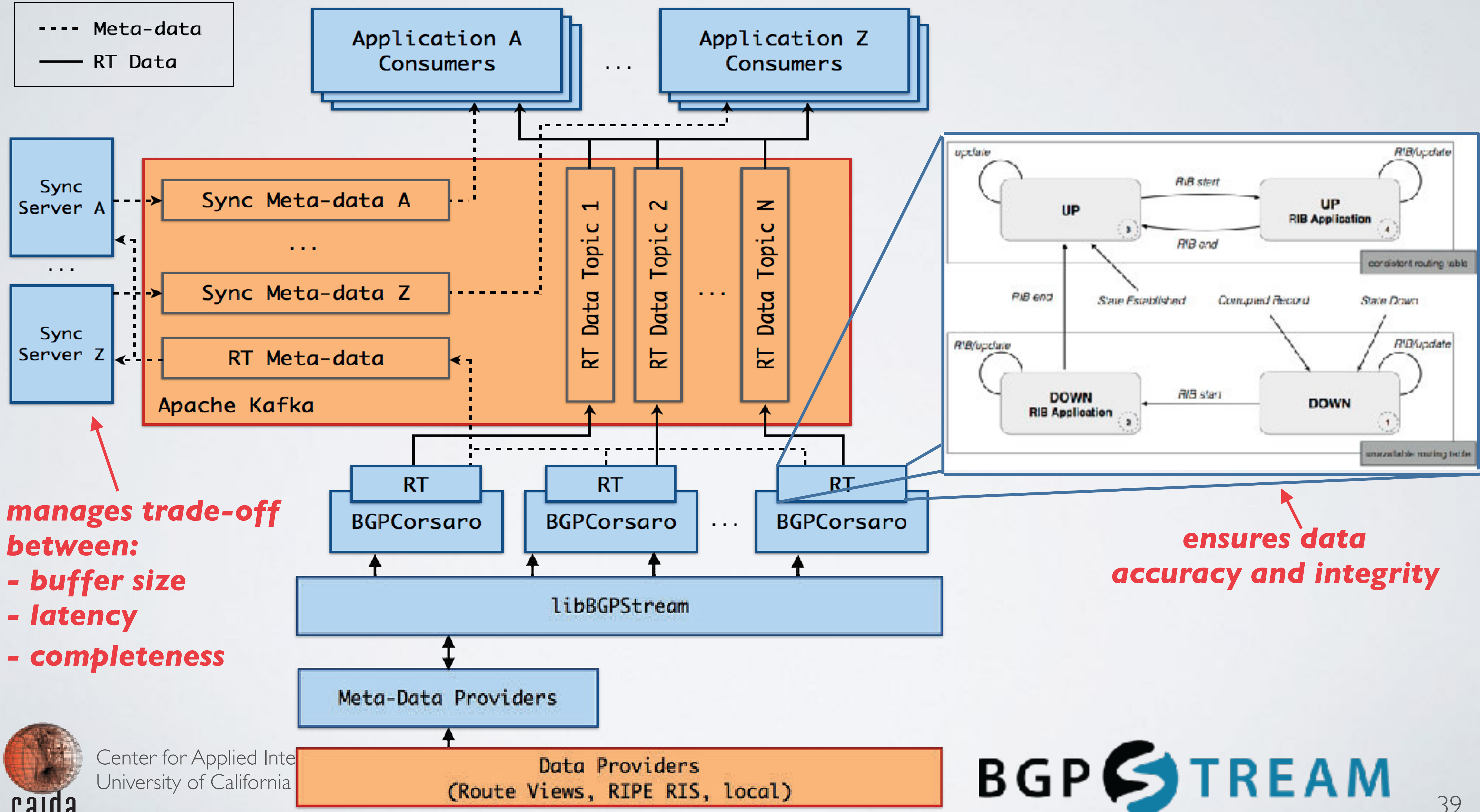
BGPSTREAM IN IODA

the toolchain we needed to process routing data



BGPSTREAM IN IODA

32 BGPCorsaro instances processing data from ~500 routers



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

ensures data accuracy and integrity

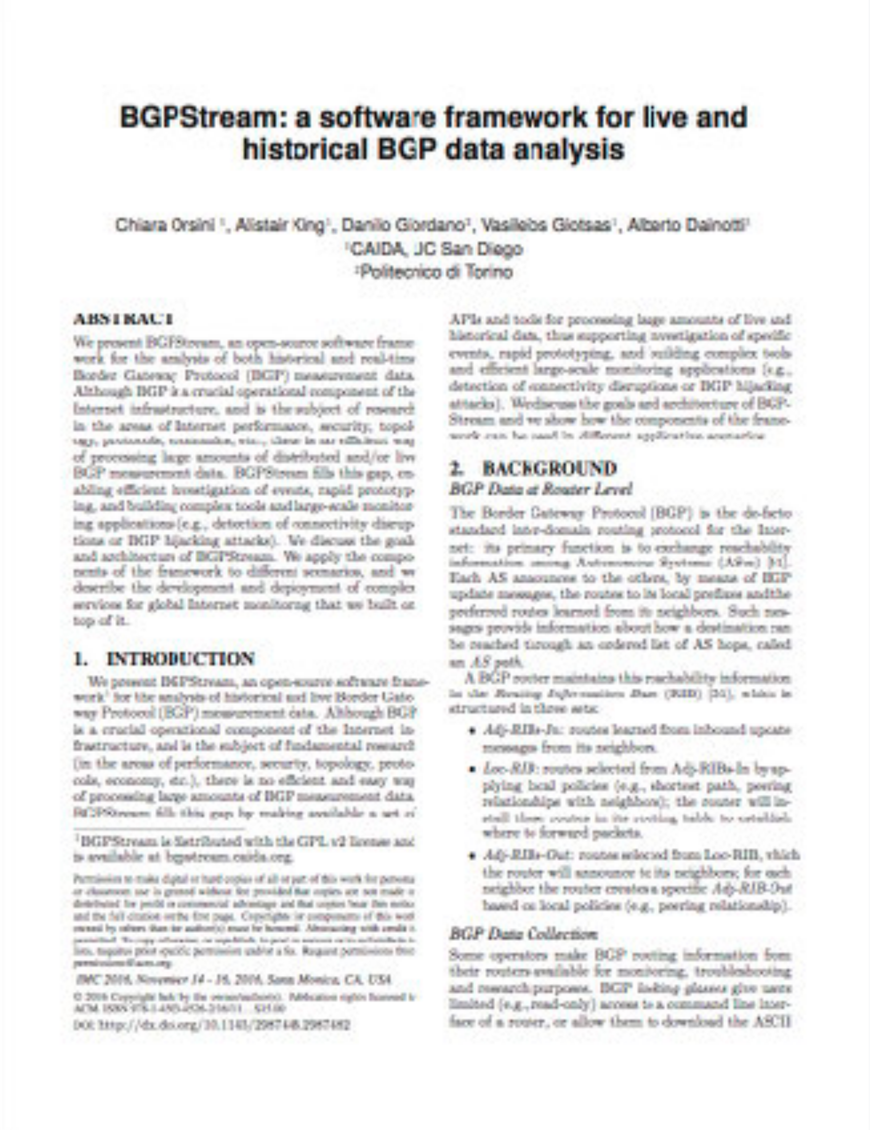
BGPSTREAM

A research + development project of its own

- We published a paper presenting BGPStream at the *ACM Internet Measurement Conference 2016*
  - Includes analysis of massive amounts of historical BGP data using Apache Spark running on SDSC's Comet!

- Alistair has been awarded the **IRTF's Applied Networking Research Prize** for this paper and will present it at the next Internet Engineering Task Force (IETF) meeting.

- Users worldwide (including students), code contributions, and several collaborations:
  - **Cisco Systems** awarded us ~$100k to collaborate to extend BGPStream functionalities to support their open-source BGP Monitoring Protocol framework



BGPStream: a software framework for live and historical BGP data analysis

Chiara Orsini[1], Alistair King[1], Danilo Giordano[2], Vasileios Giotsas[1], Alberto Dainotti[1]
[1]CAIDA, UC San Diego
[2]Politecnico di Torino

ABSTRACT

We present BGPStream, an open-source software framework for the analysis of both historical and real-time Border Gateway Protocol (BGP) measurement data. Although BGP is a crucial operational component of the Internet infrastructure, and is the subject of research in the areas of Internet performance, security, topology, protocols, economics, etc., there is no efficient way of processing large amounts of distributed and/or live BGP measurement data. BGPStream fills this gap, enabling efficient investigation of events, rapid prototyping, and building complex tools and large-scale monitoring applications (e.g., detection of connectivity disruptions or BGP hijacking attacks). We discuss the goals and architecture of BGPStream. We apply the components of the framework to different scenarios, and we describe the development and deployment of complex services for global Internet monitoring that we built on top of it.

1. INTRODUCTION

We present BGPStream, an open-source software framework[1] for the analysis of historical and live Border Gateway Protocol (BGP) measurement data. Although BGP is a crucial operational component of the Internet infrastructure, and is the subject of fundamental research (in the areas of performance, security, topology, protocols, economy, etc.), there is no efficient and easy way of processing large amounts of BGP measurement data. BGPStream fills this gap by making available a set of APIs and tools for processing large amounts of live and historical data, thus supporting investigation of specific events, rapid prototyping, and building complex tools and efficient large-scale monitoring applications (e.g., detection of connectivity disruptions or BGP hijacking attacks). We discuss the goals and architecture of BGPStream and we show how the components of the framework can be used in different application scenarios.

2. BACKGROUND

BGP Data at Router Level

The Border Gateway Protocol (BGP) is the de-facto standard inter-domain routing protocol for the Internet: its primary function is to exchange reachability information among Autonomous Systems (ASes) [31]. Each AS announces to the others, by means of BGP update messages, the routes to its local prefixes and the preferred routes learned from its neighbors. Such messages provide information about how a destination can be reached through an ordered list of AS hops, called an *AS path*.

A BGP router maintains this reachability information in the *Routing Information Base* (RIB) [31], which is structured in three sets:

- *Adj-RIBs-In*: routes learned from inbound update messages from its neighbors.
- *Loc-RIB*: routes selected from Adj-RIBs-In by applying local policies (e.g., shortest path, peering relationships with neighbors); the router will install these routes in its routing table to establish where to forward packets.
- *Adj-RIBs-Out*: routes selected from Loc-RIB, which the router will announce to its neighbors; for each neighbor the router creates a specific *Adj-RIB-Out* based on local policies (e.g., peering relationship).

BGP Data Collection

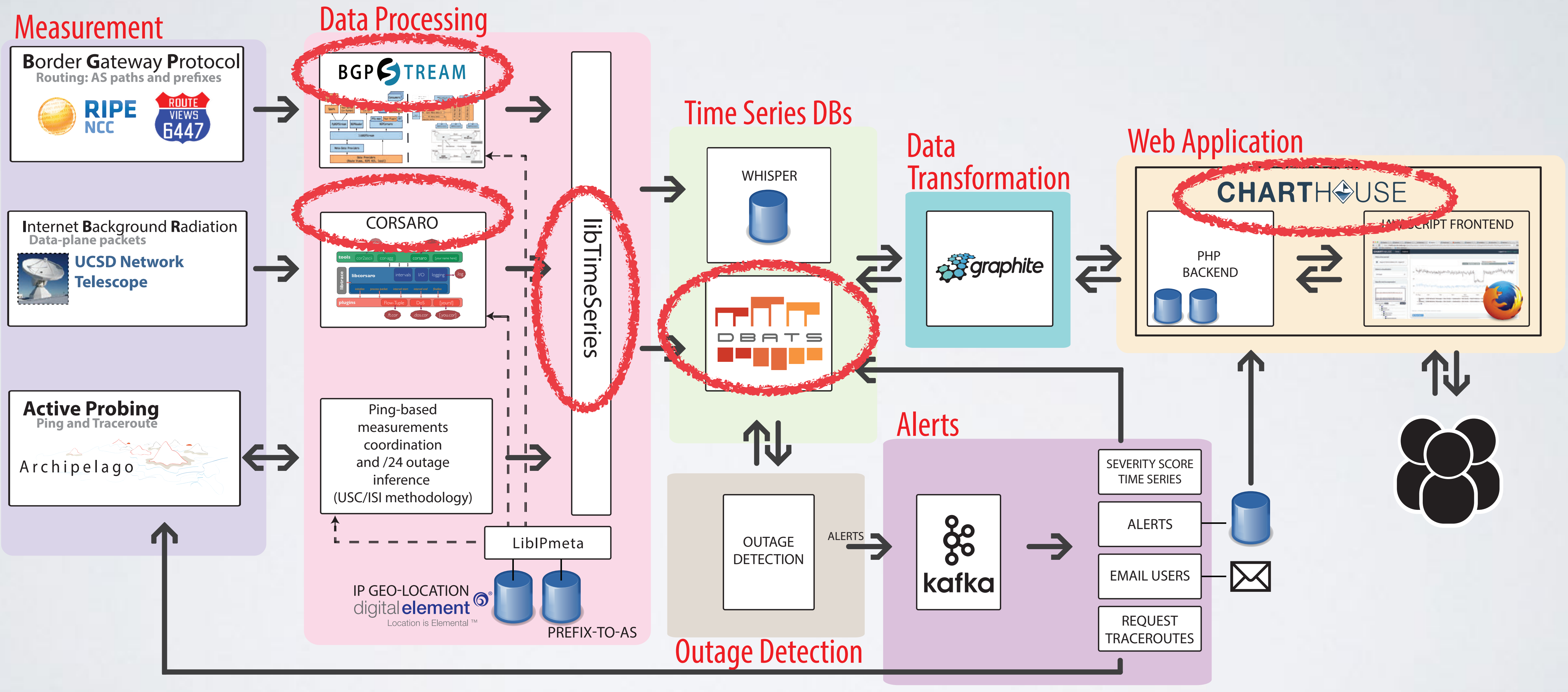
Some operators make BGP routing information from their routers available for monitoring, troubleshooting and research purposes. BGP looking glasses give users limited (e.g., read-only) access to a command line interface of a router, or allow them to download the ASCII

[1] BGPStream is distributed with the GPL v2 license and is available at bgpstream.caida.org.

IMC 2016, November 14 - 16, 2016, Santa Monica, CA, USA
© 2016 Copyright held by the owner/author(s). Publication rights licensed to ACM. ISBN 978-1-4503-4526-2/16/11 . . . $15.00
DOI: http://dx.doi.org/10.1145/2987443.2987482

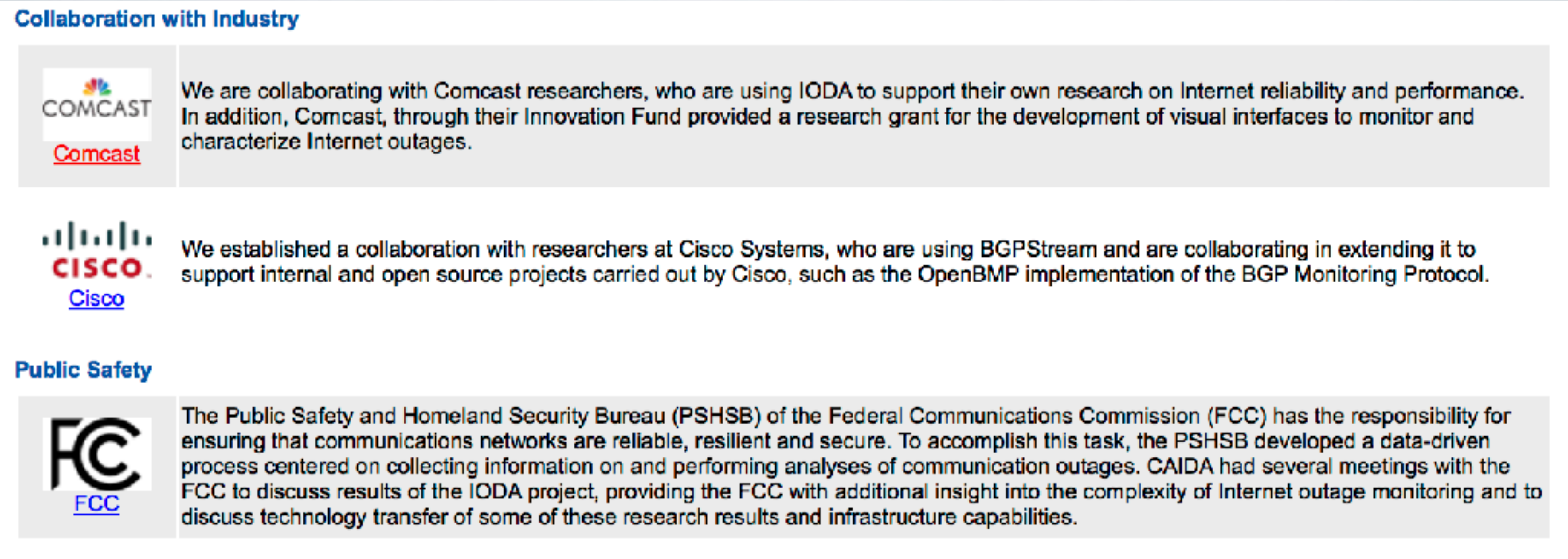
IODA SW SPIN OFFS

open-source frameworks of more general utility



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

FCC 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

next steps

- Collect feedback
- Provide to 3rd parties live+historical alert data feeds through the DHS "*Information Marketplace for Policy and Analysis of Cyber-Risk & Trust*" program
- Infrastructure Improvements/Maintenance/Documentation etc.
- Research on improving and cross-validating inferences
- Integrate other data sources

THANKS

www.caida.org/projects/ioda