

2019 S&T Cybersecurity and Innovation Showcase

Solutions Now | Innovations for the Future



Homeland
Security

Science and Technology





IODA-NP: Internet Outage Detection and Analysis

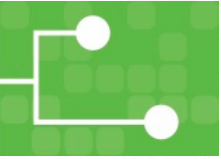
Alberto Dainotti | CAIDA, UC San Diego
March 18, 2019



**Homeland
Security**

Science and Technology





Funded Contract Information

This material is based on research sponsored by the Department of Homeland Security, Science and Technology Directorate via contract number 70RSAT18CB0000015.

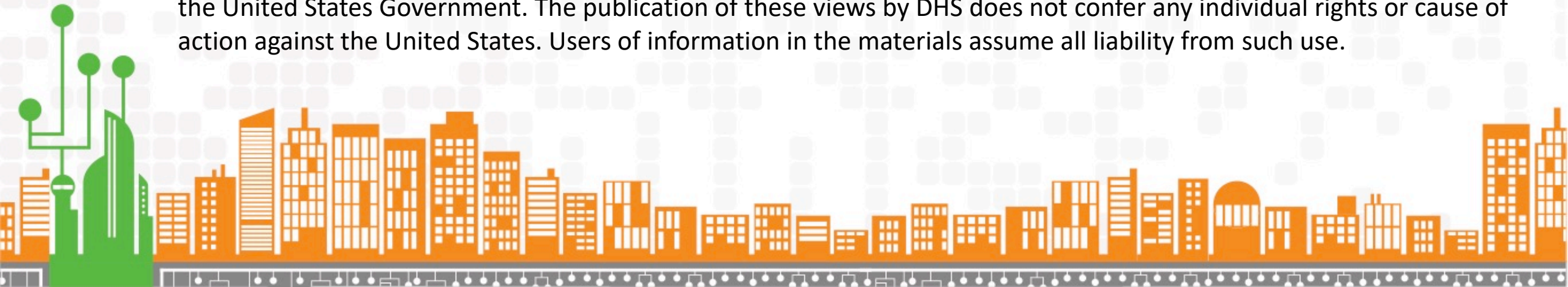
No Endorsement Notification

Any reference to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the Department of Homeland Security or the United States Government.

Hyperlinked Web sites do not constitute endorsement by DHS of the Web site or the information, products, or services contained therein. DHS does not exercise any editorial control over materials on this website or the information on non-DHS Web sites.

Disclaimer Notification

The views, opinions, findings, conclusions, or recommendations expressed in this presentation are those of the authors and do not necessarily reflect the official policy or position of the Department of Homeland Security (DHS) or the United States Government. The publication of these views by DHS does not confer any individual rights or cause of action against the United States. Users of information in the materials assume all liability from such use.

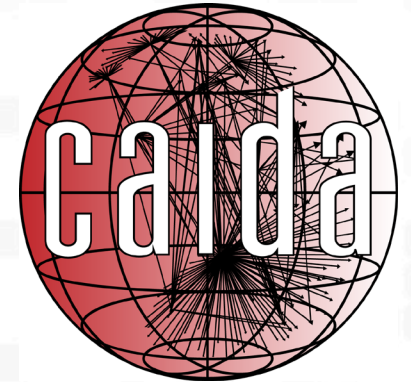




Team Profile

- **PI:** Dr. Alberto Dainotti – Research Scientist
- **CoPI:** Dr. Marina Fomenkov – Research Analyst
- **Team:** *Alistair King, Rama Padmanabhan, Philipp Winter, Dan Andersen, Paul Hick, Alex Ma, ...*

- **CAIDA** – Center for Applied Internet Data Analysis
University of California, San Diego

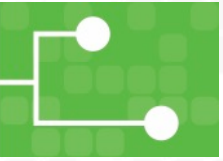




Customer Need

- **Goal:** Timely Detect and Analyze Internet Connectivity Outages
 - Focus on macroscopic events, affecting the network edge
 - *E.g., a connectivity black-out significantly affecting customers of a large network operator or a large geographic area*
- **Context:** cyber attacks, physical attacks, natural disasters, bugs and misconfiguration, government orders, ...
- **Application:** Public Safety, Situational Awareness, Disaster Recovery, Insurance, Internet Reliability & Performance



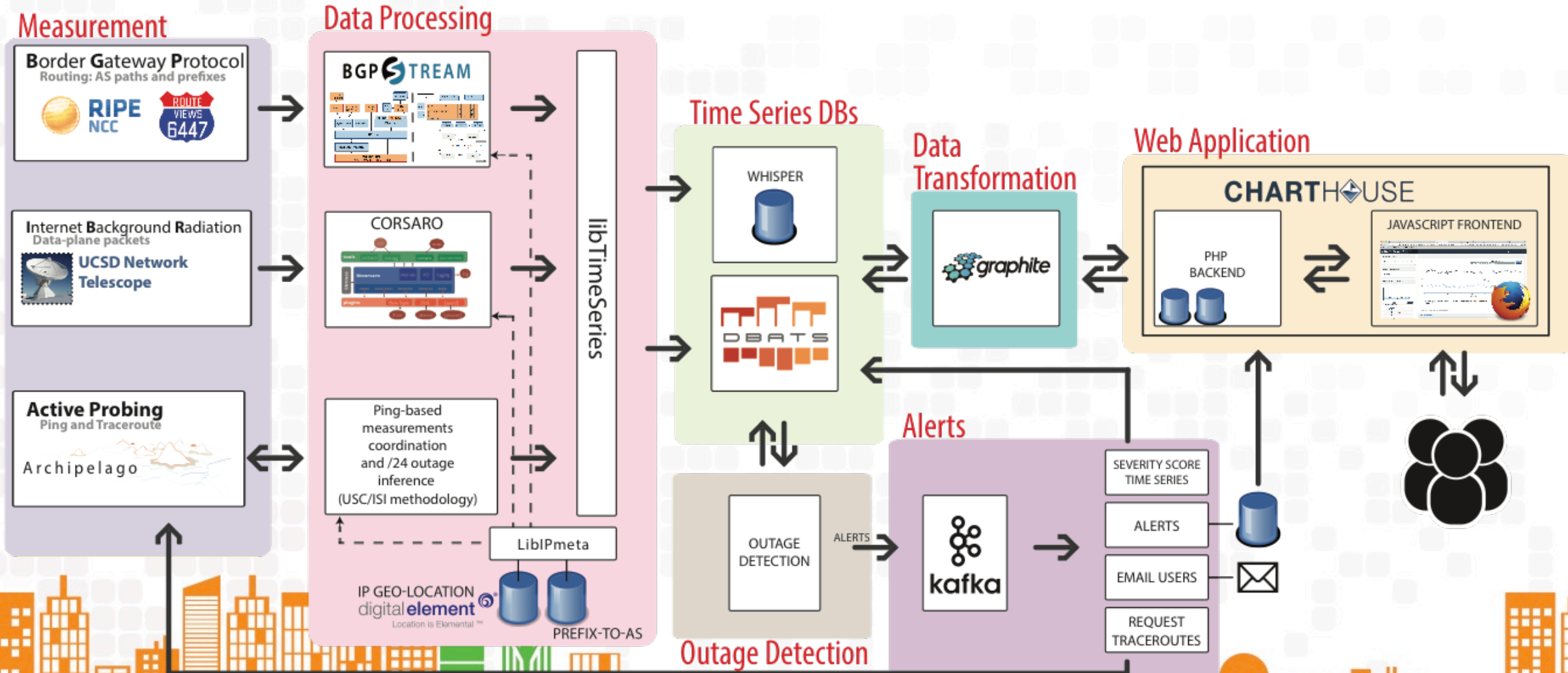


Approach - Overview

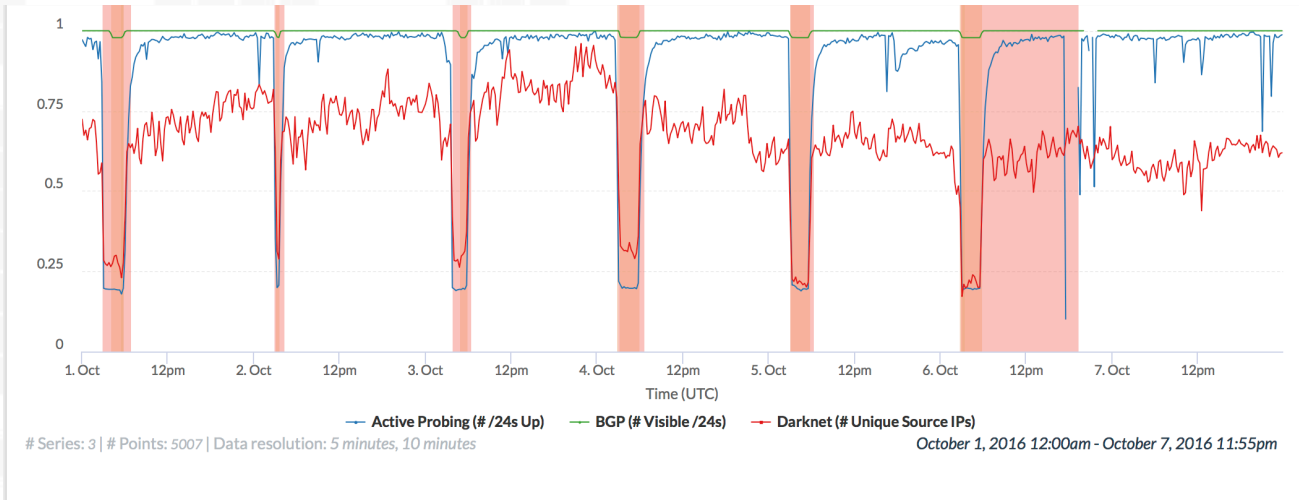
- IODA: *Internet Outage Detection & Analysis (NSF 2012-2016)*
 - Combine *active* and *passive* measurements both at the *data plane* and *control plane*
 - Data **aggregation** and event detection per Autonomous System (AS) and Geographic Area
 - Interactive **Visualization**
- IODA-NP: *Next Phase*
 - Methodological improvements and evaluation based on rigorous definitions, metrics, ground-truth, cross-validation
 - Reporting events
 - API Framework and Documentation



Approach - Architecture



Approach – Visualization

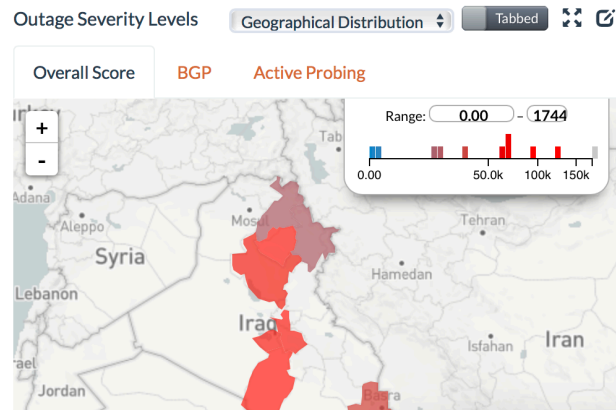


Time	Category	Value 1	Value 2
7:20pm	Probing		
✓ Oct 6th 2016 5:50am	BGP	71,527	71,563
✓ Oct 6th 2016 3:28am	Darknet	28	94
✗ Oct 6th 2016 3:03am	Darknet	22	94
✗ Oct 6th 2016 3:00am	Active Probing	208	949
✗ Oct 6th 2016 2:55am	BGP	70,255	71,563
✗ Oct 6th 2016 2:50am	Active Probing	603	949
✓ Oct 5th 2016 6:20am	Active Probing	791	950

Showing 1 to 15 of 30 entries

[Previous](#) [Next](#)

Regional Outages for Iraq

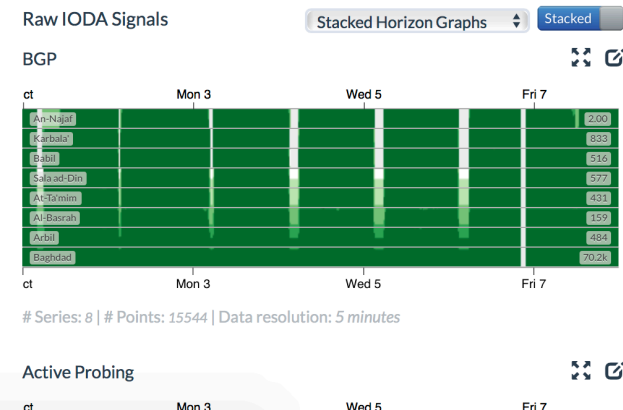


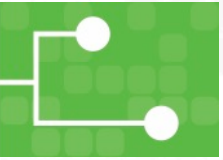
Outage Severity Levels

Show 10 entries

Search:

Region	Overall Score	Active Probing	BGP	Darknet
Baghdad	130M	97.8k	1.33k	
Al-Basrah	51.7M	1.60k	32.3k	
An-Najaf	91.3k		91.3k	
Babil	70.3k		70.3k	
Karbala'	68.9k		68.9k	
Sala ad-Din	62.7k		62.7k	








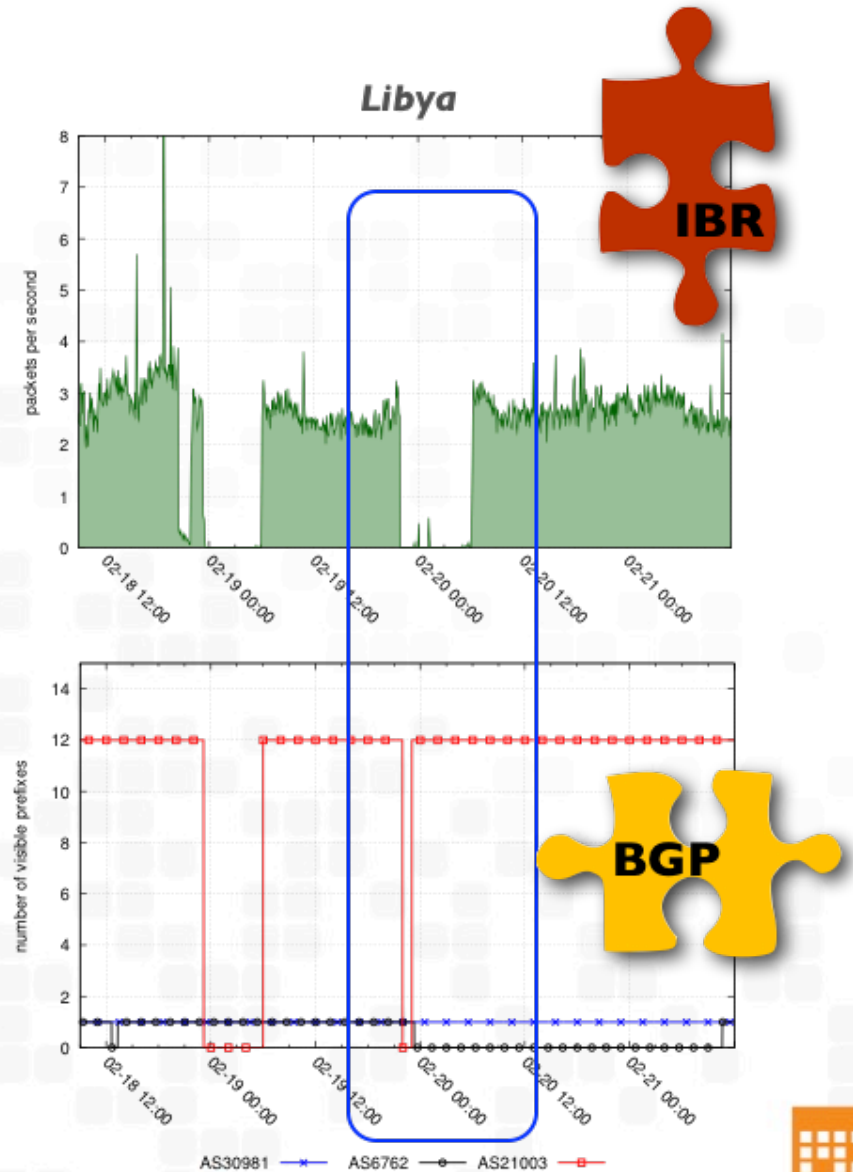
Benefits

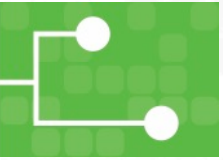
- Benefits
 - Near-realtime alerts
 - Multi-source
 - Visualization
 - API
- Risks / Challenges
 - Complex infrastructure
 - Improve resolution
 - Validation

*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 





Competition/Alternatives

- Oracle's Internet Intelligence Map
 - Focus on country-level
 - Limited interaction/viz functionalities in interface
- ISI / John Heidemann's work
 - IODA uses ISI Trinocular for one data source
 - IODA focuses on per-AS / geographic aggregations
- Akamai
 - State of the Internet reports and tweets
- Bgpmon.com
 - BGP only

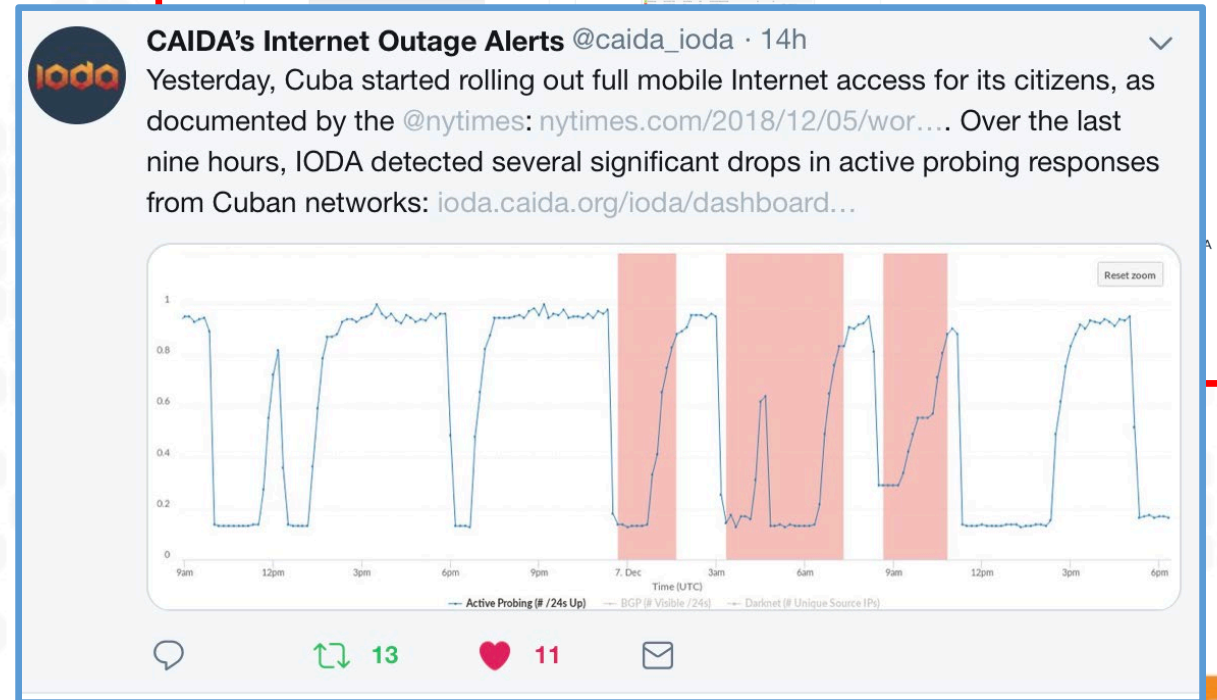
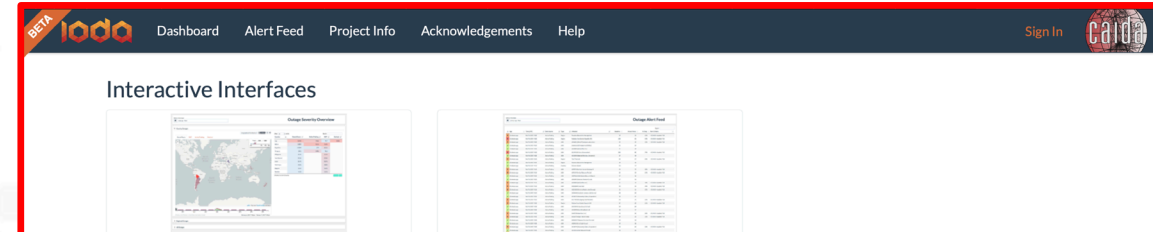




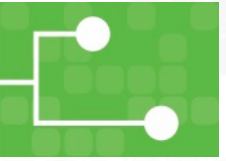
Current Status 1/2

<https://ioda.caida.org>

- Prototype running
 - Web dashboard
 - Tweets and blog posts
- Several events detected
- Deliverables:
 - Rigorous definitions (also for evaluation framework) [NID]
 - Methodology [NAFD]



 [@caida_ioda](https://twitter.com/caida_ioda)



Current Status 2/2

- Improvements to BGP Geolocation
- BGP detection new deployment
- Collection of Power Outages events
- A new detection model for IBR based on Seasonal ARIMA models
- Investigated cross/partial-24block outages

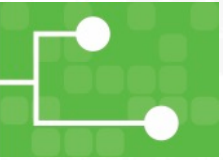




Next Steps

- Architectural improvements to IBR capture and processing infrastructure to reduce latency
- Deploy new SARIMA-based IBR detection
- Develop and deploy detection fusing multiple data sources
- API & Documentation
- Validation and reporting
- Investigate characteristics of outages in the US





Potential Transition Activities

- *Application: Public Safety, Situational Awareness, Disaster Recovery, Insurance, Internet Reliability & Performance*
- Year 3 Pilot Task
 - potential use by FCC or DHS NCICC
- Potential collaboration with industry
 - E.g. cyber-insurance
- Release components as open source





Contact Info

Alberto Dainotti

CAIDA, University of California San Diego

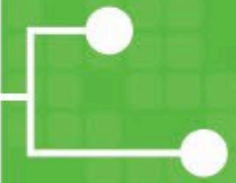
alberto@caida.org

+1-858-534-9249

🐦 @AlbertoDainotti

<https://ioda.caida.org> - 🐦 @caida_ioda





2019 S&T Cybersecurity and Innovation Showcase

Solutions Now | Innovations for the Future



Homeland
Security

Science and Technology

