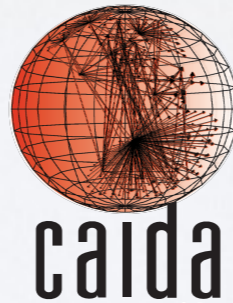


*IETF 94 - Technical Plenary  
4th Nov 2015, Yokohama, JP*

# *Measuring and Monitoring BGP*

**Alberto Dainotti,  
*alberto@caida.org***



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

# MEASURING BGP

Why?

**BGP is the central nervous system of the Internet**

**BGP's design** is known to contribute to issues in:

- **Availability**

- Labovitz et al. "*Delayed Internet Routing Convergence*", IEEE/ACM Trans. Netw., 2001.
- Varadhan et al. "*Persistent Route Oscillations in Inter-domain Routing*". Computer Networks, 2000.
- Katz-Bassett et al. "*LIFEGUARD: Practical Repair of Persistent Route Failures*", SIGCOMM, 2012.

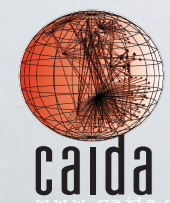
- **Performance**

- Spring et al. "*The Causes of Path Inflation*". SIGCOMM, 2003.

- **Security**

- Zheng et al. "*A Light-Weight Distributed Scheme for Detecting IP Prefix Hijacks in Realtime*". SIGCOMM, 2007.

**Need to engineer protocol evolution!**



# MEASURING BGP

## Why?

Defining problems and make **protocol engineering** decisions through realistic evaluations is difficult also because **we know little about the structure and dynamics of the BGP ecosystem!**

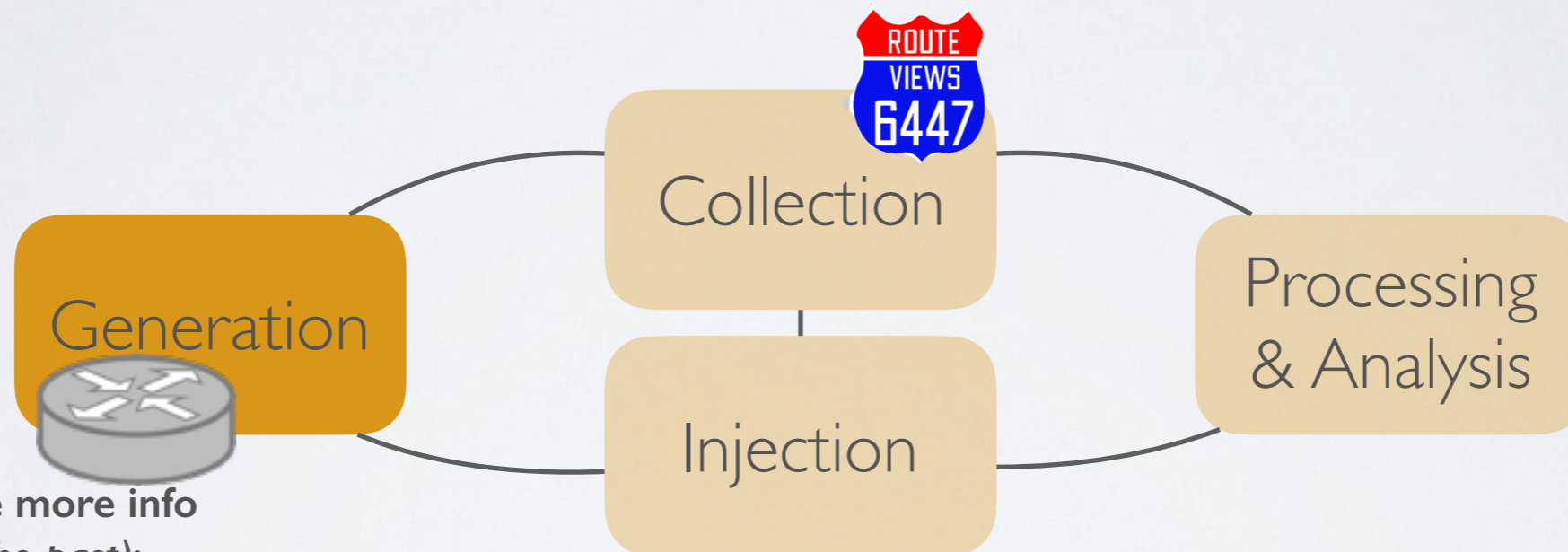
- AS-level topology
  - Gregori et al. “On the *incompleteness* of the AS-level graph: a novel methodology for BGP route collector placement”, IMC 2012
- AS relationships
  - Giotsas et al. “*Inferring* Complex AS Relationships”, IMC 2014
- AS interactions: driven by relationships, policies, network conditions, operator updates
  - Anwar et al. “*Investigating* Interdomain Routing Policies in the Wild”, IMC 2015
  - Lychev et al. “BGP *Security* in Partial Deployment: *Is the Juice Worth the Squeeze?*”, SIGCOMM 2013

# MEASURING BGP

*two issues - somehow related*

I. Literature shows that **we need more/better data**

- more info from the protocol/routers



Attempts to generate more info  
(not much traction in the past):

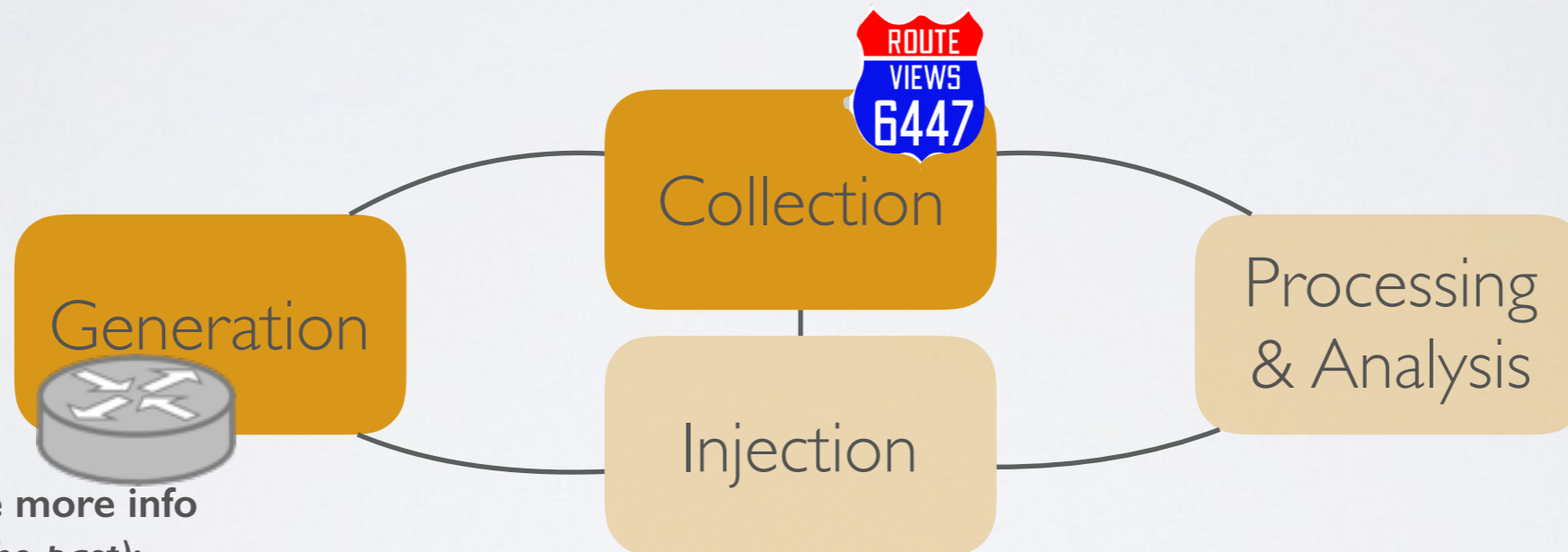
- RFC 4384 BGP Communities for Data Collection
- `draft-ymbk-grow-bgp-collector-communities`

# MEASURING BGP

*two issues - somehow related*

I. Literature shows that **we need more/better data**

- more info from the protocol/routers, more collectors,



Attempts to generate more info  
(not much traction in the past):

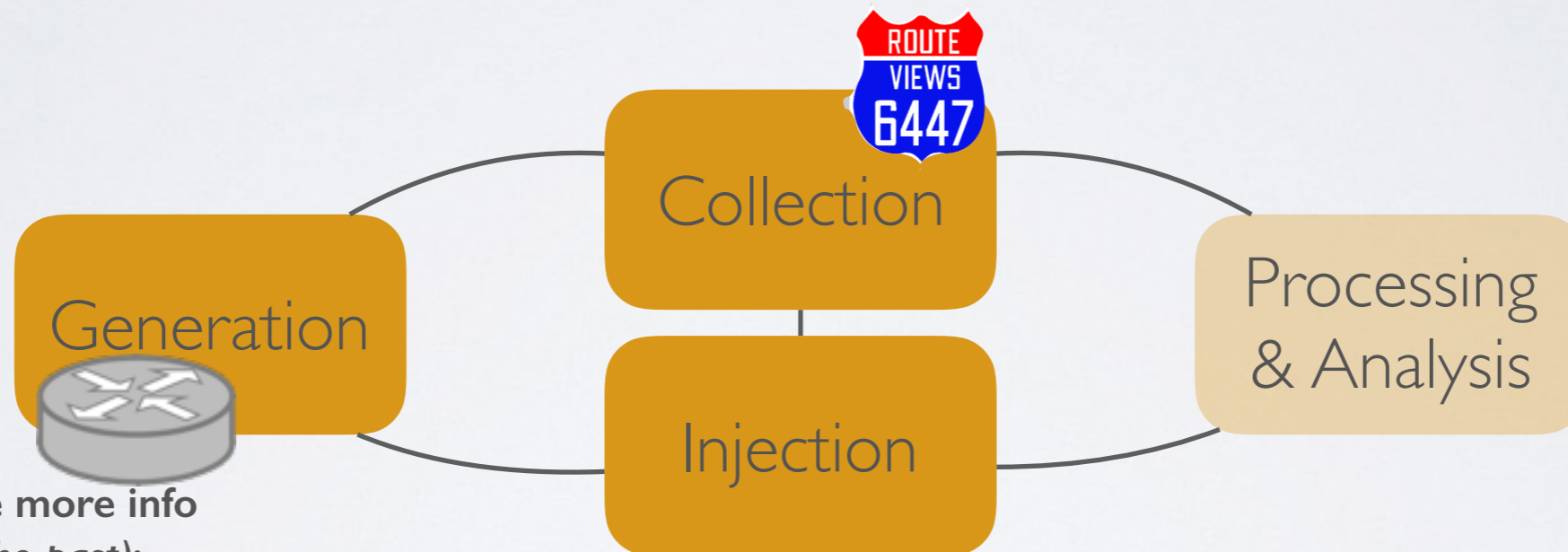
- RFC 4384 BGP Communities for Data Collection
- draft-ymbk-grow-bgp-collector-communities

# MEASURING BGP

*two issues - somehow related*

I. Literature shows that **we need more/better data**

- more info from the protocol/routers, more collectors, more experimental testbeds, ...



Attempts to generate more info  
(not much traction in the past):

- RFC 4384 BGP Communities for Data Collection
- draft-ymbk-grow-bgp-collector-communities

Inject/Receive Routes & Traffic.  
PEERING - <http://peering.usc.edu>  
Schlinker et al. "PEERING: An AS for Us", HotNets 2014

# MEASURING BGP

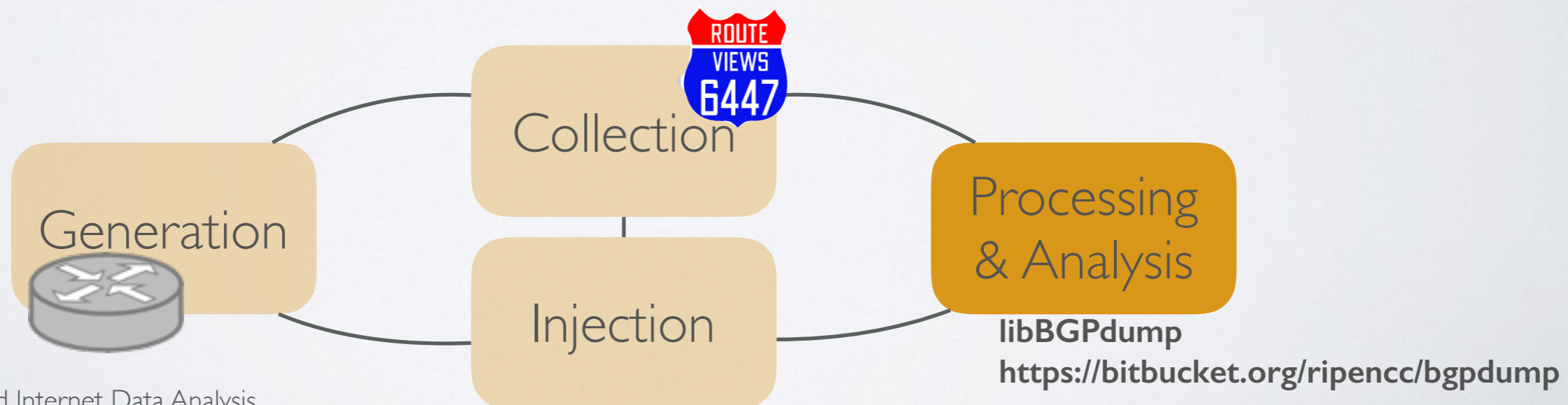
*two issues - somehow related*

1. Literature shows that **we need more/better data**

- more info from the protocol/routers, more collectors, more experimental testbeds, ...

2. But we also **need better tools to learn from the data**

- to make data analysis: *easier, faster, able to cope with BIG and heterogeneous data*
- to monitor BGP in near-realtime
- tightening data collection, processing, visualization, ...



# BGP EVENTS & DYNAMICS

## *IODA: Detection and Analysis of Internet Outages*

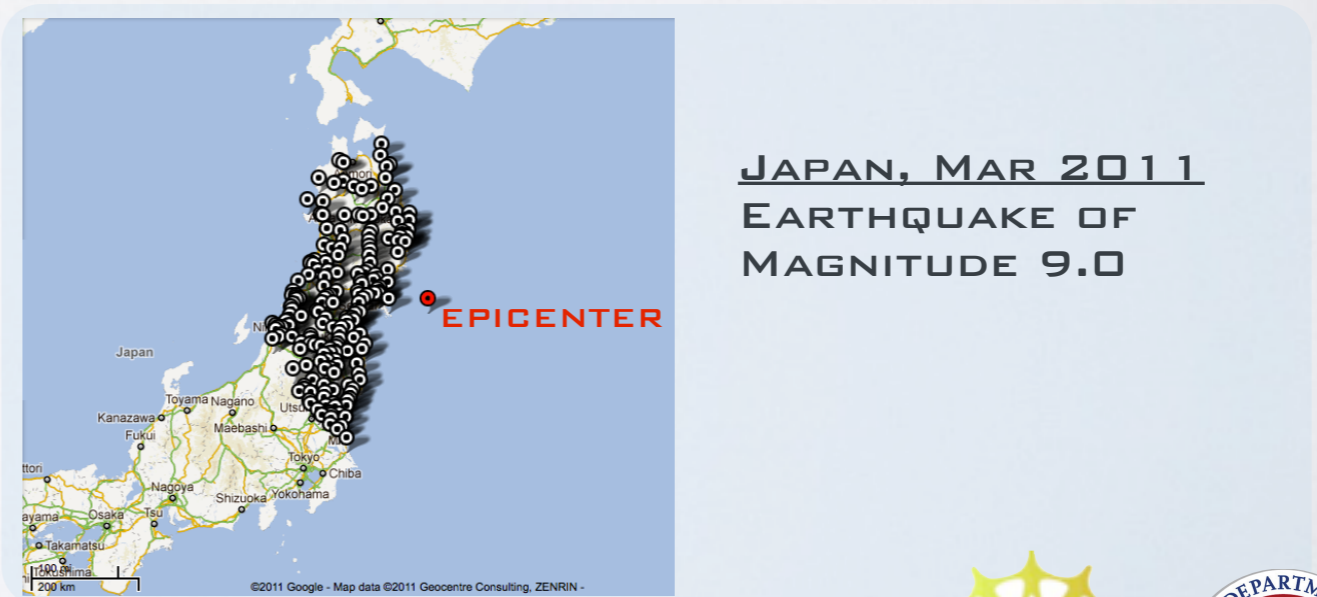
- Country-level Internet Blackouts during the Arab Spring

*Dainotti et al. "Analysis of Country-wide Internet Outages Caused by Censorship"*  
IMC 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"*  
SIGCOMM CCR 2012

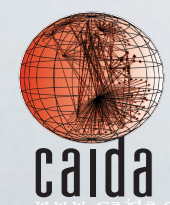
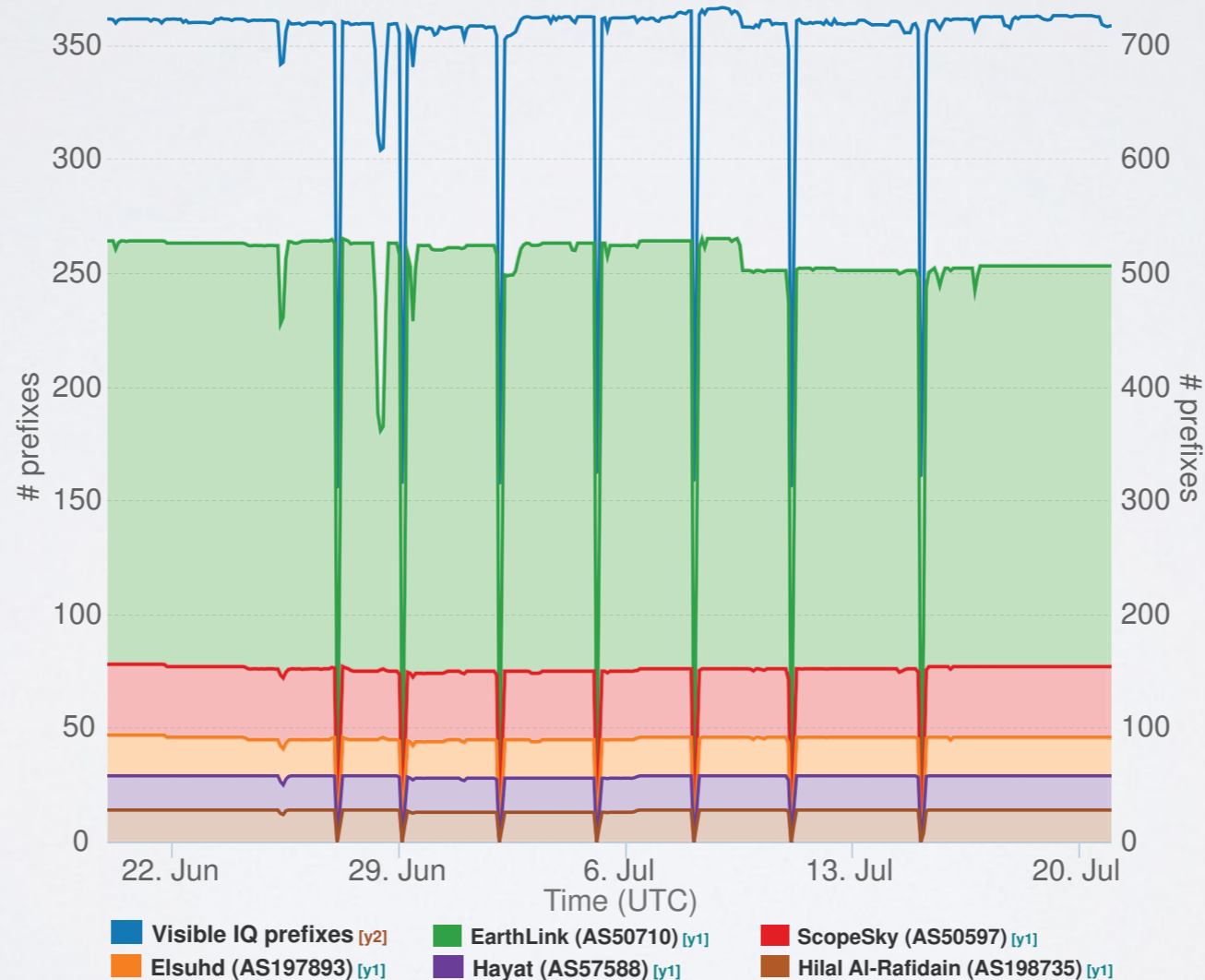




# BGP EVENTS & DYNAMICS

## *IODA: Detection and Analysis of Internet Outages*

Country-wide Internet outages in Iraq that the government ordered in conjunction with the ministerial preparatory exams - Jul 2015



Center for Applied Internet Data Analysis  
University of California San Diego

[www.caida.org/funding/iodal/](http://www.caida.org/funding/iodal/)



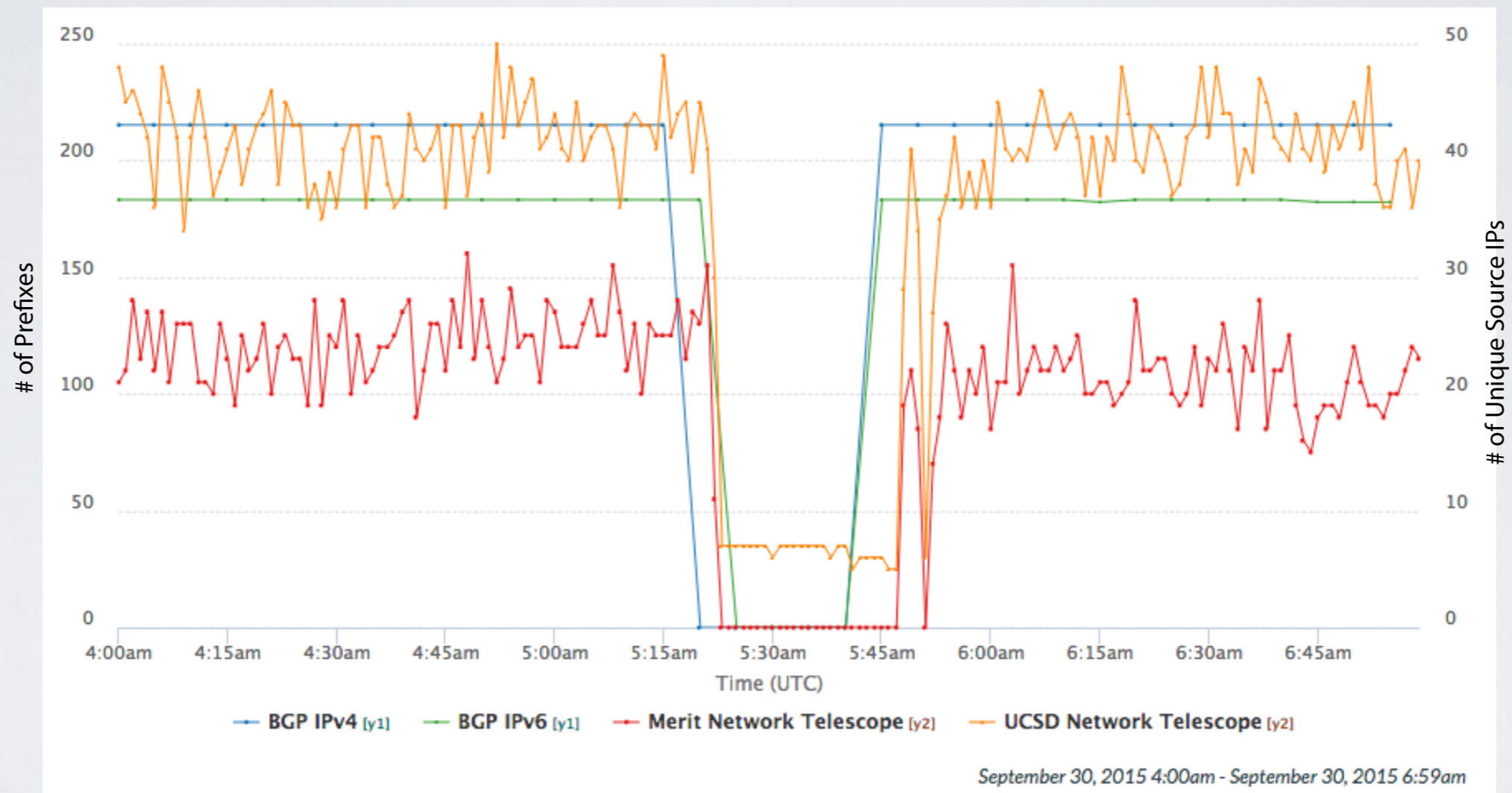
COMCAST



# BGP EVENTS & DYNAMICS

## *IODA: Detection and Analysis of Internet Outages*

Outage of AS11351 (Time Warner Cable LLC)  
September 30, 2015

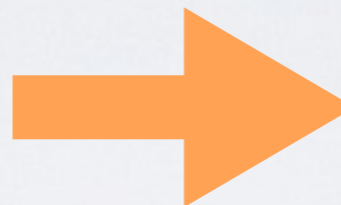


# BEFORE IODA

## 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 2011, several North African countries and those of the Middle East experienced a series of internet outages. In this paper, we analyze the traffic patterns of these outages, using a combination of network-level data, application-level data, and user reports. We use this information to determine which outages are caused by BGP announced outages, which are caused by local network outages, and which are caused by a combination of the two. We then analyze the impact of these outages on the Internet as a whole, and on the specific countries affected. Our analysis shows that the outages are caused by a combination of BGP announced outages and local network outages. The impact of these outages is significant, as they affect a large number of users and services. We discuss the implications of these findings for the future of the Internet in the Middle East and North Africa.

Categories and Subject Descriptors  
C.2.3 [Networks]: Internet  
C.2.1 [Local and Wide Area Networks]

General Terms  
Measurement, Security

Permission to make digital or hard copies of this work for personal or classroom use is granted by ACM, provided that the fee code for users to reproduce this work is paid to ACM. Copyright 2011 ACM 978-0-955-585-24-1/11/000000...\$10.00.

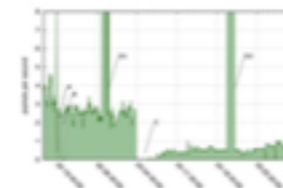


Figure 12: UCSD telescope's traffic coming from Libya. Labels A, B, C indicate the three outages. Points labeled D1 and D2 are due to background fluctuations of service attacks.

related to protests in the country. The web site of the Ministry of Communications ([www.mca.gov.ly](http://www.mca.gov.ly)) was attacked with a randomly-specified 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 backbone traffic to the Internet shows a significant increase in 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](http://www.moi.gov.eg)) was targeted by two DoS attacks just after the end of the censorship from 13:08 to 13:30 GMT and from 15:08 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 [36], 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.

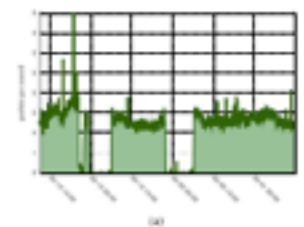
In Libya three different outages in early 2011 were identified and publicly discussed (Figure 1). Figure 12 shows the traffic observed by the UCSD network telescope from Libya throughout an interval encompassing the outages. The points labeled A, B, and C indicate three different blackout episodes; points 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

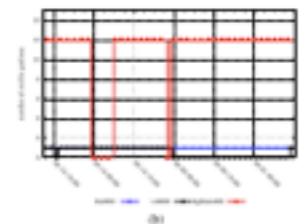
The first two outages happened during two consecutive nights. Figure 13(a) shows a more detailed view of these two outages as observed by the UCSD telescope. Figure 13(b) shows BGP data over the same interval: in both cases, within a few minutes, 12 out of the 15 IPv4 prefixes associated with IP address ranges officially delegated to Libya were withdrawn. These twelve IPv4 prefixes were announced by LibNetAS, the local telecom operator, while the remaining IPv4 prefixes were managed by IRIAS2. As of May 2011, there were no IPv4 prefixes in IRIAS2'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 SatAS, 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 dataset generally observed a significant amount of truncated traffic coming from IPs in those 12 ranges before the first outage (about 5k 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 23:58:55 UTC, exactly matching the sharp decrease of distinct traffic from Libya (and in accordance with reports on Libyan traffic seen by Aben Networks [14]) 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-



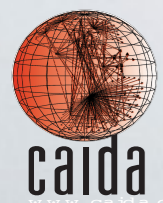
(a)



(b)

Figure 13: The first two Libyan outages: (a) uncollected traffic to UCSD dataset coming from Libya; (b) visibility of Libyan IPv4 prefixes in BGP data from Rome/Aben and RIPE NCC/RIPE collectors. Note that the corresponding and data plane observations of connectivity do not match, suggesting that different techniques for censorship were being used during different intervals.

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



Center for Applied Internet Data Analysis  
University of California San Diego

# IODA TODAY

*live Internet monitoring*

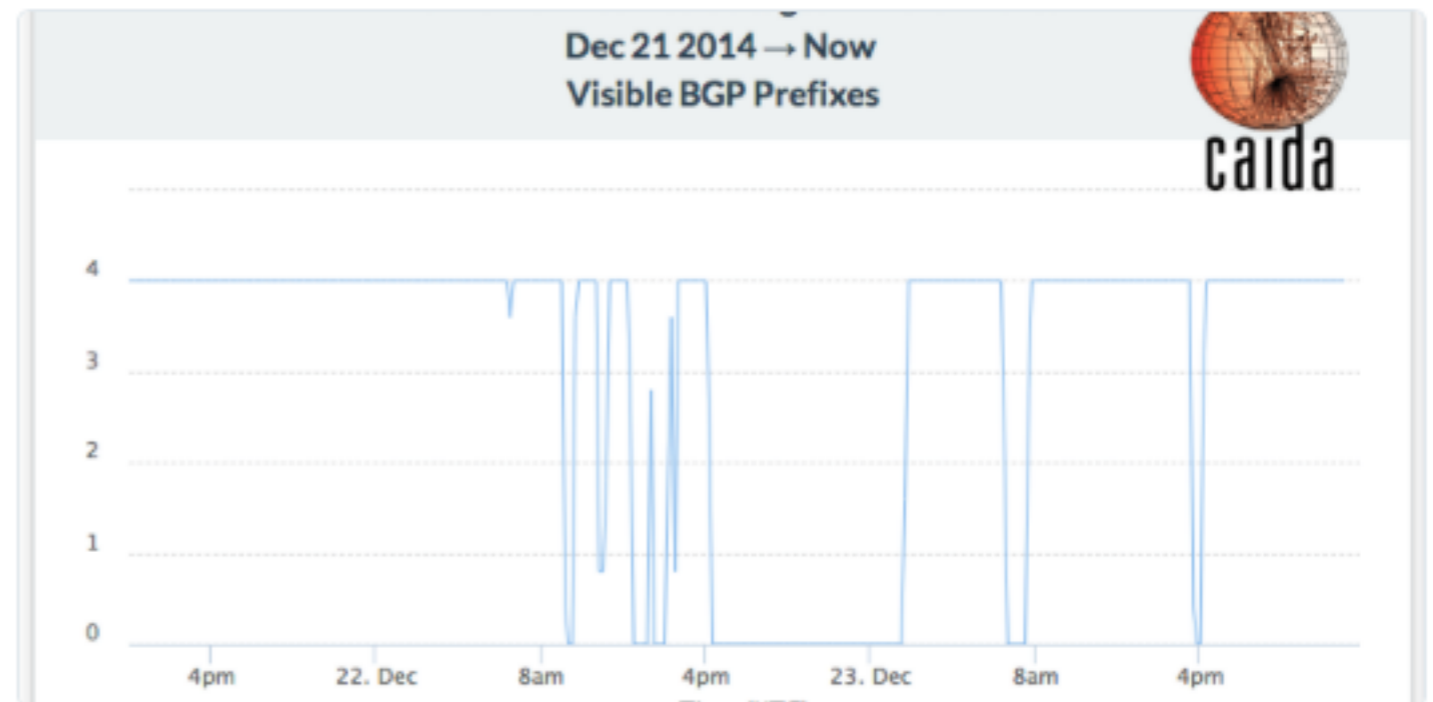


*Last Christmas we made it possible for anybody to follow the North Korean disconnection almost live*



CAIDA @caidaorg · Dec 23

Follow outages in #NorthKoreaInternet in almost real-time (30min delay) at [charthouse.caida.org/public/kp-outage...](https://charthouse.caida.org/public/kp-outage)

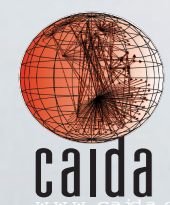


↻ 3

★ 4



[View more photos and videos](#)



Center for Applied Internet Data Analysis  
University of California San Diego

<https://charthouse.caida.org/public/kp-outage>

# MEASURING BGP

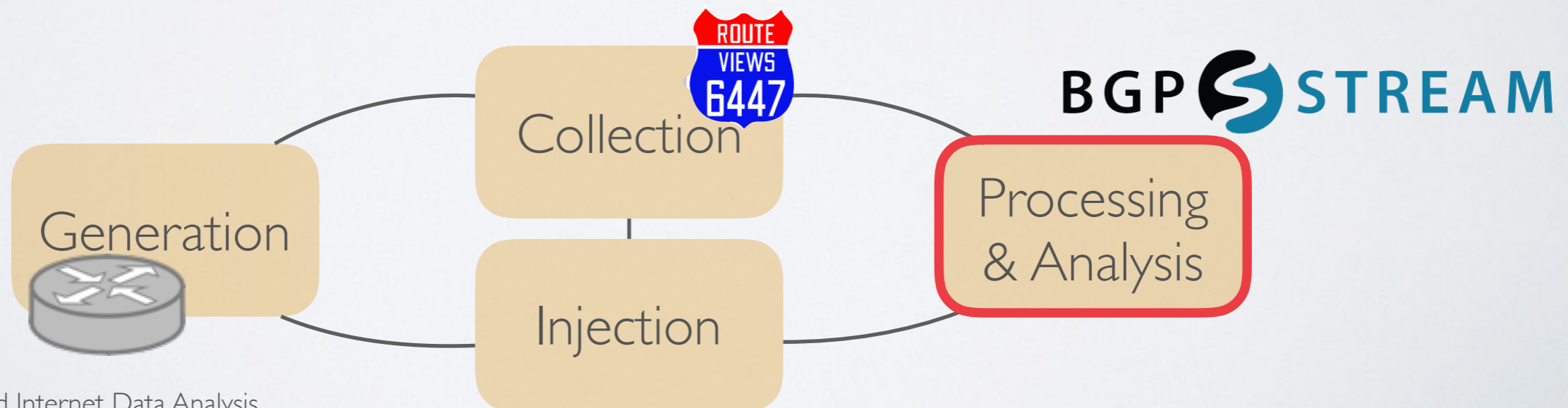
*two issues - somehow related*

1. Literature shows that **we need more/better data**

- more info from the protocol/routers, more collectors, more experimental testbeds, ...

2. But we also **need better tools to learn from the data**

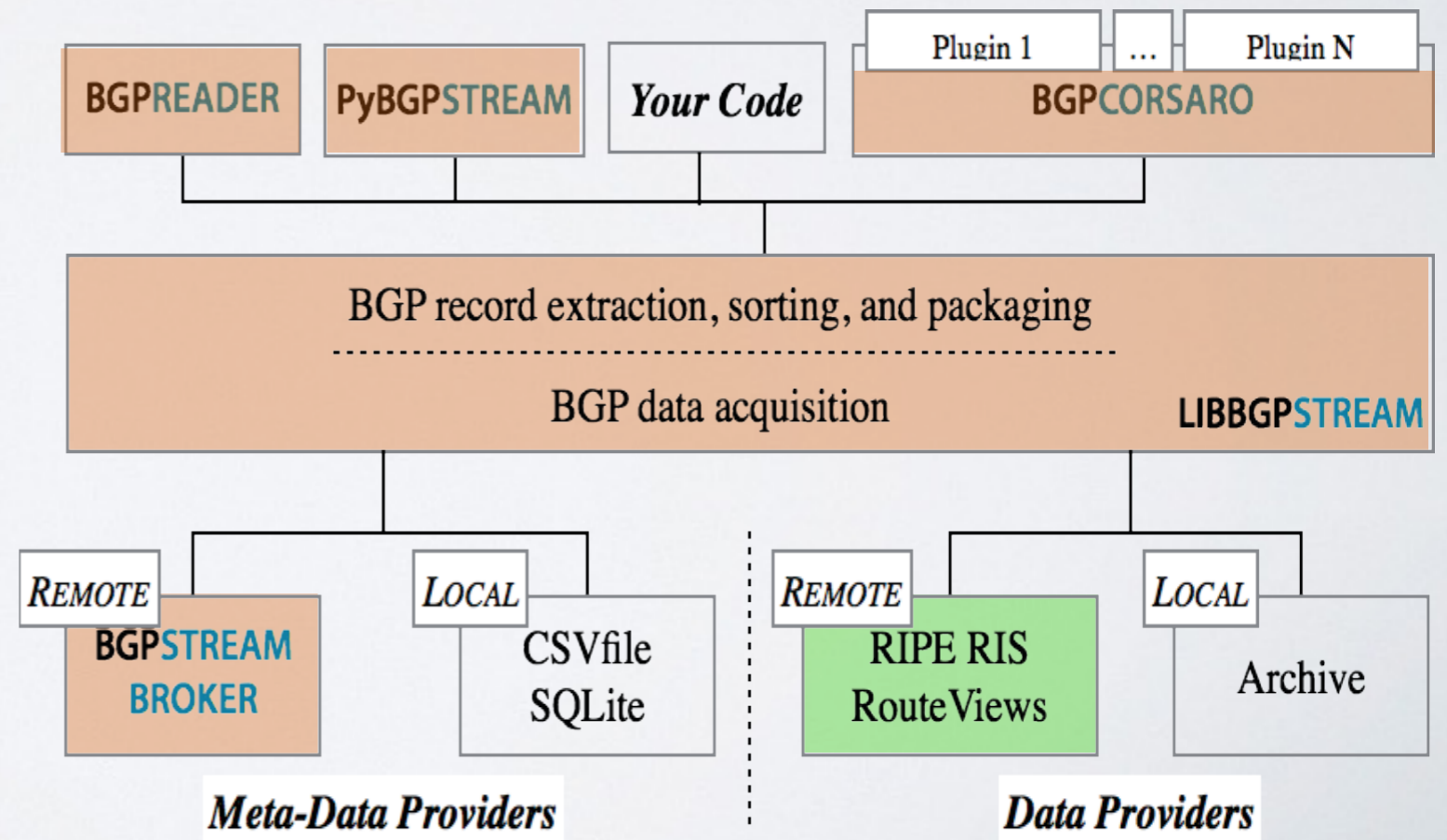
- to make data analysis: *easier, faster, able to cope with BIG and heterogeneous data*
- to monitor BGP in near-realtime
- tightening data collection, processing, visualization, ...



# BGP STREAM

[bgpstream.caida.org](http://bgpstream.caida.org)

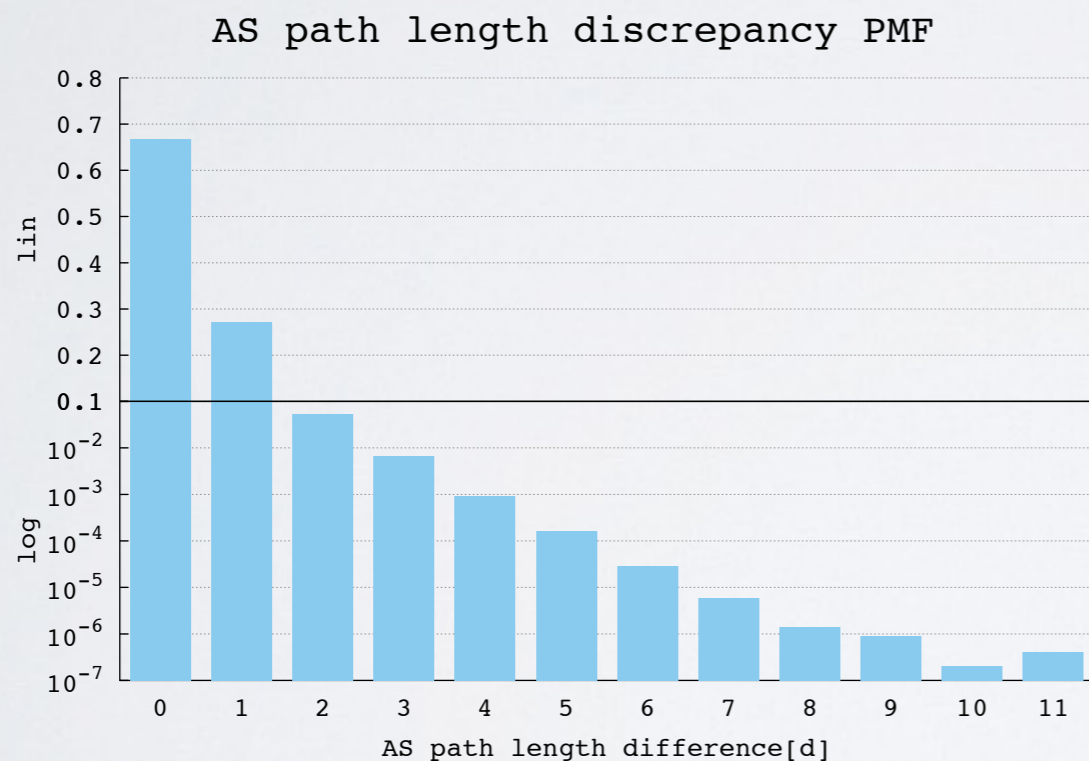
- A software framework for **historical** and **live** BGP data analysis
- Design goals:
  - Efficiently deal with large amounts of distributed BGP data
  - Offer a time-ordered data stream of data from heterogeneous sources
  - Support near-realtime data processing
  - Target a broad range of applications and users
  - Scalable
  - Easily extensible



# PYBGPSTREAM

## Example: studying AS path inflation

How many AS paths are longer than the shortest path between two ASes due to routing policies? (directly correlates to the increase in *BGP convergence time*)



```
1 from _pybgpstream import BGPStream, BGPRecord, BGPElem
2 from collections import defaultdict
3 from itertools import groupby
4 import networkx as nx
5
6 stream = BGPStream()
7 as_graph = nx.Graph()
8 rec = BGPRecord()
9 bgp_lens = defaultdict(lambda: defaultdict(lambda: None))
10 stream.add_filter('record-type', 'ribs')
11 stream.add_interval_filter(1438415400, 1438416600)
12 stream.start()
13
14 while(stream.get_next_record(rec)):
15     elem = rec.get_next_elem()
16     while elem:
17         monitor = str(elem.peer_asn)
18         hops = [k for k, g in groupby(elem.fields['as-path'].split(" "))
19                 if len(hops) > 1 and hops[0] == monitor)
20         origin = hops[-1]
21         for i in range(0, len(hops)-1):
22             as_graph.add_edge(hops[i], hops[i+1])
23             bgp_lens[monitor][origin] = \
24                 min(filter(bool, [bgp_lens[monitor][origin], len(hops)]))
25         elem = rec.get_next_elem()
26 for monitor in bgp_lens:
27     for origin in bgp_lens[monitor]:
28         nxlen = len(nx.shortest_path(as_graph, monitor, origin))
29         print monitor, origin, bgp_lens[monitor][origin], nxlen
```

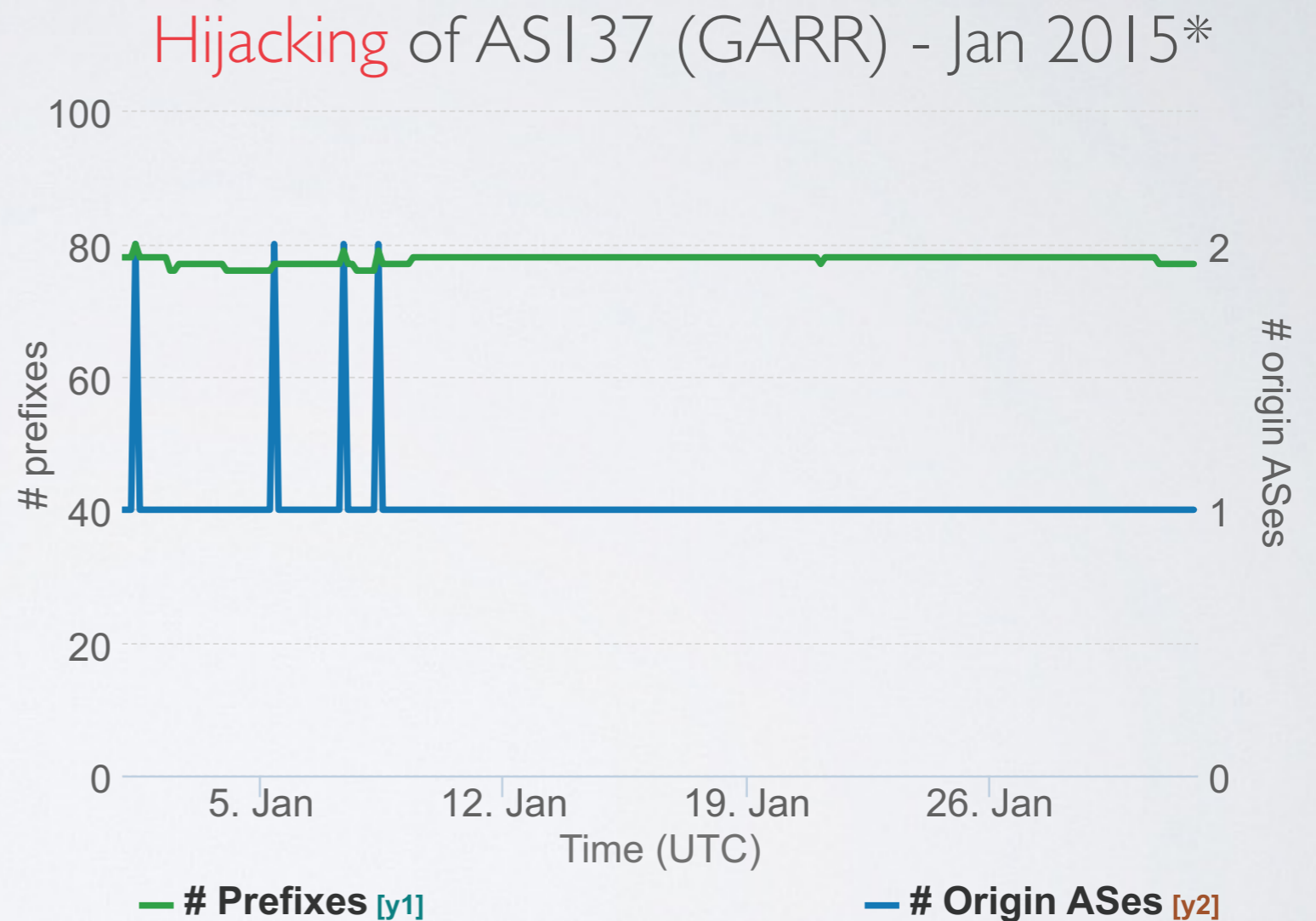
30 LINES OF  
PYTHON CODE

# BGPCORSARO

*Example: monitor your own address space on BGP*

The “**prefix-monitor**” plugin  
(distributed with source)  
monitors a set of IP ranges as  
they are seen from BGP monitors  
distributed worldwide:

- how many prefixes reachable
- how many origin ASes
- generates detailed logs



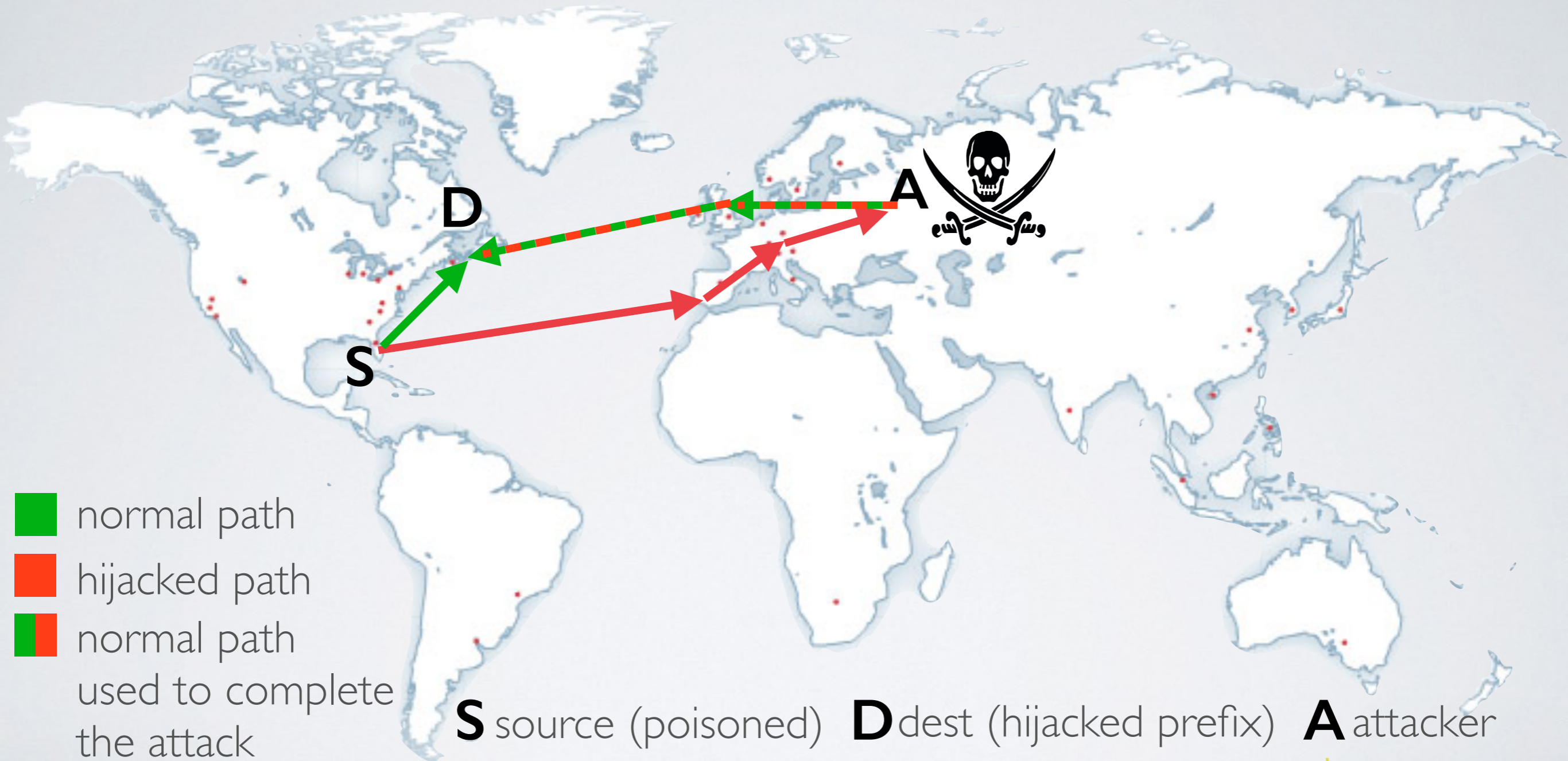
\*Originally discovered by Dyn:

<http://research.dyn.com/2015/01/vast-world-of-fraudulent-routing/>



# ANOTHER SUPPORTED PROJECT

*Hijacks: detection of MITM BGP attacks*

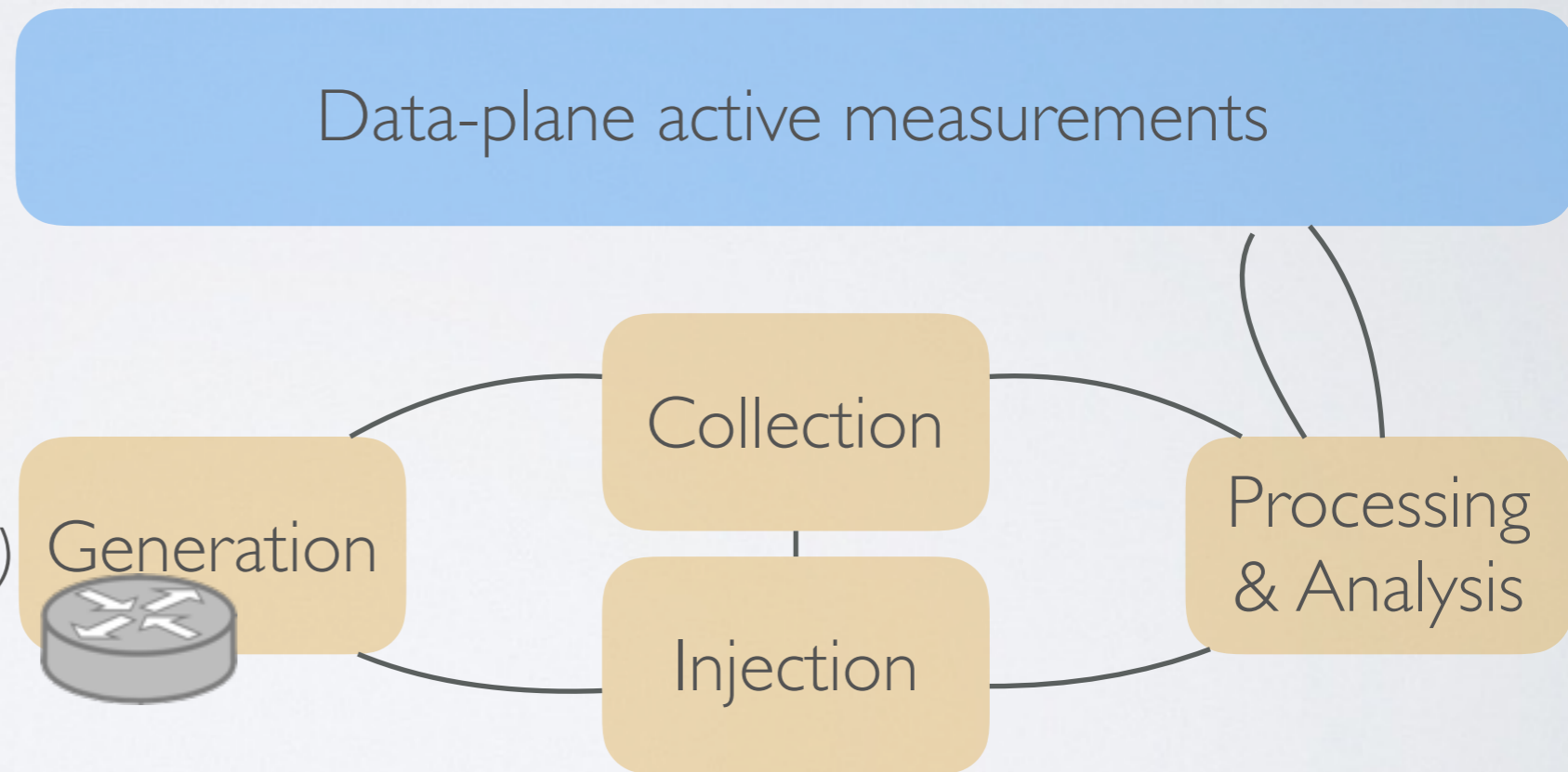


# ANOTHER SUPPORTED PROJECT

## *Hijacks: detection of MITM BGP attacks*

Research informed by (and tested with) **data in the wild**

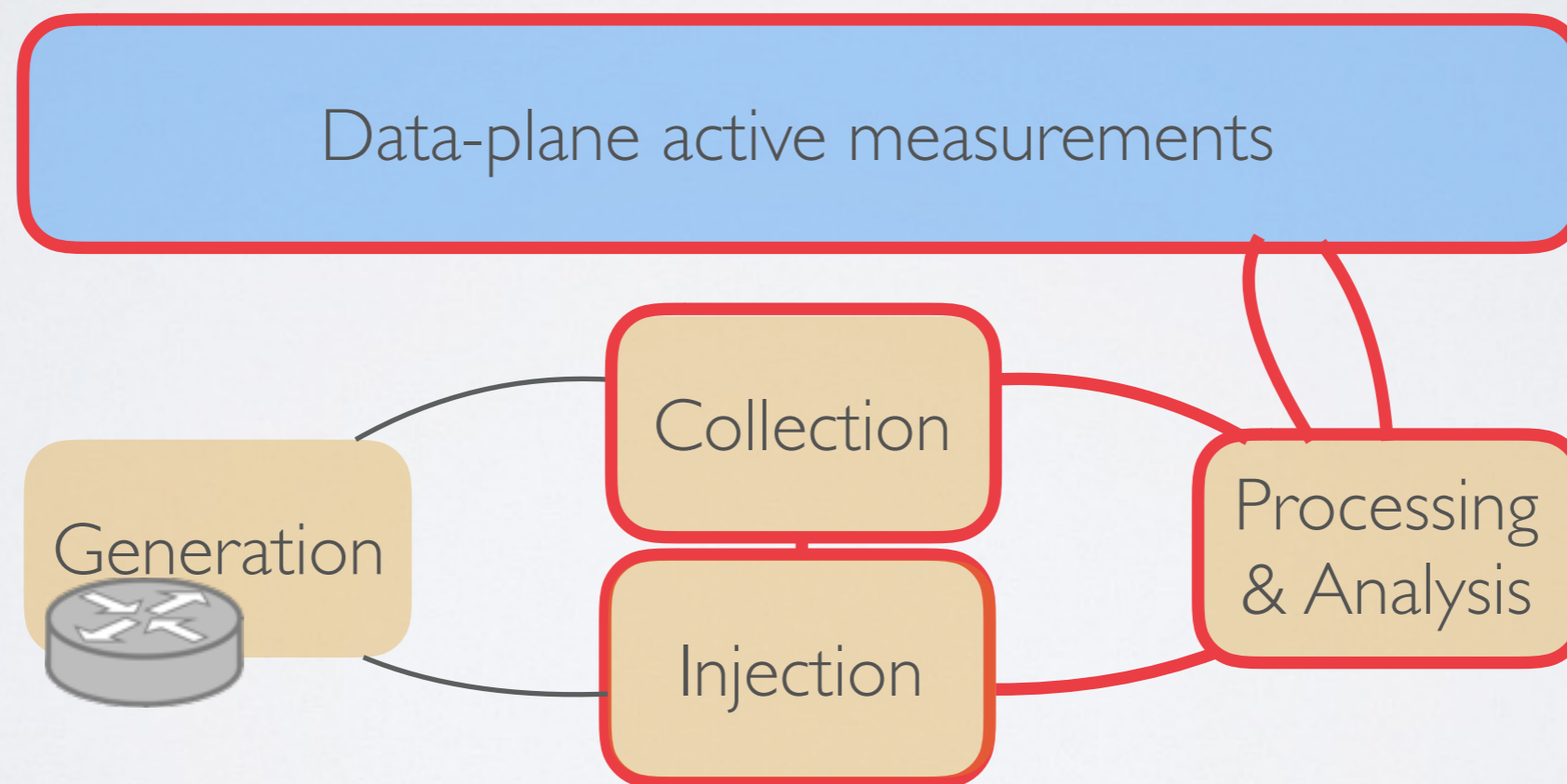
Live BGP measurements trigger on-demand dataplane measurements (e.g., traceroutes) **during** a suspicious event.



# BGP HACKATHON - FEB 2016

theme: “**live** BGP measurements & monitoring”

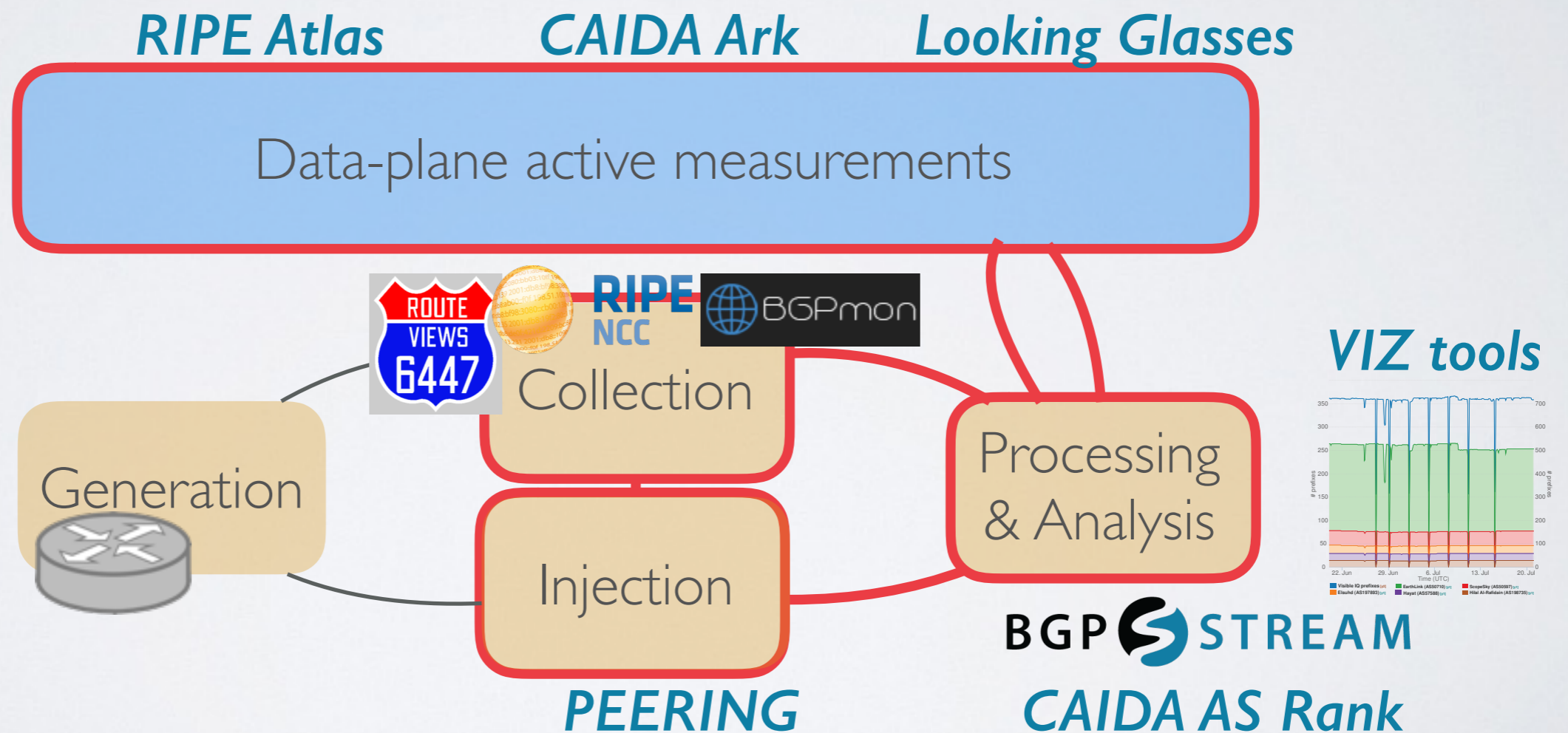
Improve/Integrate tools to study the BGP eco-system. Target practical problems: topology, hijacks, outages, RPKI deployment, path inflation, circuitous paths, policies, relationships, visualize dynamics, ...



# BGP HACKATHON - FEB 2016

theme: “**live** BGP measurements & monitoring”

We will provide a rich toolbox and “live” data access:



# BGP HACKATHON

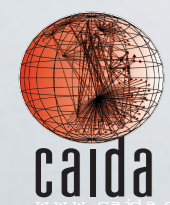
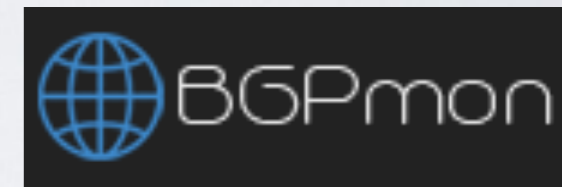
<http://github.com/CAIDA/bgp-hackathon/wiki>

- **6-7 February 2016** (weekend before NANOG 66)
- **San Diego** Supercomputer Center, UC San Diego
- **Theme: live BGP measurements** and monitoring
- Toolbox: *BGPMon, RIPE RIS, PEERING, BGPStream, RIPE Atlas, CAIDA Archipelago, Route Views, looking glasses, AS relationships, AS Rank, Visualization tools, ...*

- How to **contribute:**

- *join us and come over to hack!*
- *help teams as a domain expert*
- *propose projects that hacking teams may pick*
- *offer to join the jury that will assign awards*

>>> [bgp-hackathon-info@caida.org](mailto:bgp-hackathon-info@caida.org) <<<



Center for Applied Internet Data Analysis  
University of California San Diego

# THANKS

[bgpstream.caida.org](http://bgpstream.caida.org)

[github.com/CAIDA/bgp-hackathon/wiki](https://github.com/CAIDA/bgp-hackathon/wiki)

