IETF 84 - IRTF Open Meeting
July 31, 2012- Vancouver, Canada

Analysis of Country-wide Internet Outages Caused by Censorship

A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, A. Pescapé

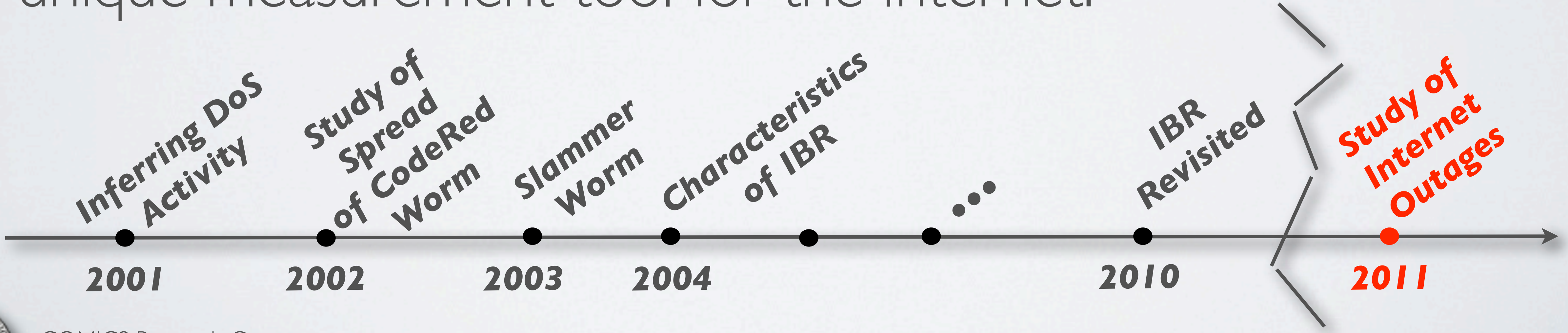
alberto@caida.org
Cooperative Association for Internet Data Analysis
University of California, San Diego

CONTEXT

Project goal & main message

- Analysis of **macroscopic Internet events** using multiple large-scale data sources

- Revival of Network Telescopes: ***Internet Background Radiation*** can be used as a unique measurement tool for the Internet!



Inferring DoS Activity

2001

Study of Spread of CodeRed Worm

2002

Slammer Worm

2003

Characteristics of IBR

2004

...

IBR Revisited

2010

Study of Internet Outages

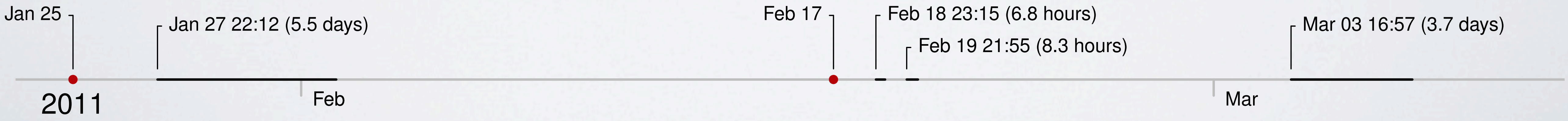
2011

THE EVENTS

Internet Disruptions in North Africa

- Egypt
  - *January 25th, 2011*: protests start in the country
  - The government orders service providers to "shut down" the Internet
  - ***January 27th, around 22:34 UTC***: several sources report the withdrawal in the Internet's global routing table of almost all routes to Egyptian networks
  - The disruption lasts ***5.5 days***

- Libya
  - *February 17th, 2011*: protests start in the country
  - The government controls most of the country's communication infrastructure
  - ***February 18th (6.8 hrs), 19th (8.3 hrs), March 3rd (3.7 days):*** three different connectivity disruptions:



NETWORK INFO

Prefixes, ASes, Filtering

- Egypt
  - **3165 *IPv4*** and 6 *IPv6* **prefixes** are delegated to Egypt by AfriNIC
  - They are managed by **51 Autonomous Systems**

  - **Filtering** type: **BGP only**
  - Filtering dynamic: synchronized; progressive

- Libya
  - **13 *IPv4* prefixes**, no *IPv6* prefixes
  - **3 Autonomous Systems** operate in the country

  - **Filtering** type: mix of **BGP, packet filtering, satellite signal jamming**
  - Filtering dynamic: testing different techniques; somehow synchronized

WHAT WE DID

Combined different measurement sources

- BGP
  - BGP updates from route collectors of ***RIPE-NCC RIS*** and ***RouteViews***
  - We combined information from both databases
  - Graphical Tools: ***REX***, ***BGPlay***, ***BGPviz***

- Active Traceroute Probing
  - Archipelago Measurement Infrastructure (***ARK***)
  - We underutilized this data source..
- Internet Background Radiation (IBR)
  - Traffic reaching the ***UCSD Network Telescope***
  - Capable of revealing different kinds of blocking

ROUTE VIEWS 6447

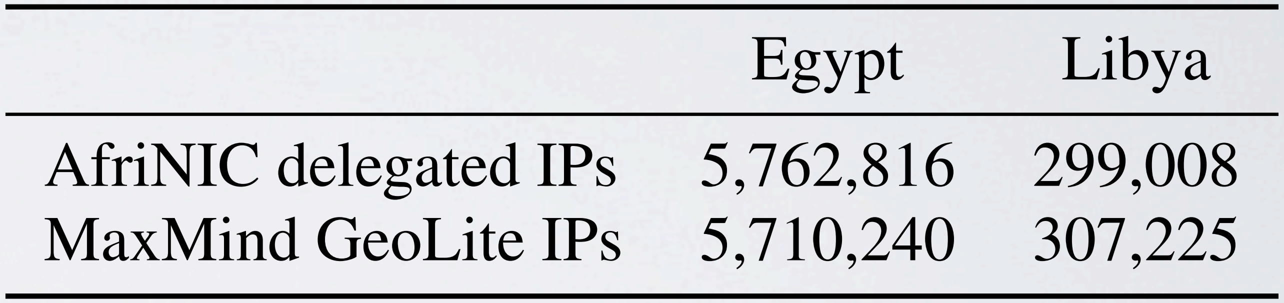
RIPE NCC

caida www.caida.org

DATA SELECTION

Geolocation + announced prefixes

- IP ranges associated with the country of interest
  - Delegations from Regional Internet Registries (RIR)
  - Commercial geolocation database



	Egypt	Libya
AfriNIC delegated IPs	5,762,816	299,008
MaxMind GeoLite IPs	5,710,240	307,225

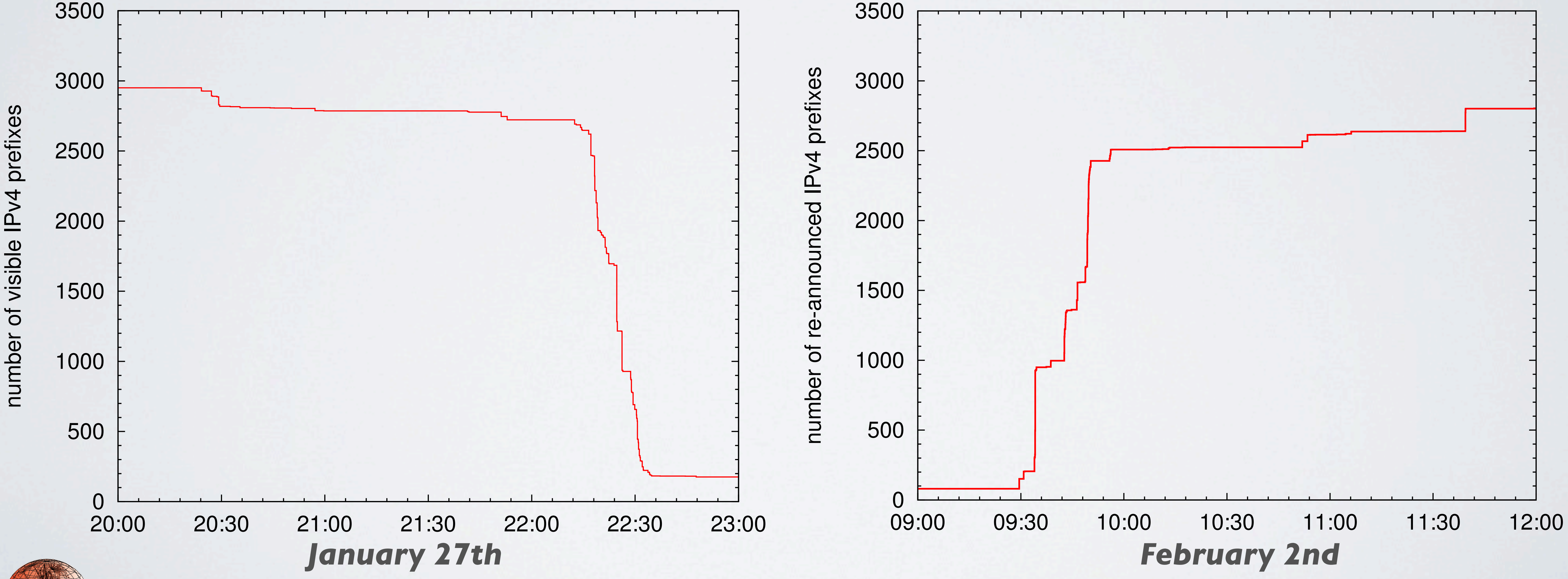
- Gather prefixes to be monitored by looking at BGP announcements. For each IP range:
  - Look up for an exactly matching BGP prefix
  - Find all the more specific (strict subset, longer) prefixes
  - Otherwise, retrieve the longest BGP prefix entirely containing it
- When referring to an AS, we actually refer to the IPs of that AS that are associated with the country of interest

BGP

prefix reachability

- We reconstruct prefixes losing and regaining reachability
  - we build the routing history of every collector's peer for each collector
  - using both RIBs and UPDATES
  - we mark a prefix as disappeared if it is withdrawn in each routing history

Egyptian disconnection and reconnection NOTE: IPv6 routes stayed up!

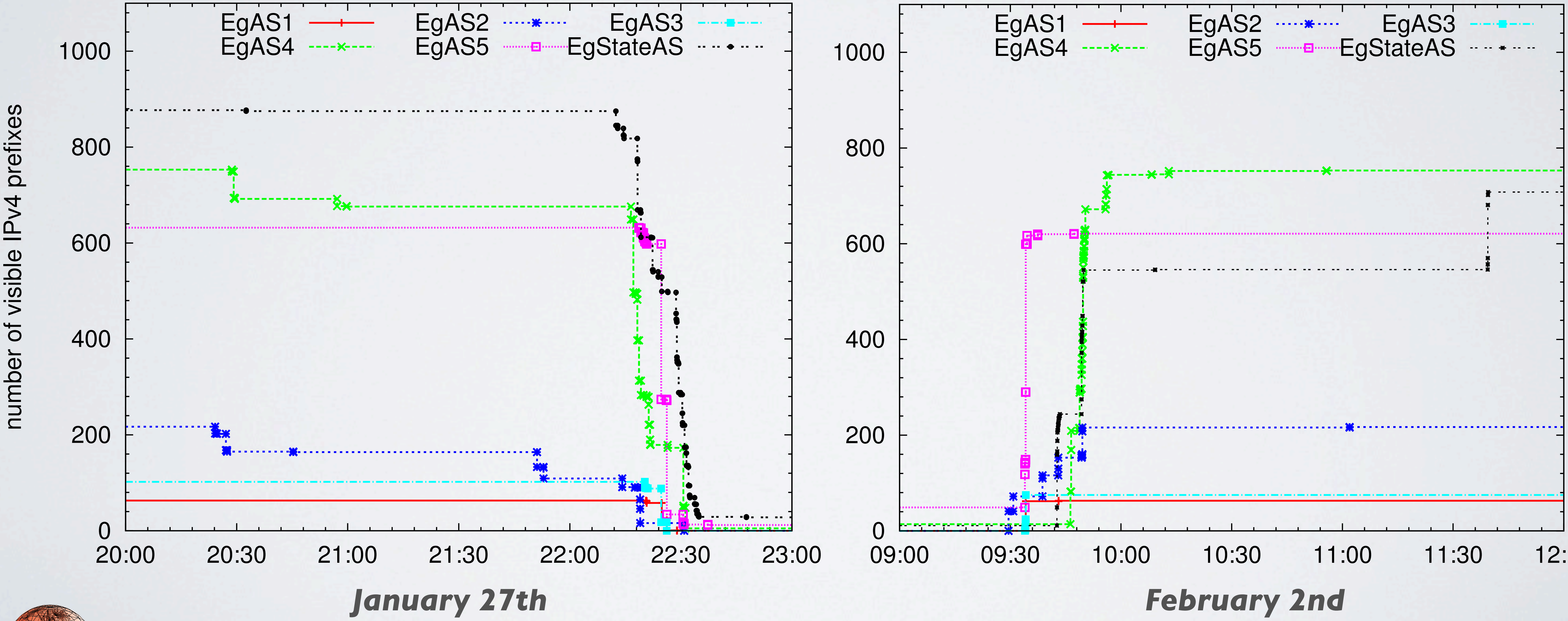


BGP

per-AS analysis

- A detailed analysis shows there is synchronization among ASes

Detail of Egyptian disconnection/reconnection: 6 major ASes



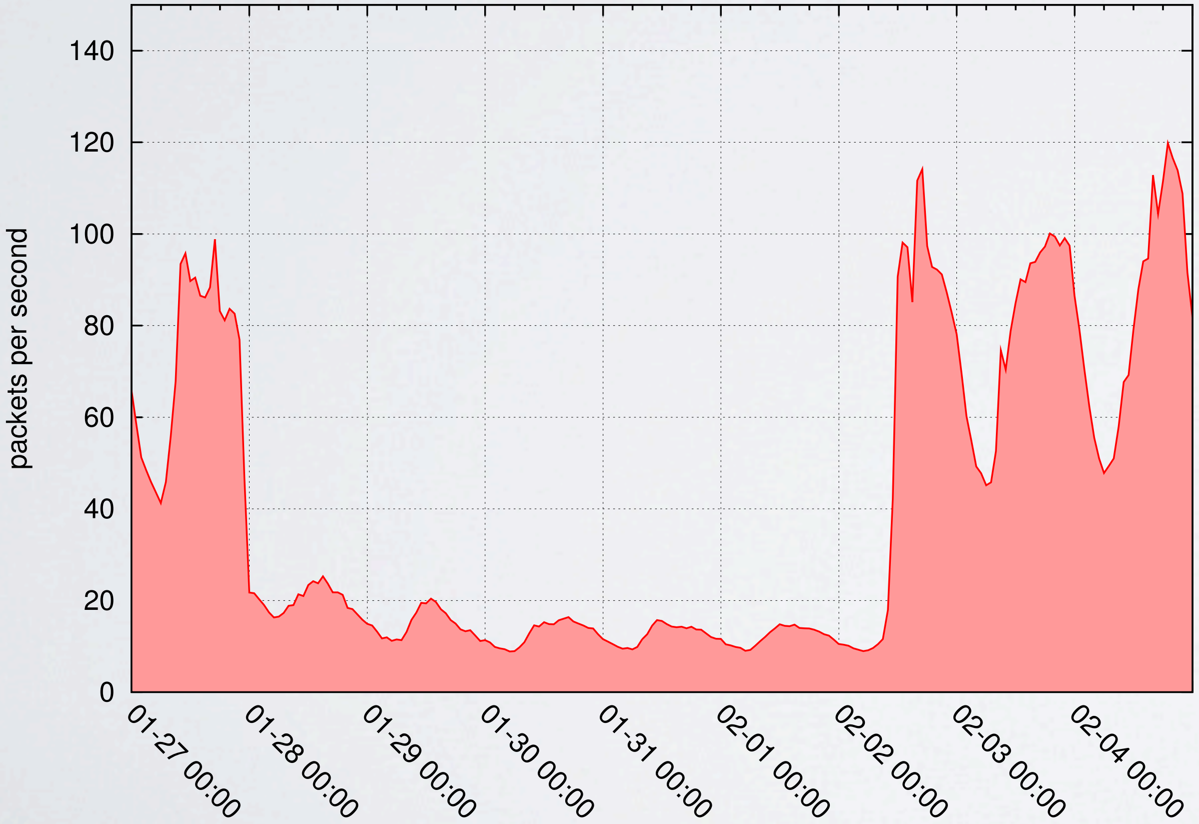
Cooperative Association for Internet Data Analysis
University of California San Diego

UCSD TELESCOPE

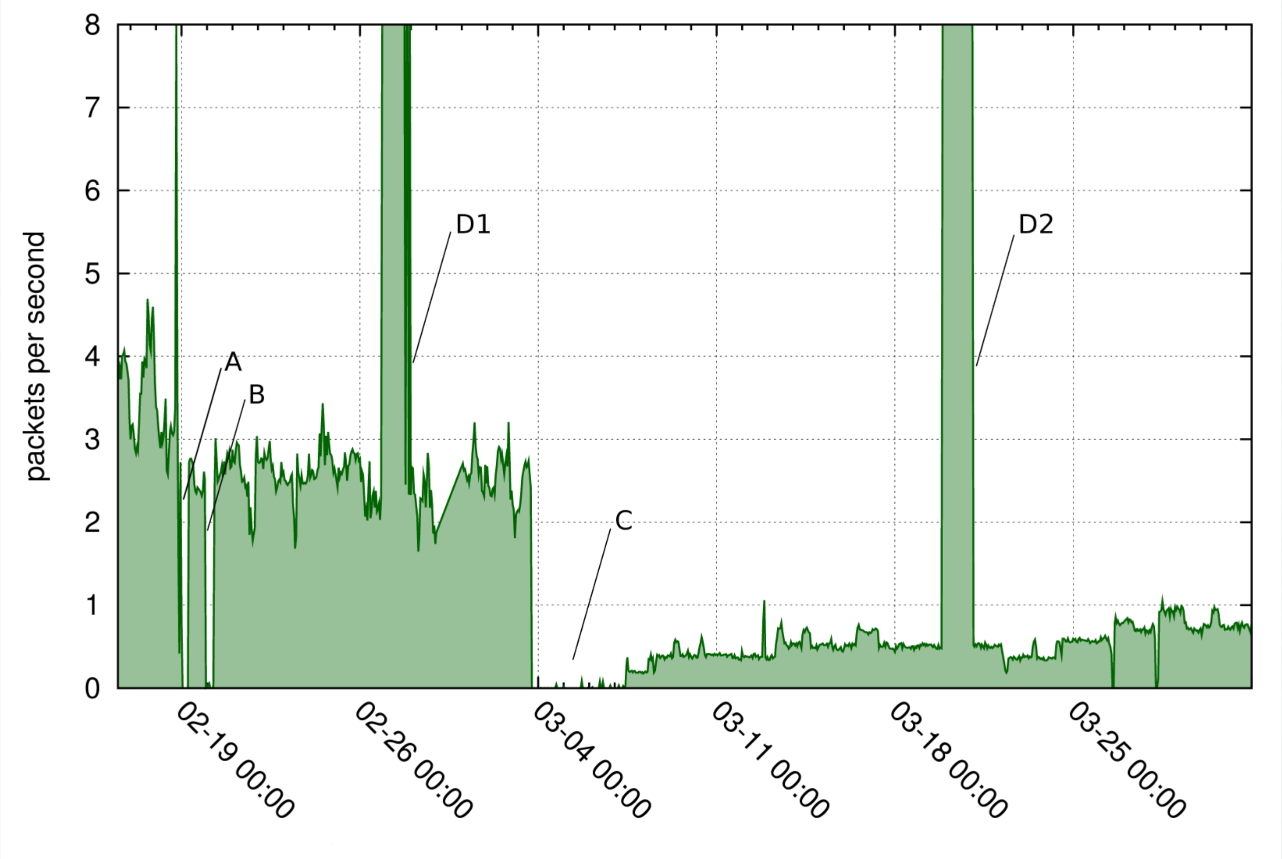
when malware helps..

- Unsolicited traffic, *a.k.a. Internet Background Radiation* - e.g. scanning from conficker-infected hosts - from the observed country reveals several aspects of these outages!

Egypt



Libya



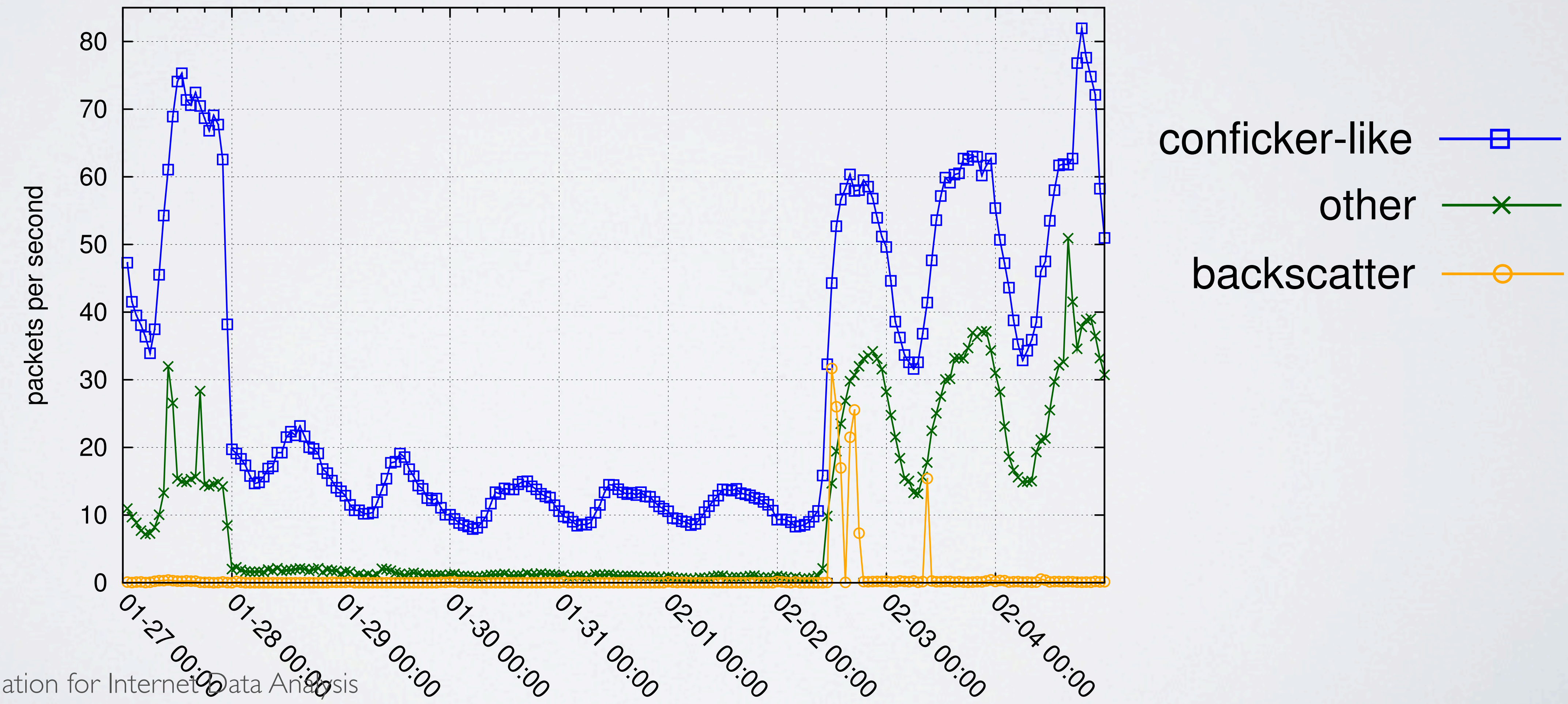
A,B,C: Outages
D1, D2: Denial of Service attacks

UCSD TELESCOPE

need to dissect traffic

- We classified traffic to the telescope in
  - ***Conficker-like***
  - ***Backscatter*** (e.g. SYN-ACKs to randomly spoofed SYNs of DoS attacks)
  - ***Other***

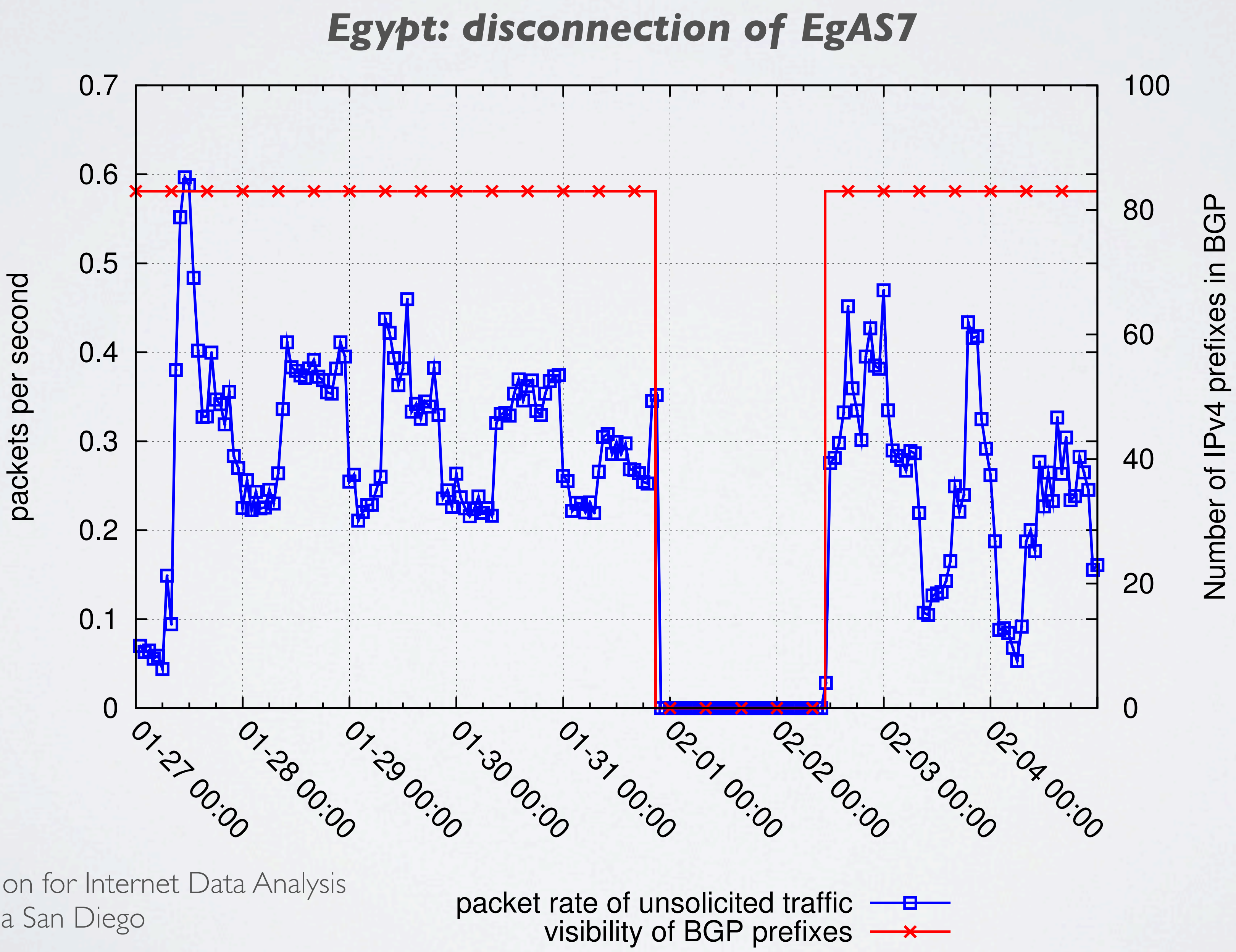
Egypt: telescope traffic



TELESCOPE VS BGP

Consistency

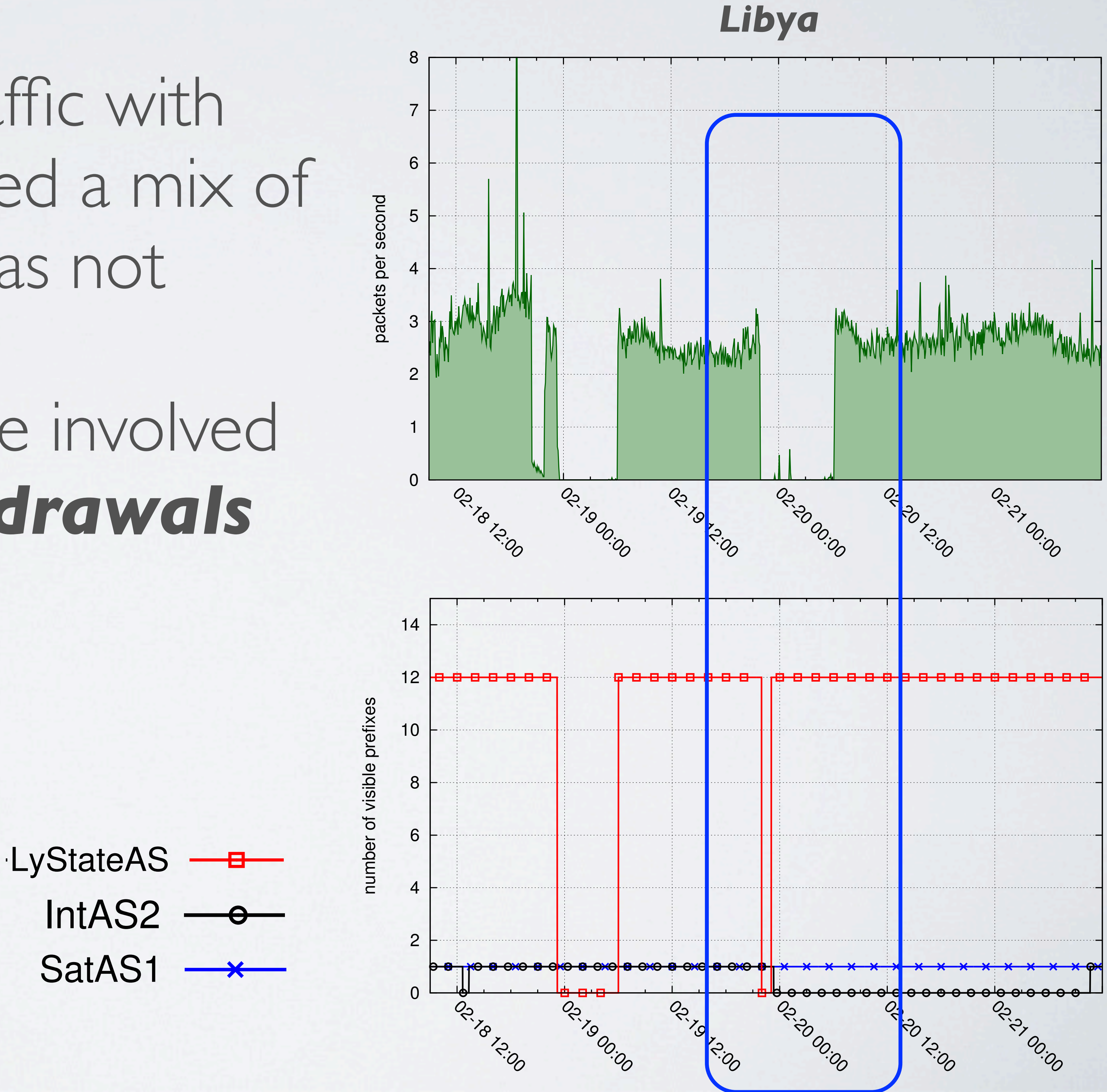
- The sample case of *EgAS7*shows the consistency between telescope traffic and BGP measurements



TELESCOPE vs BGP

Complementarity

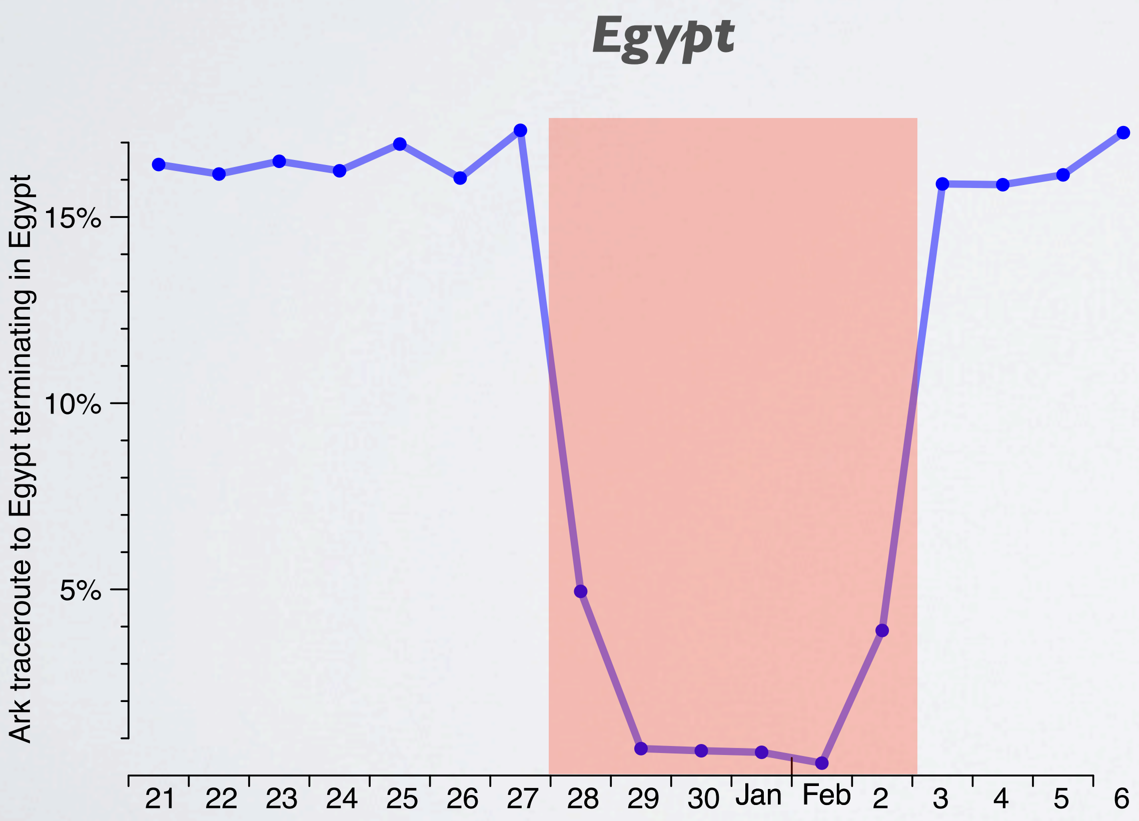
- Contrasting telescope traffic with BGP measurements revealed a mix of blocking techniques that was not publicized by others
- The second Libyan outage involved overlapping of ***BGP withdrawals*** and ***packet filtering***

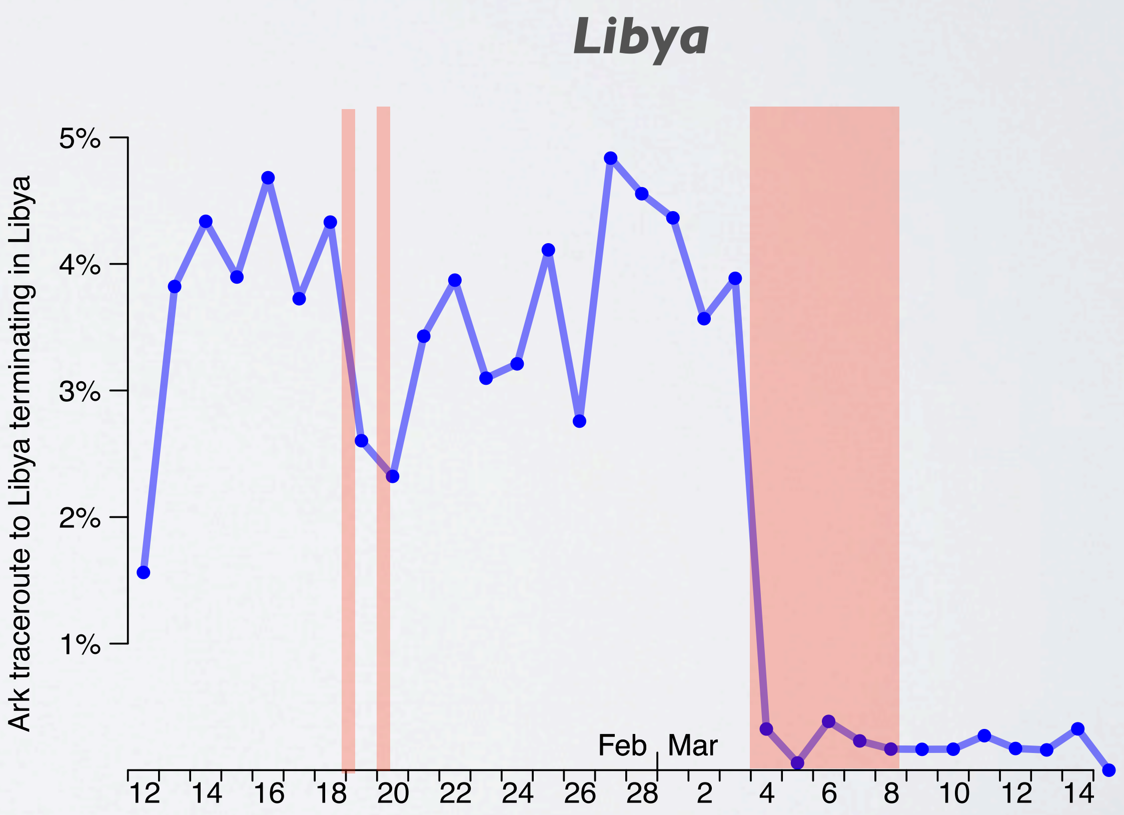


ARK

active measurements

- ARK active measurements are consistent with other sources
  - limitation due to frequency of probes and because they target random addresses
  - the first two Libyan outages are not visible
  - we used them only to test *reachability*, not to analyze topology





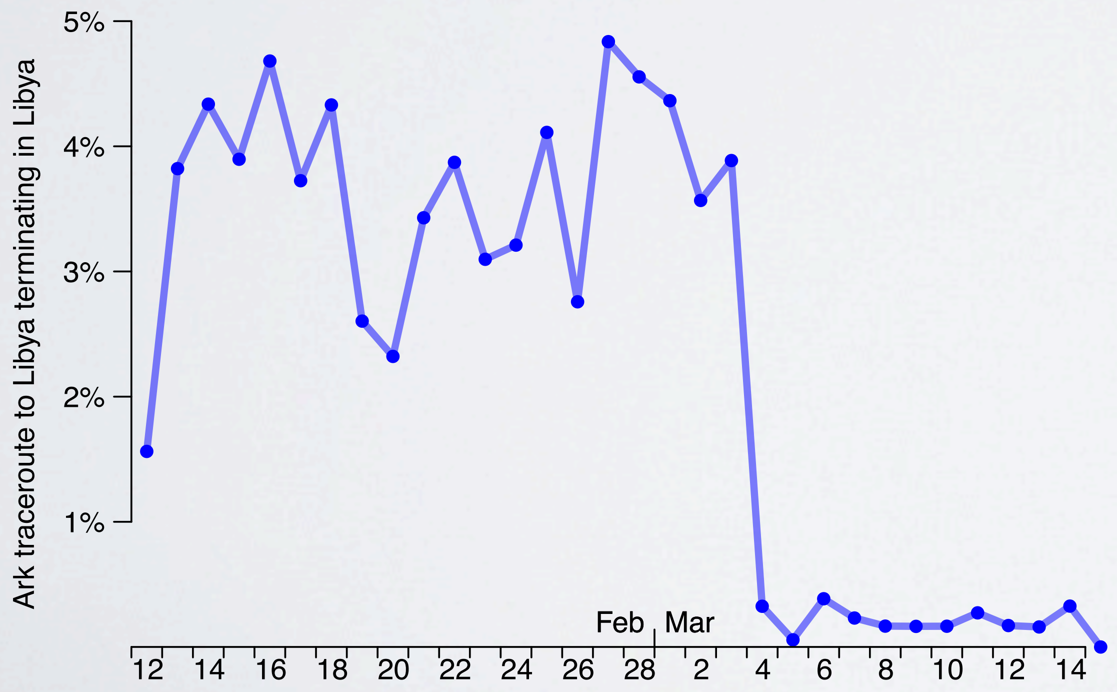
ARK

confirming telescope's findings

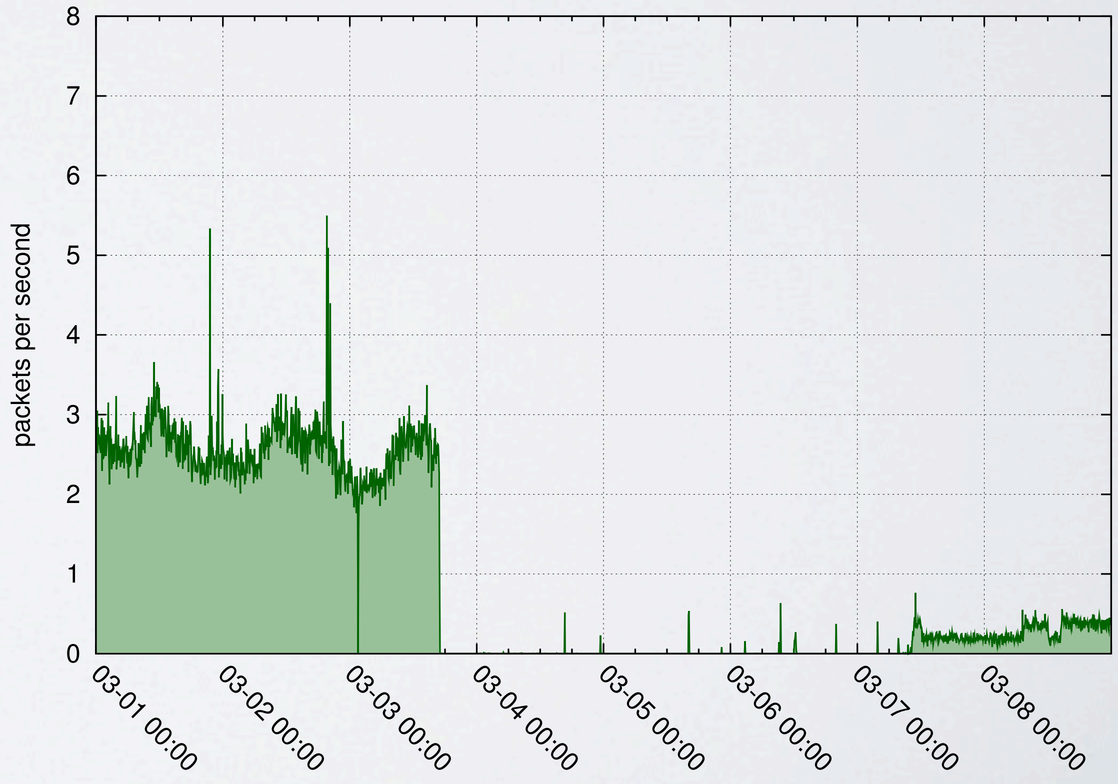
- Third Libyan outage: while BGP reachability was up, most of Libya was disconnected
  - ARK measurements confirmed the finding from the telescope
    1) disconnection
    2) identification of some reachable networks

  suggesting the use of packet filtering by the censors

Libya seen by ARK



Libya seen by the Telescope

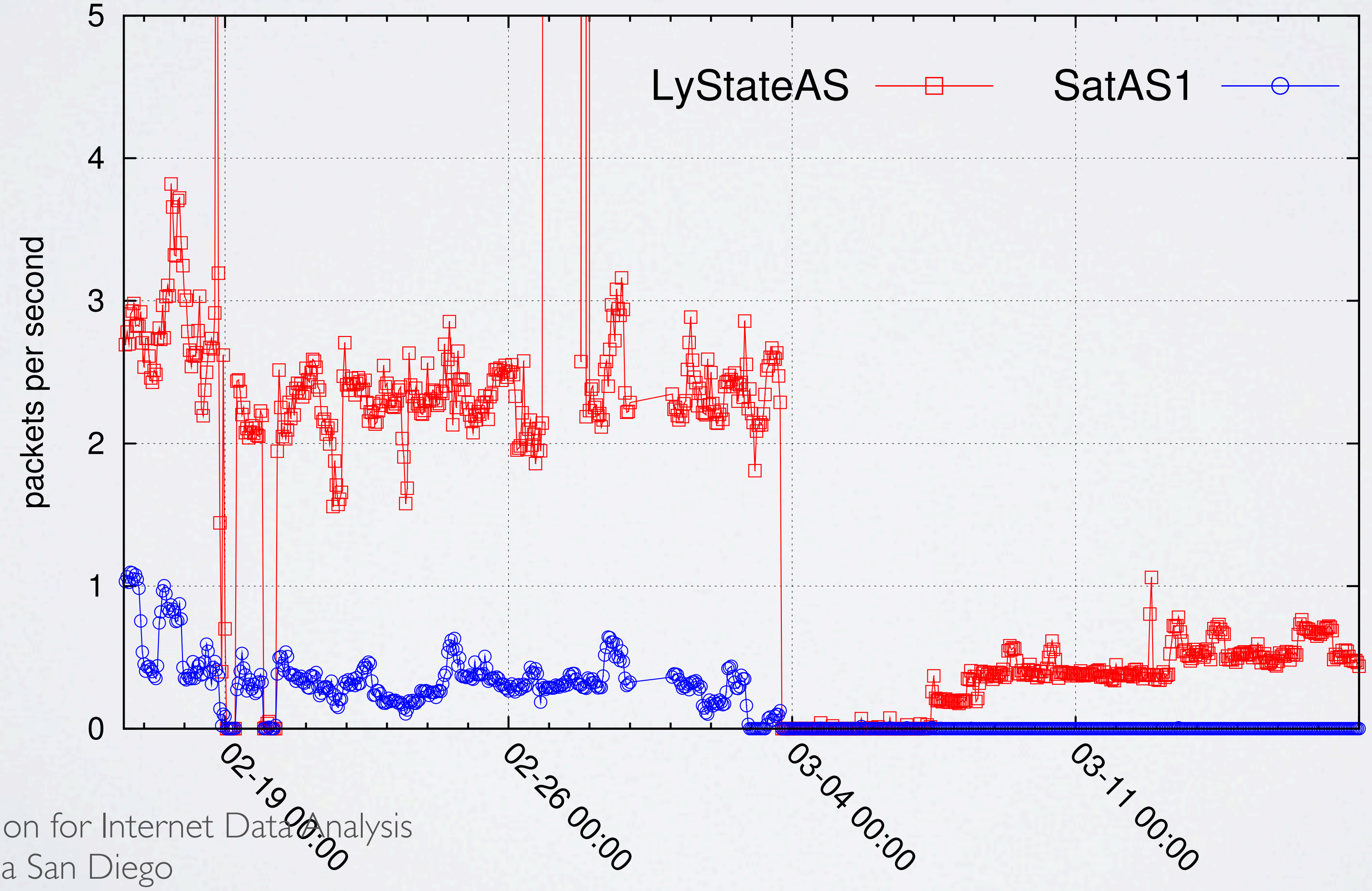


SATELLITE CONNECTIVITY

probable signal jamming

- Third Libyan outage
  - A Libyan IPv4 prefix managed by SatAS1 was BGP-reachable
  - Only a small amount of traffic from that prefix reaches the telescope during the outage

Libya: Telescope traffic from national operator and satellite-based ISP



CONCLUSION

& work in progress

- Contributions
  - a detailed **analysis of macroscopical political events** combining different measurement sources allowing to reveal insights not available from any individual data source
  - **1st-time use of IBR for this kind of analysis** - *extracting benefit from harm*!
  - Interesting findings
    - **IPv6 was neglected** by censors
    - Detected **packet filtering** and identified networks unfiltered by the regime
    - Identified **Denial of Service attacks**
    - Detected probable use of **signal jamming on satellite**-based connectivity

- Current work
  - Automated detection + triggered active measurements
  - Analysis of other types of network outages (e.g. caused by natural disasters)
  - Analysis of AS-level topology

THANKS