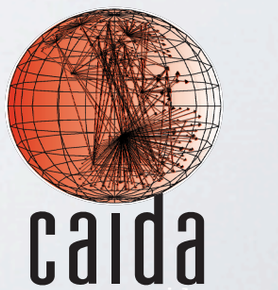
CAIDA Workshop on BGP and Traceroute data
August 22nd, 2011 - San Diego (CA), USA

Analysis of Country-wide Internet Outages Caused by Censorship

Alberto Dainotti - *alberto@unina.it*
University of Napoli "Federico II"

These slides are based on the following paper to be presented at ACM IMC 2011:
A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, A. Pescapé,
"Analysis of Country-wide Internet Outages Caused by Censorship"



THE EVENTS

Internet Disruptions in North Africa

- Egypt
  - Protests in the country start around January 25th, 2011
  - The government orders service providers to "shutdown" the Internet
  - On **January 27th, around 22:34 GMT**, 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
  - Protests in the country start around 17th February 2011
  - The government controls most of the country's communication infrastructure
  - Three different connectivity disruptions: **February 18th (6.8 hrs), 19th (8.3 hrs), March 3rd (3.7 days)**

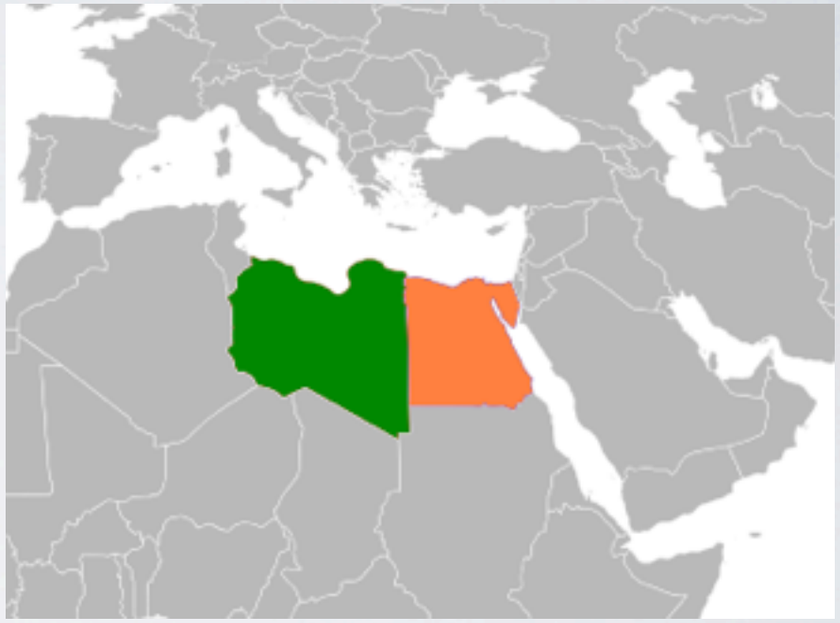
- *Similar events in other countries but we did not analyze them*

SOME FACTS

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
- 2 (+ 1) Autonomous Systems operate in the country
- Filtering type: mix of BGP, packet filtering, satellite signal jamming
- Filtering dynamic: testing different techniques; somehow synchronized

COMICS Research Group
University of Napoli "Federico II" - Italy

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 it..

- Internet Background Radiation (IBR)
  - Traffic reaching the ***UCSD network telescope***
  - Capable of revealing different kinds of blocking

COMICS Research Group
University of Napoli "Federico II" - Italy

THE DATA

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

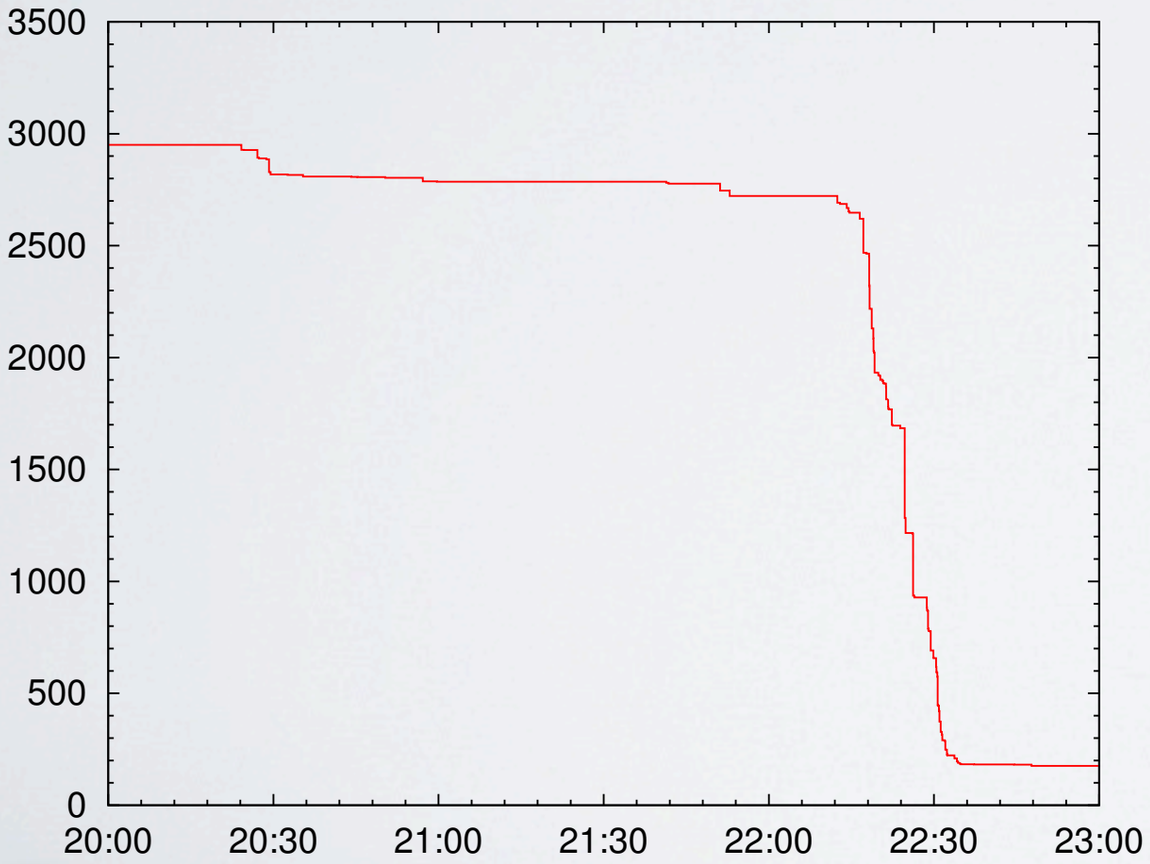
- Gather prefixes to be monitored. For each IP range:
  - We look up the address space in the BGP database of announced prefixes, to find an exactly matching BGP prefix
  - We find all the more specific (strict subset, longer) prefixes of this prefix
  - If the two previous steps yielded no prefix, we retrieve the longest BGP prefix entirely containing the address space
- Every time we refer to an AS we actually refer to the IPs of that AS that are associated to the country of interest

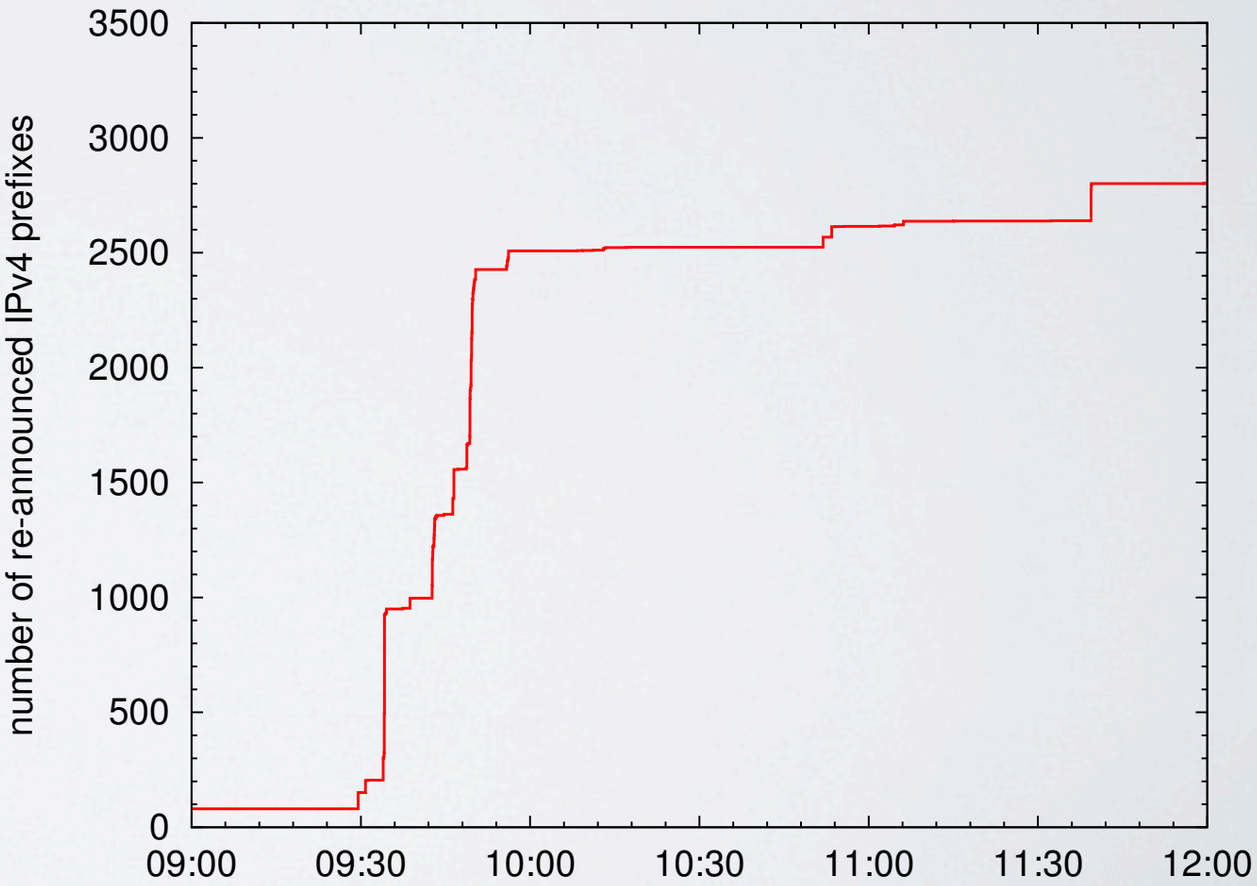
BGP

prefix reachability

- We reconstruct prefixes losing and regaining reachability
  - we build the routing history of a 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!]



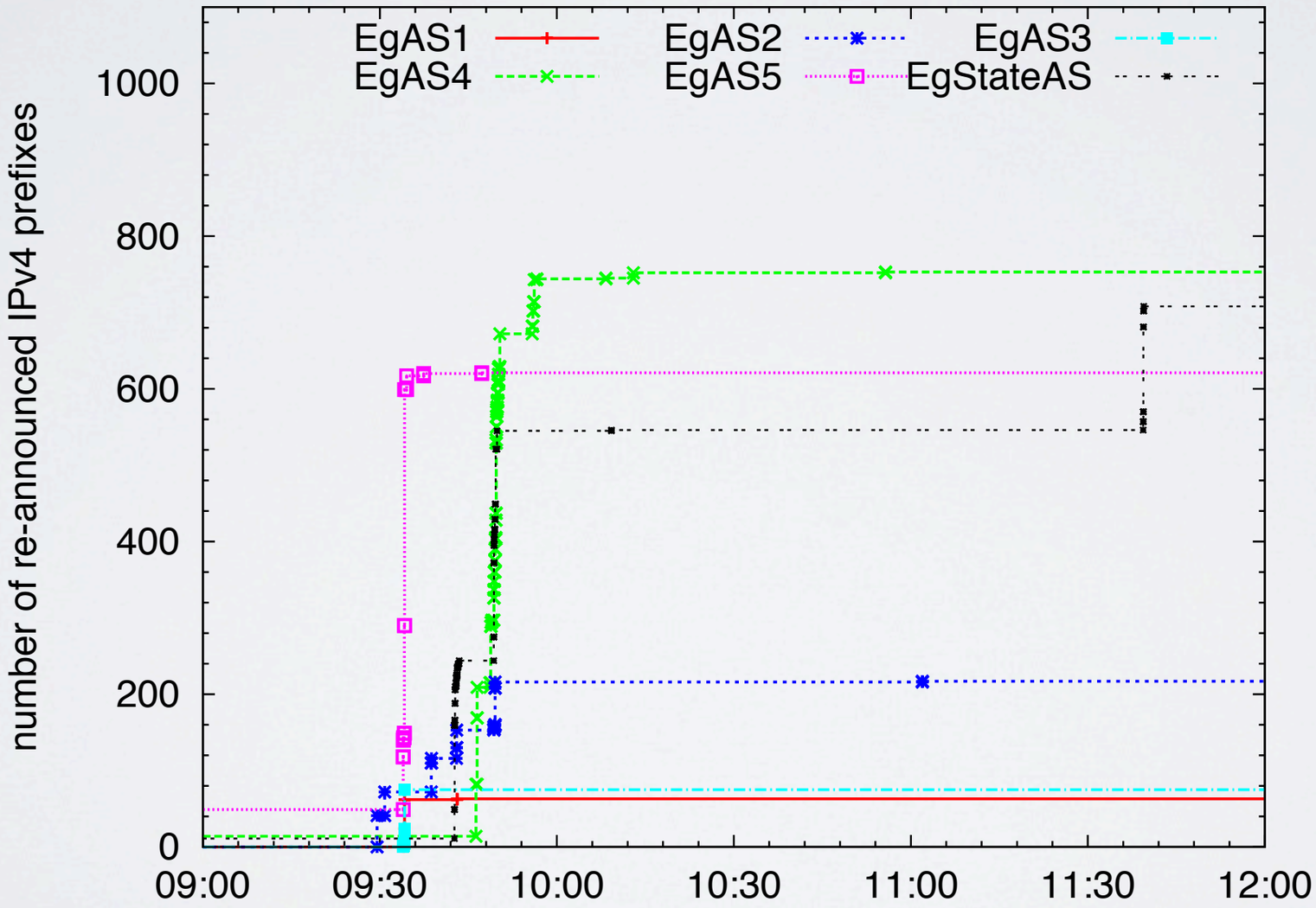


COMICS Research Group
University of Napoli "Federico II" - Italy

BGP

per-AS analysis

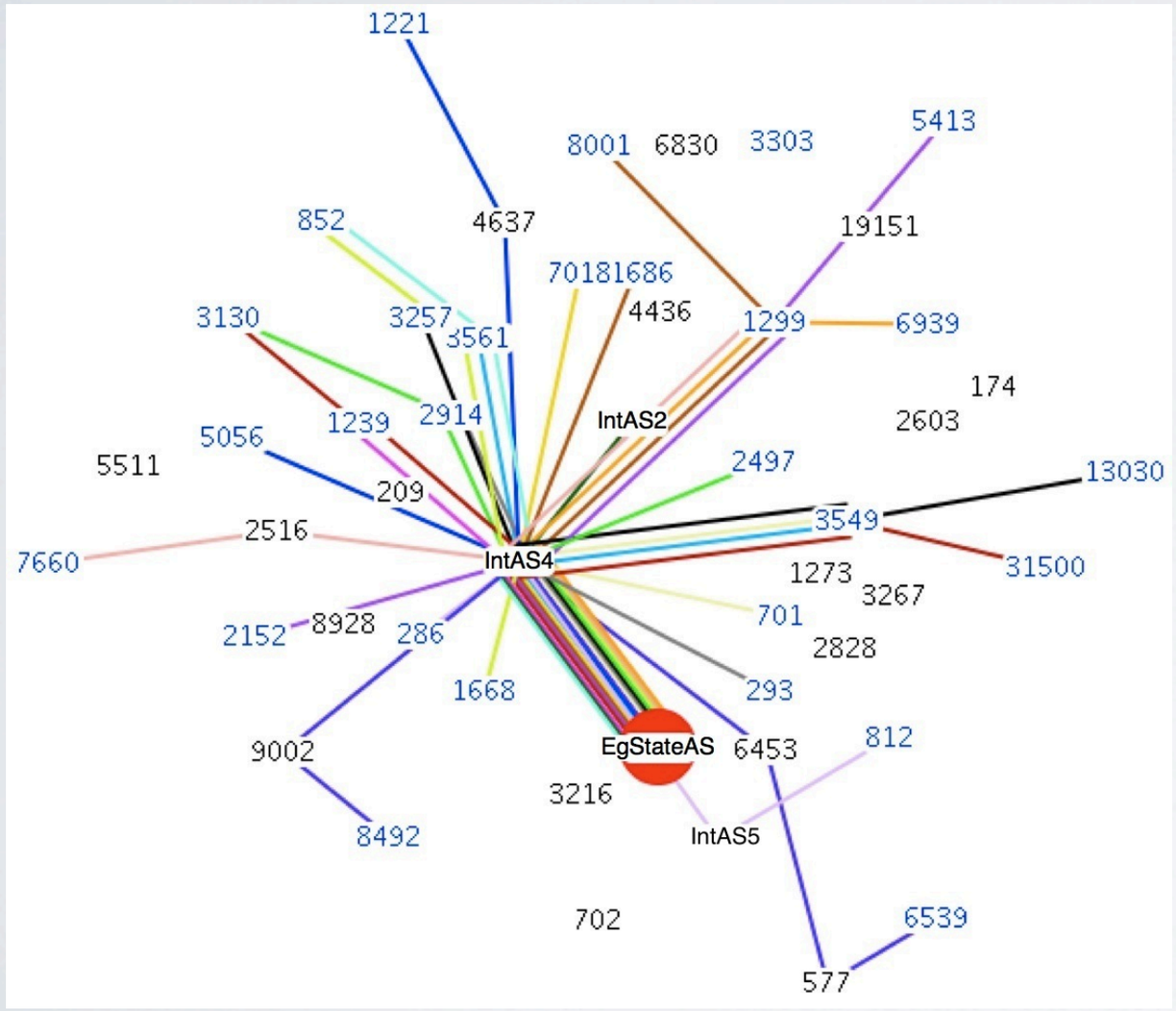
- A detailed analysis shows there is synchronization among ASes

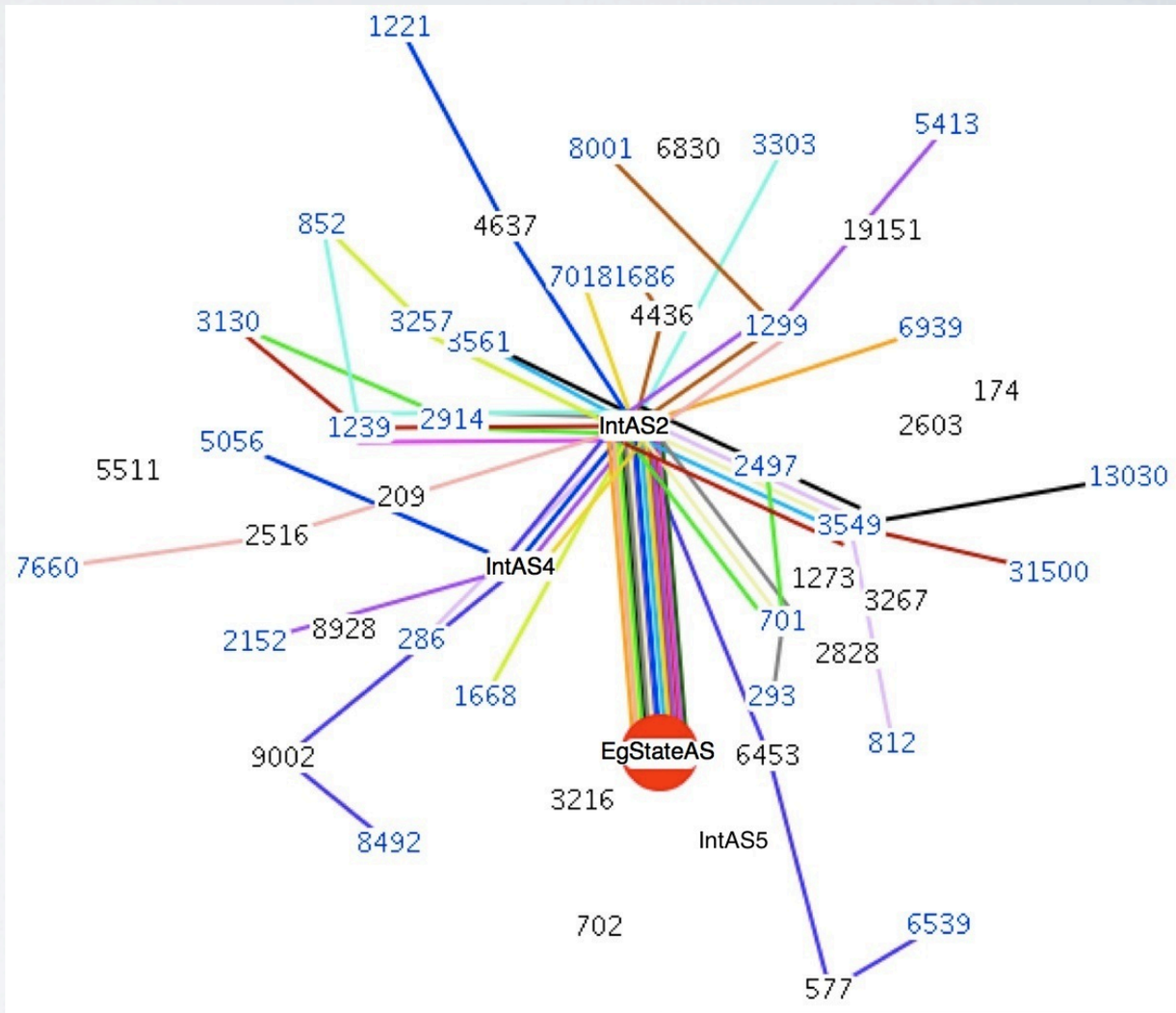


ROUTE CHANGES

BGPlay

- The massive disconnection caused some path changes too



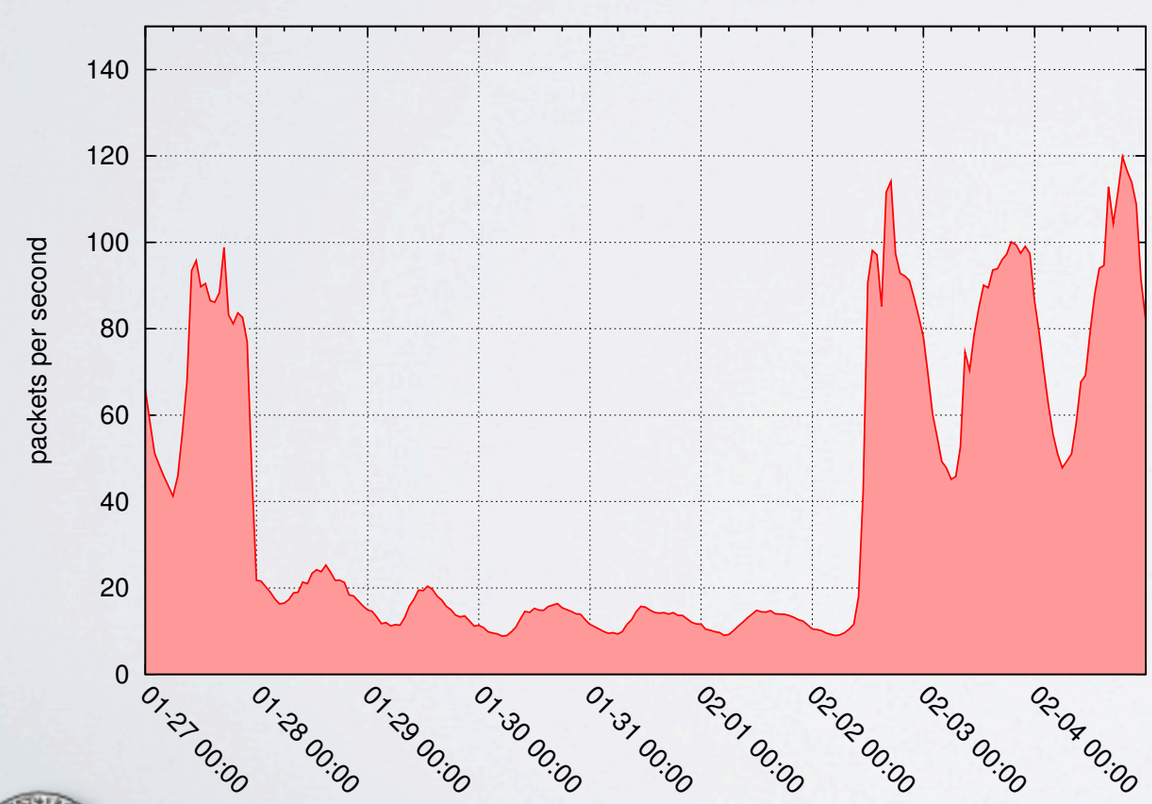


UCSD TELESCOPE

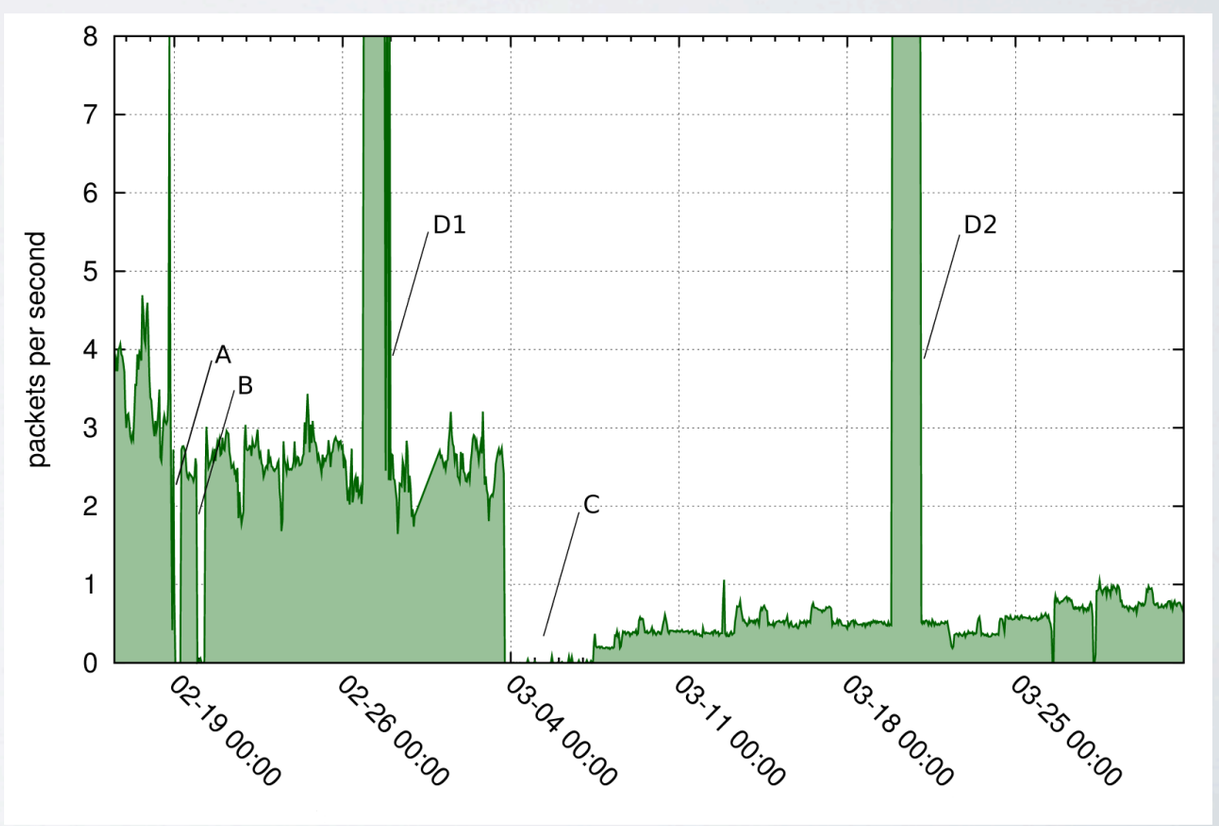
when malware helps..

- Unsolicited traffic - *e.g. scanning from conficker-infected hosts* - from the observed country and reaching a (mostly) unused /8 network at UCSD

Egypt



Libya



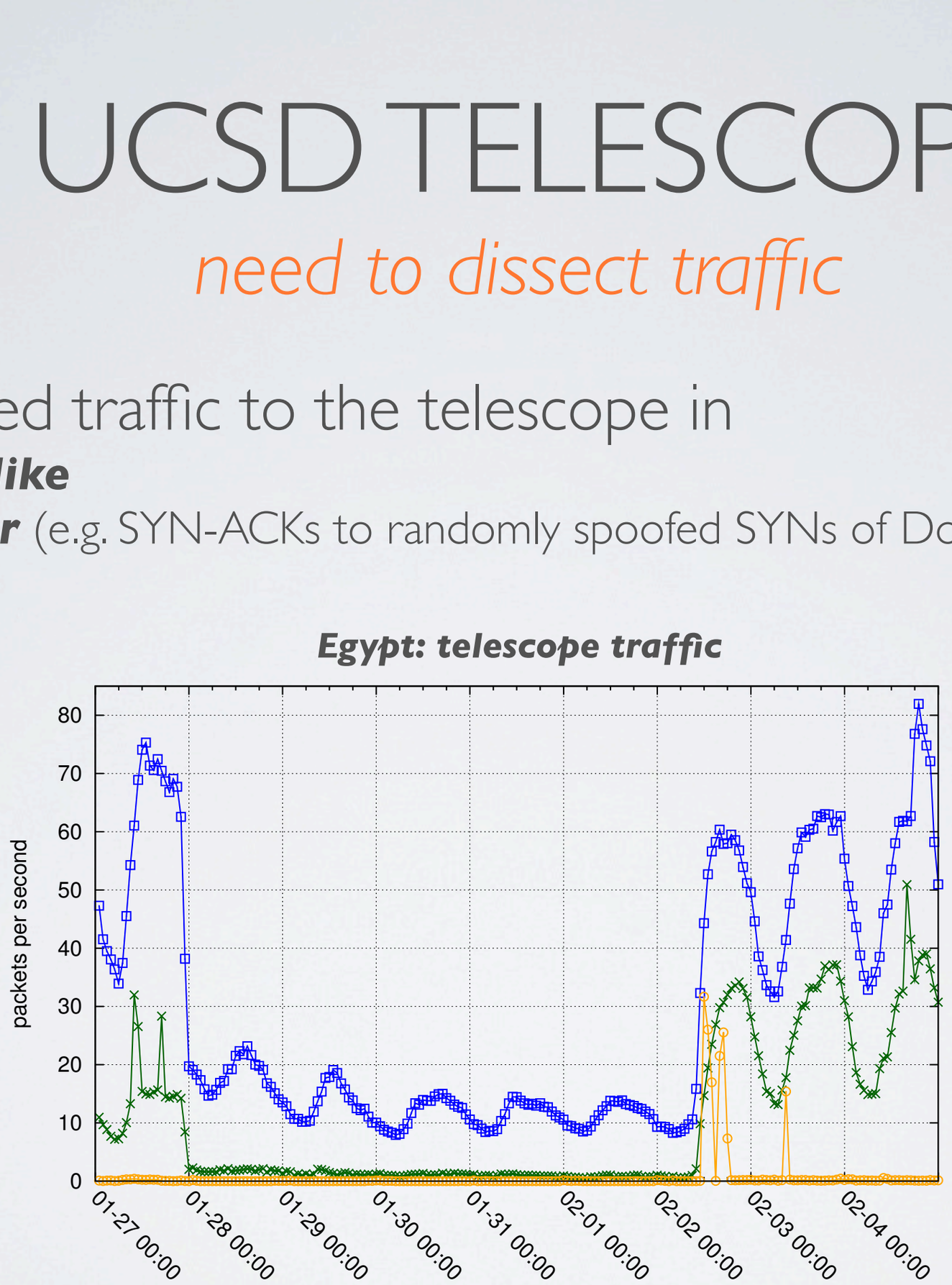
COMICS Research Group
University of Napoli "Federico II" - Italy

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***

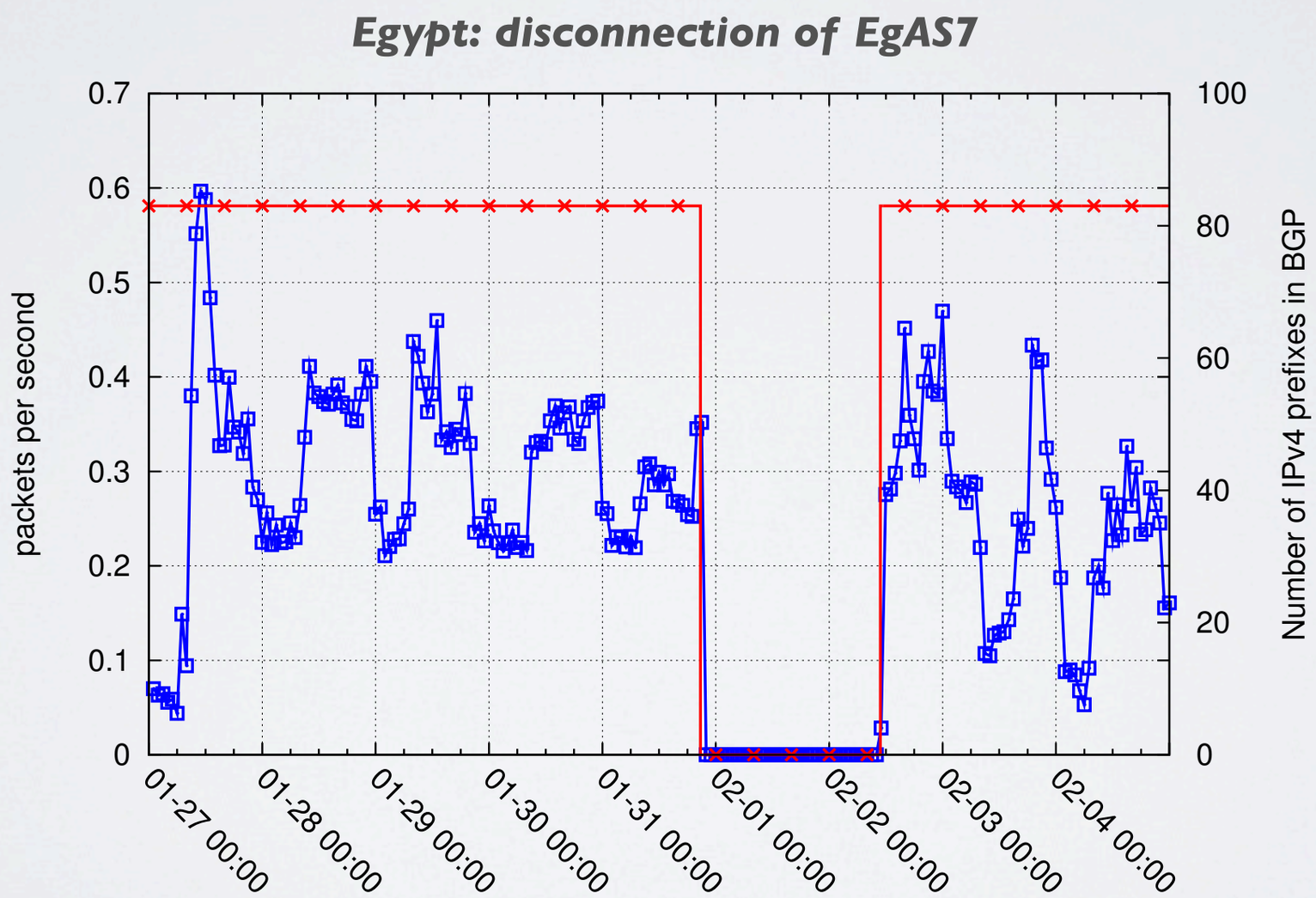
Egypt: telescope traffic



TELESCOPE *vs* BGP

Co*nsistency*

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



COMICS Research Group
University of Napoli "Federico II" - Italy

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***

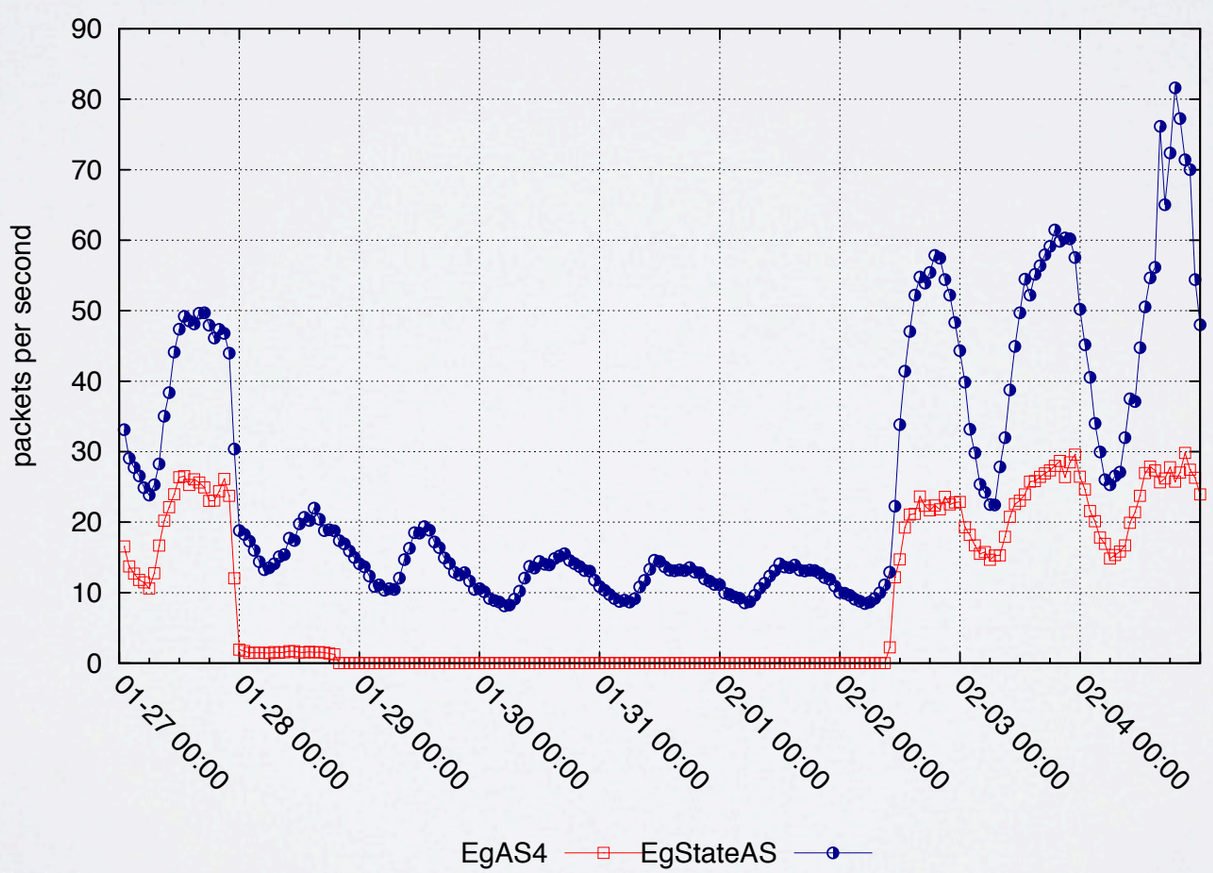
COMICS Research Group
University of Napoli "Federico II" - Italy

TELESCOPE *vs* BGP

Confusion?

- BGP-unreachability doesn't, in general, prevent outbound traffic
  - We found networks that were BGP-unreachable sending traffic to the telescope
  - and networks BGP-reachable that were not
  - Topology analysis may help to better understand this behavior

Telescope traffic from two Egyptian ASes

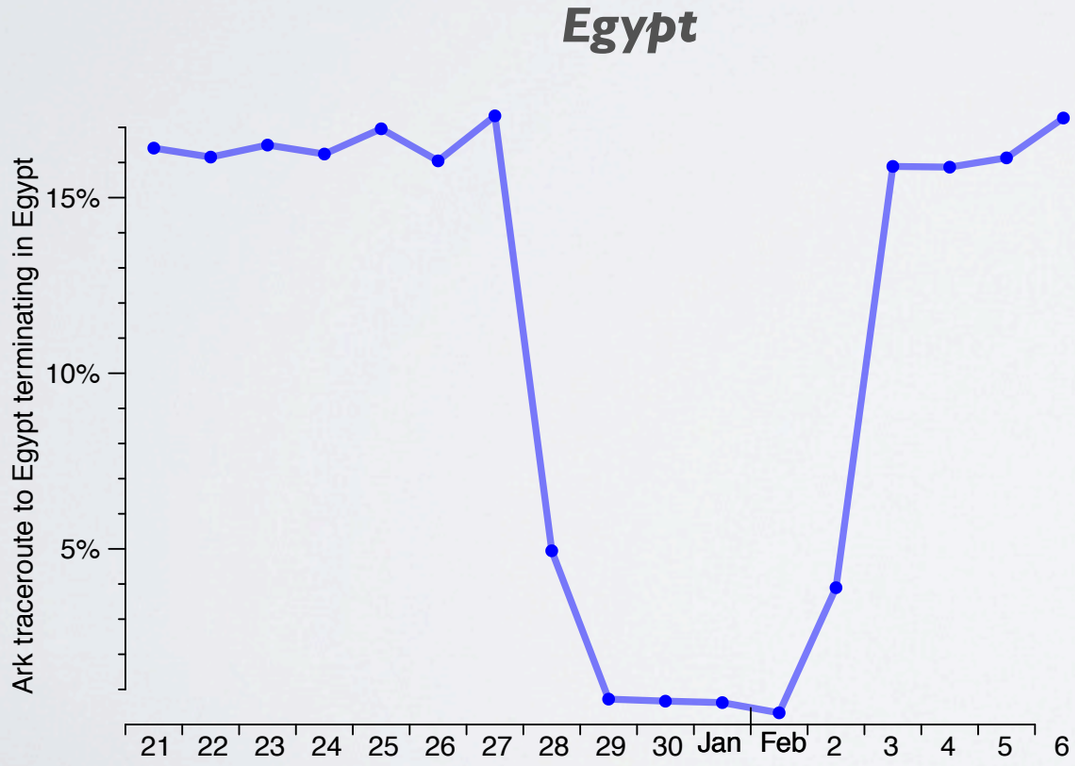


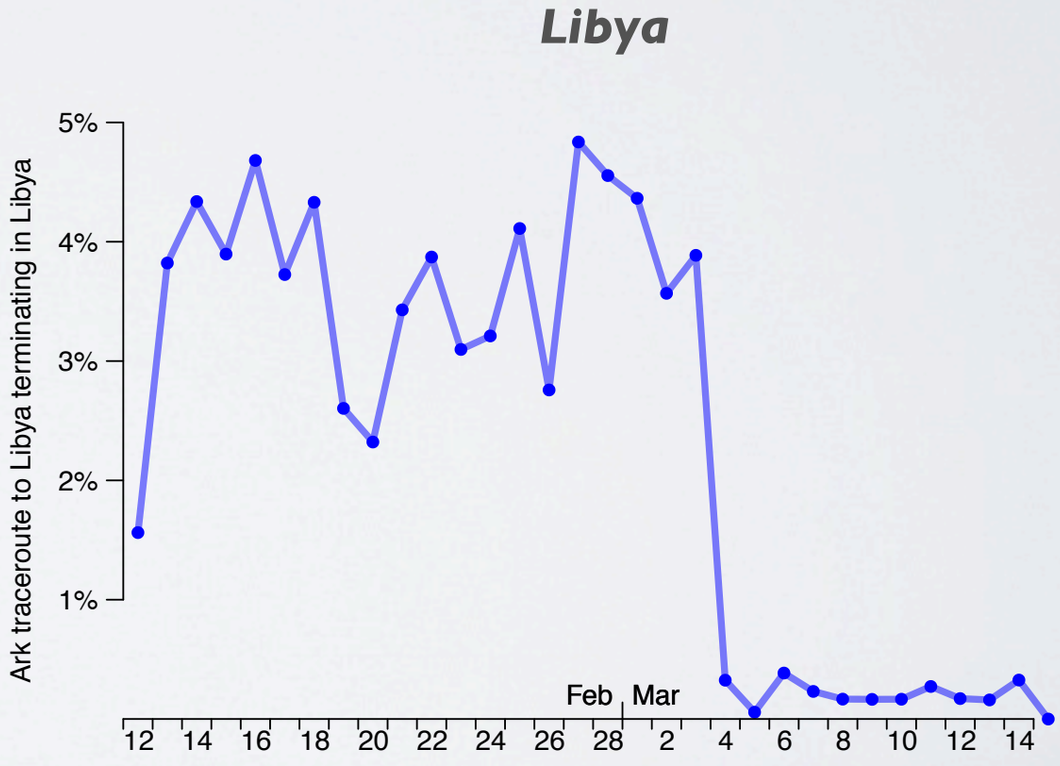
COMICS Research Group
University of Napoli "Federico II" - Italy

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





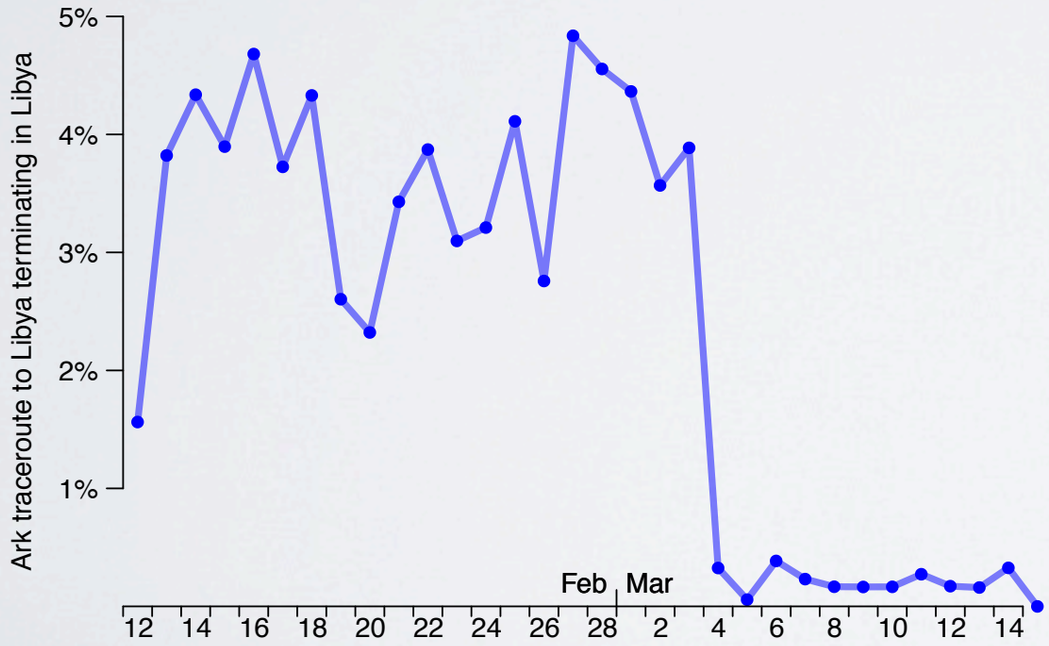
COMICS Research Group
University of Napoli "Federico II" - Italy

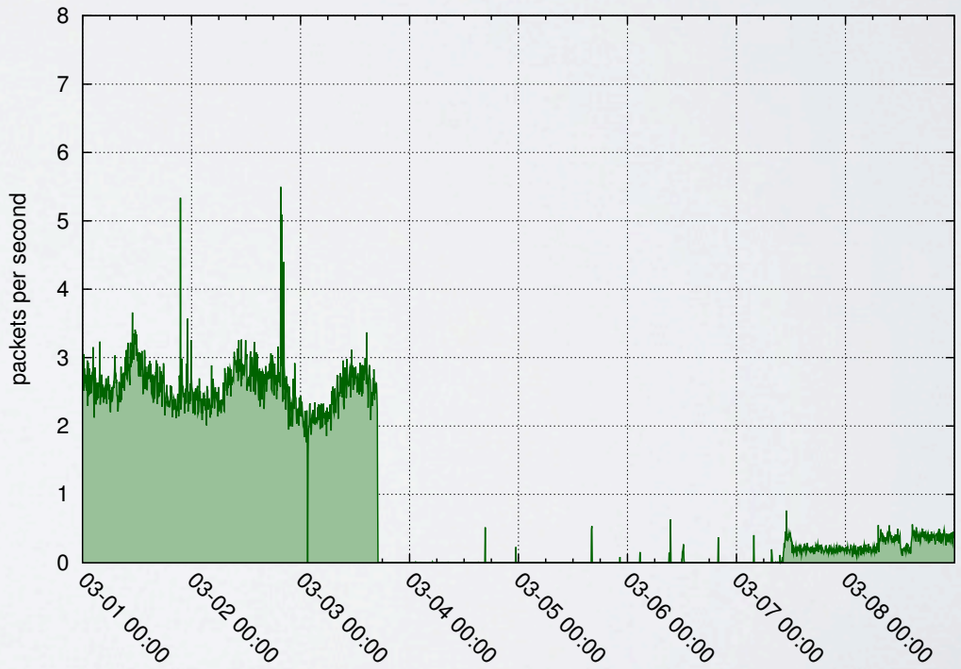
ARK

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, plus identified some reachable hosts, suggesting the use of packet filtering by the censors

Libya: ARK (left) , Telescope (right)





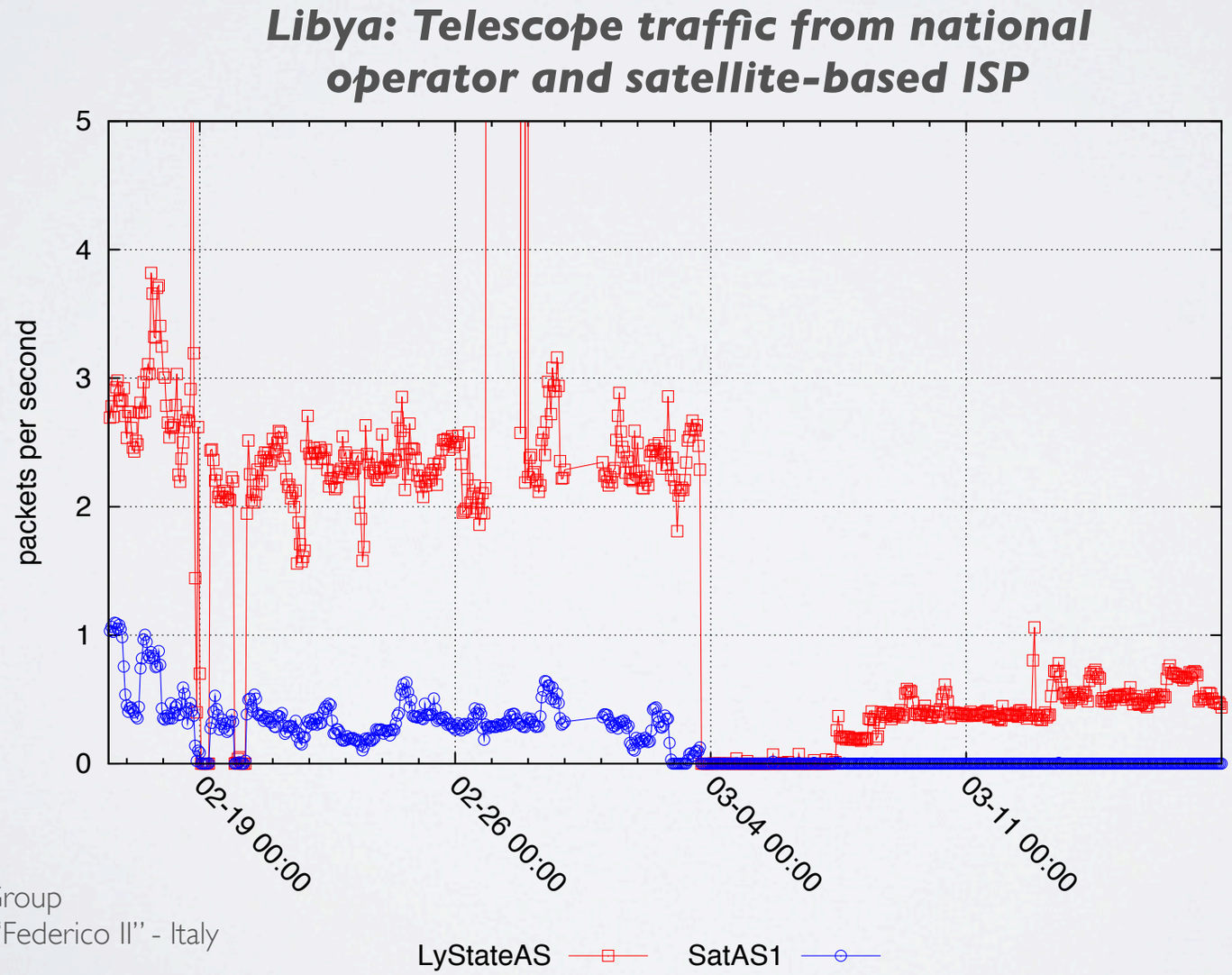
COMICS Research Group
University of Napoli "Federico II" - Italy

SATELLITE CONNECTIVITY

probable signal jamming

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

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



COMICS Research Group
University of Napoli "Federico II" - Italy

CONSIDERATIONS

- Telescopes can be used for studying macroscopic connectivity problems and they complement BGP-based measurements
  - BGP-unreachable networks sometimes still *send* unsolicited packets
- Ark measurements
  - Probing frequency + destination sampling = (too) small resolution
  - Better/more detailed measurements should be triggered by other measurements when interesting events occur
- Detection would need *both* telescope & BGP measurements
- IPv6 was neglected by the censors
- We depend on geolocation
- Time resolution of BGP measurements: can we improve it?
- We would like to look at AS-level topology
- We couldn't study, e.g., Syria cause of very selective filtering and low volume of unsolicited traffic

THANKS

COMICS Research Group
University of Napoli "Federico II" - Italy