SplinterCon

How to monitor Internet connectivity and track shutdowns with IODA

Georgia Tech

Agenda:

- Introduction to Using IODA
  - What is IODA?
  - IODA Signals
  - How to identify an Internet disruption
- Rapid Response Protocol
- Limitations of IODA
- Recent and Ongoing Research

Georgia Tech

What is IODA?

Internet Outage Detection and Analysis (IODA) is an open-source project at Georgia Tech that provides measurements of the connectivity of Internet infrastructure at the country, subnational and Internet operator level that is available via a public, online dashboard (*https://ioda.live*).

IODA should be used for instances involving complete Internet connectivity outages such as the shutdowns.

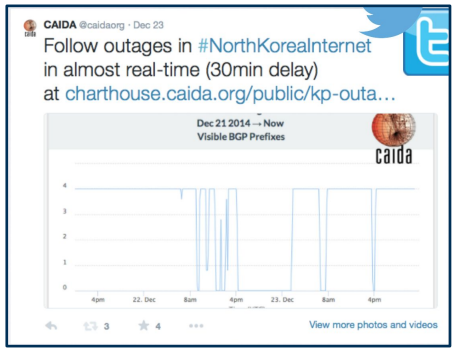
IODA

Georgia Tech

History of IODA

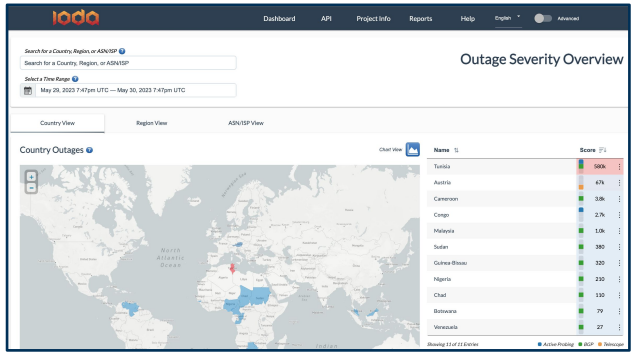
Arab Spring 2011

Experimental research at UC San Diego CAIDA on how to measure the Internet, using Arab Spring as a case study



Dashboard v1 2014

An open-source, publicly available dashboard that provides Internet infrastructure connectivity measurements in near real time



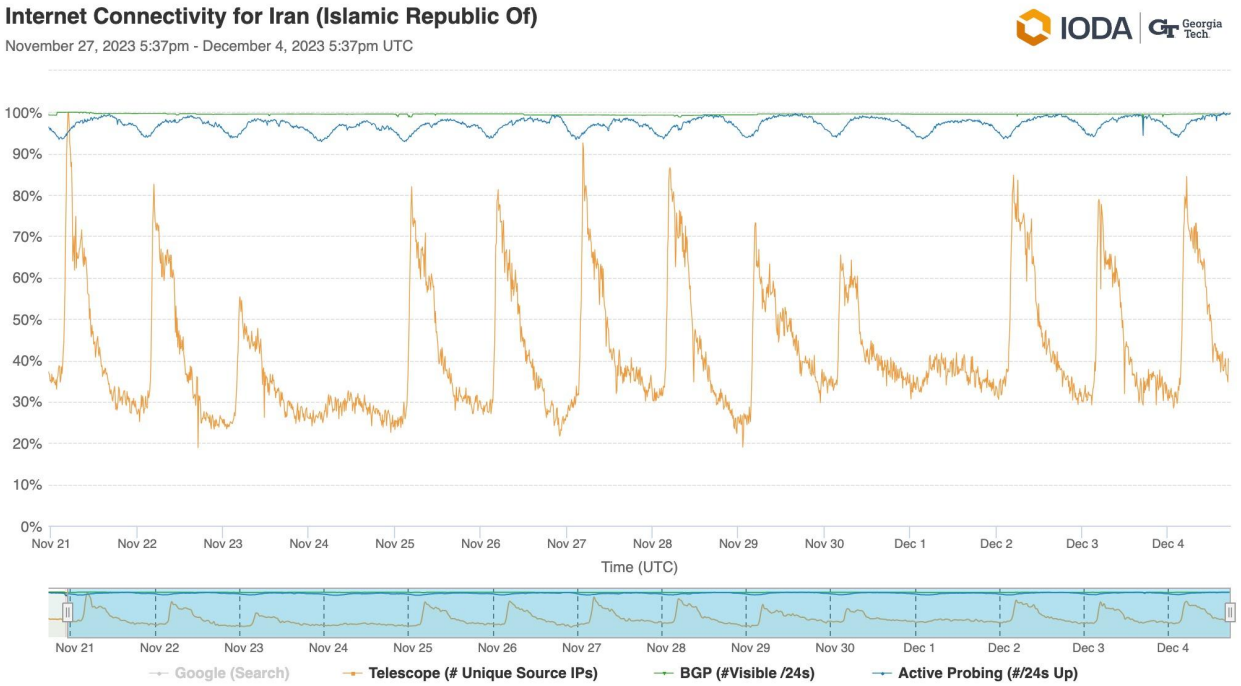
2022

Ongoing research to improve geographic granularity, measure throttling; user-centered design; community engagement

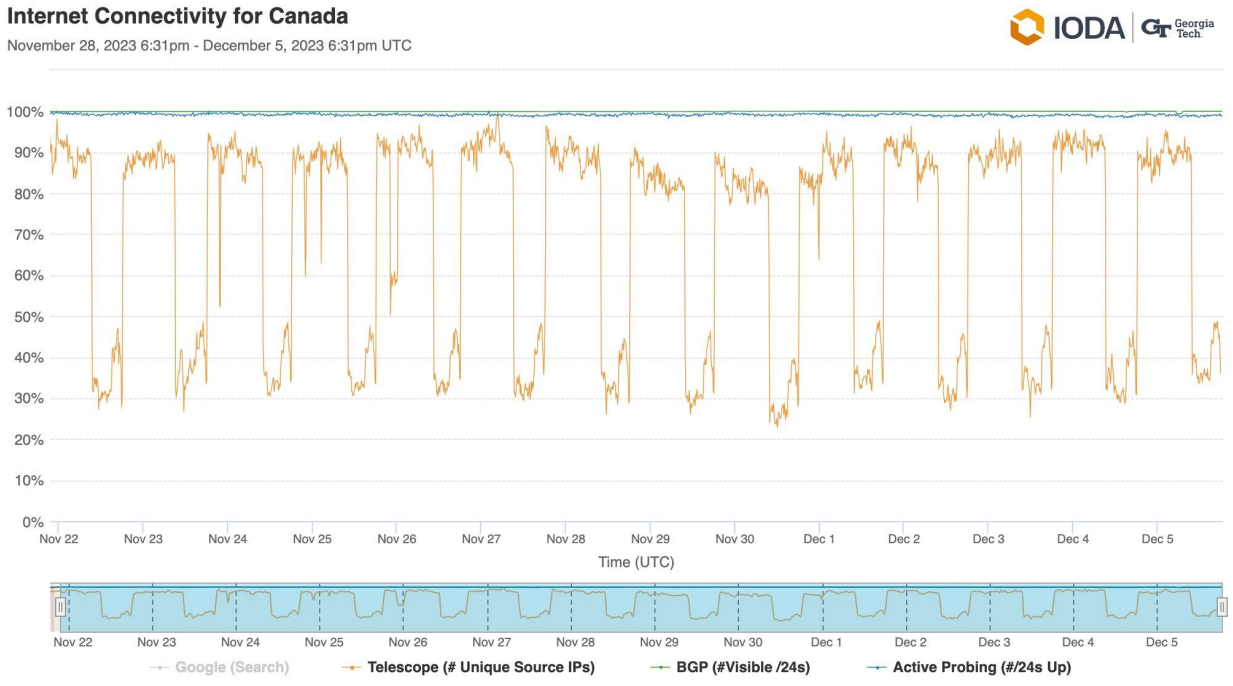
IODA

Georgia Tech

IODA's Measurements



IODA's Internet connectivity measurements for Iran

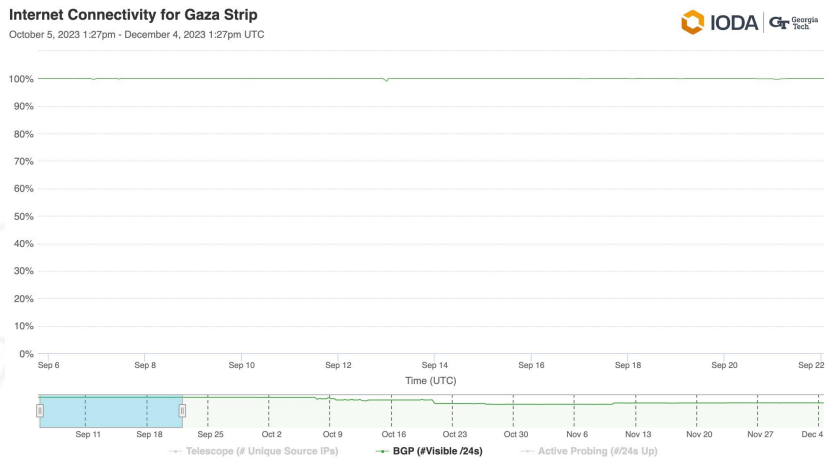


IODA's Internet connectivity measurements for Canada

IODA

Georgia Tech

IODA's measurements: Routing Announcements (BGP)



Normal BGP Signal Behavior

Disrupted/ Abnormal BGP Signal Behavior

Routers, which are network hardware that forward packets of data, use Border Gateway Protocol (BGP) to announce what networks they are responsible for routing data to.

The BGP protocol provides a global routing method that guides the flow of Internet traffic through various networks over the Internet.

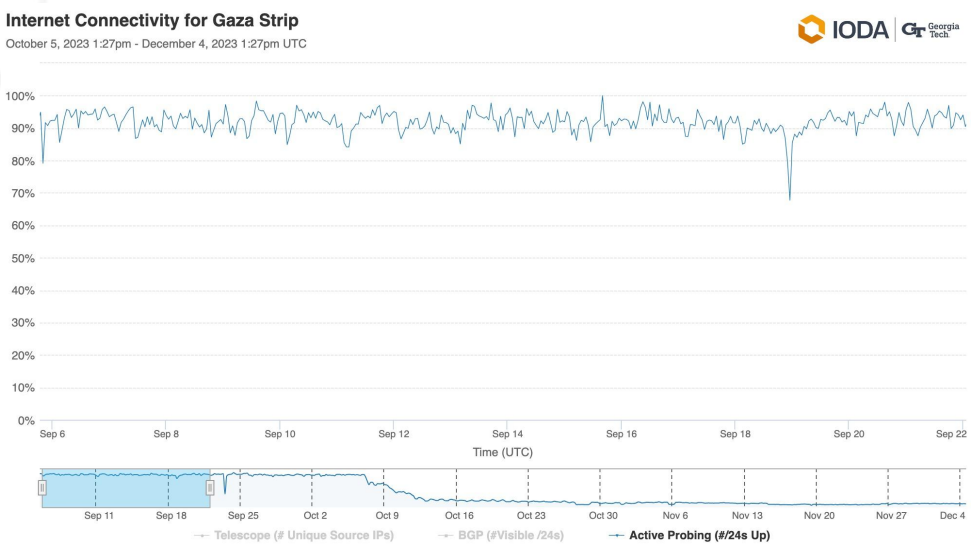
Every 5 minutes, IODA collects updated Internet routing information. These Routing Announcements form IODA's BGP signal.

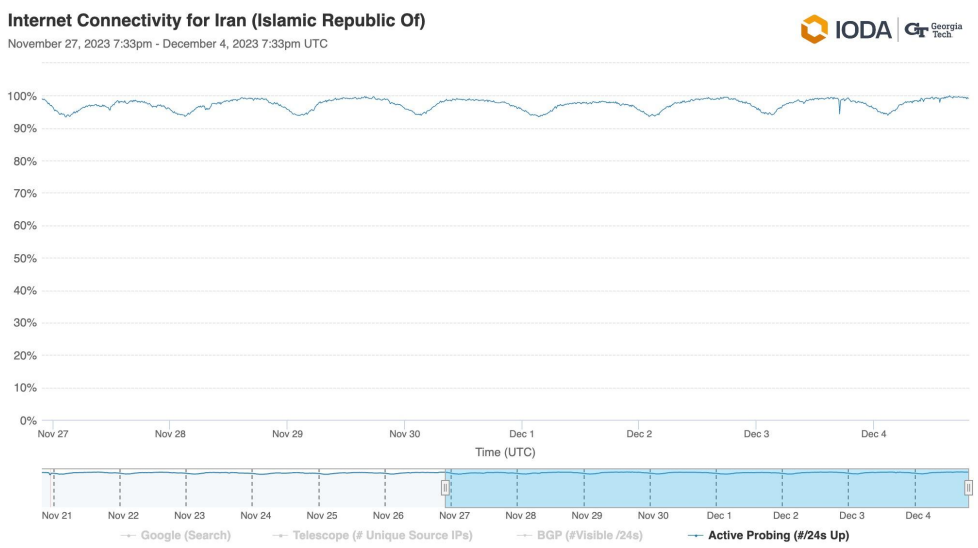
IODA

Georgia Tech

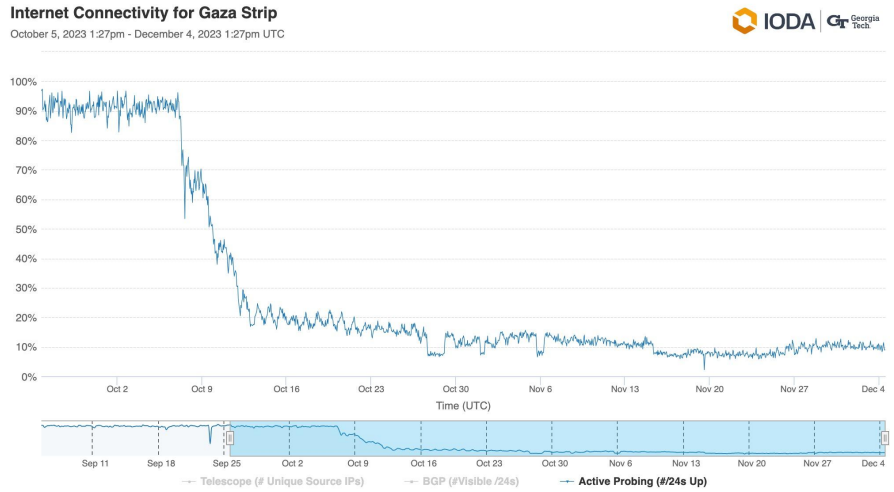
IODA's measurements: Active Probing

Normal AP Signal Behavior





Disrupted/ Abnormal AP Signal Behavior



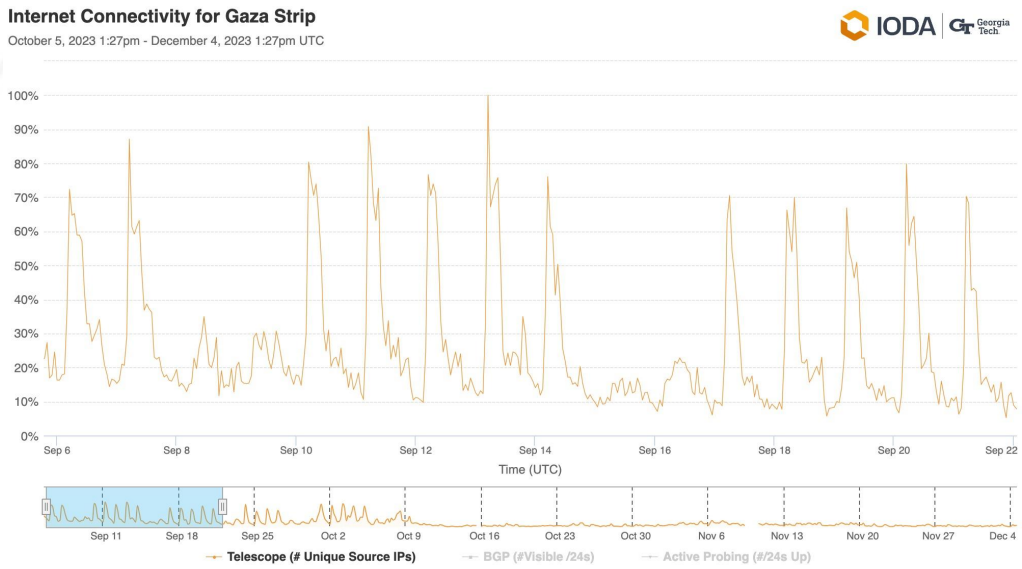
To create the Active Probing signal, IODA continuously pings networks known to be at a certain geographic location. Most networks are designed to automatically respond to pings by echoing them back to the sender.

If networks stop responding to pings, the active probing signal will drop and this may indicate a disruption in connectivity.

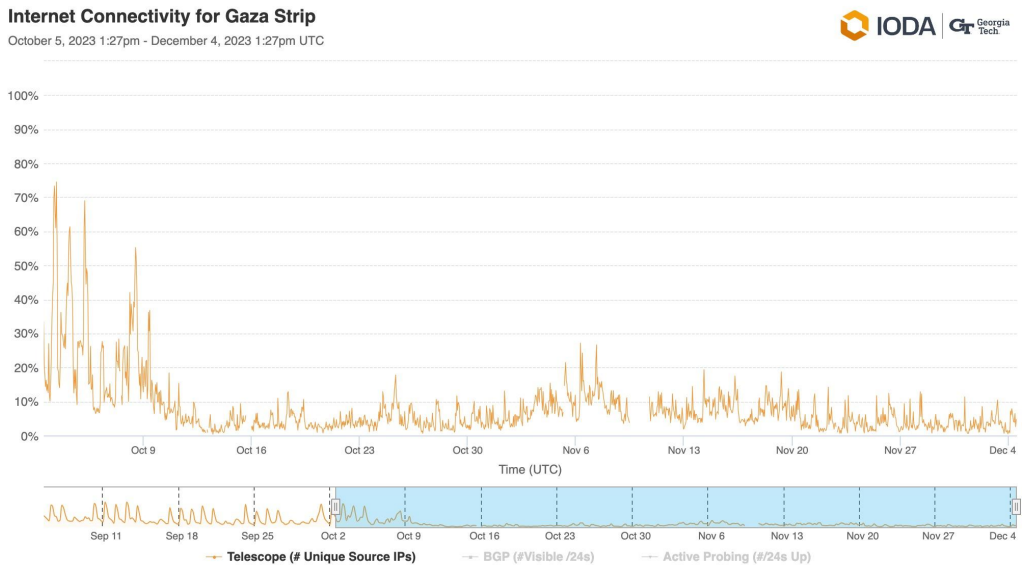
Georgia Tech

IODA's measurements: Telescope

Normal Telescope Signal Behavior



Disrupted/ Abnormal Telescope Signal Behavior



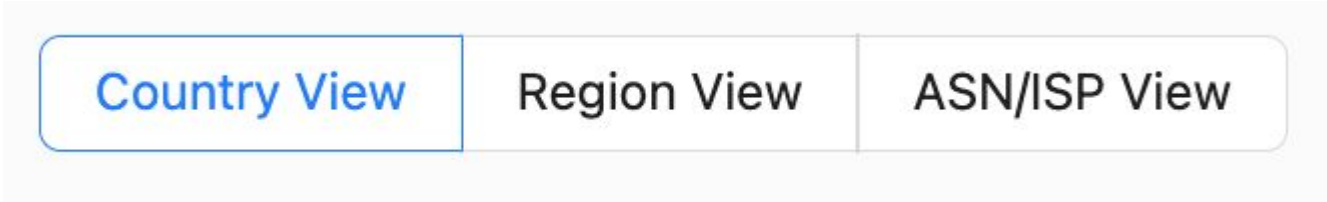
IODA collects and processes Telescope traffic data, which is unsolicited network traffic captured through dedicated research infrastructure called a telescope.

This traffic is a sort of Internet pollution, a continuously evolving mix, created by a variety of sources including misconfiguration, network scanning, malware, misconfigured peer to peer file sharing, infected computers and by other unexpected phenomena.

If the corresponding telescope signal suddenly drops below what is normally observed may indicate an outage.

Georgia Tech

IODA Levels of Measurement: Country, Region, ISP



Country
- signals available: BGP, Active Probing, Telescope, Google Products

Region
- signals available: BGP, Active Probing, Telescope

Internet Service Provider/ Autonomous System
- signals available: BGP, Active Probing, Telescope

IODA

Georgia Tech

IODA Alerts, Events, Overall Outage Scores

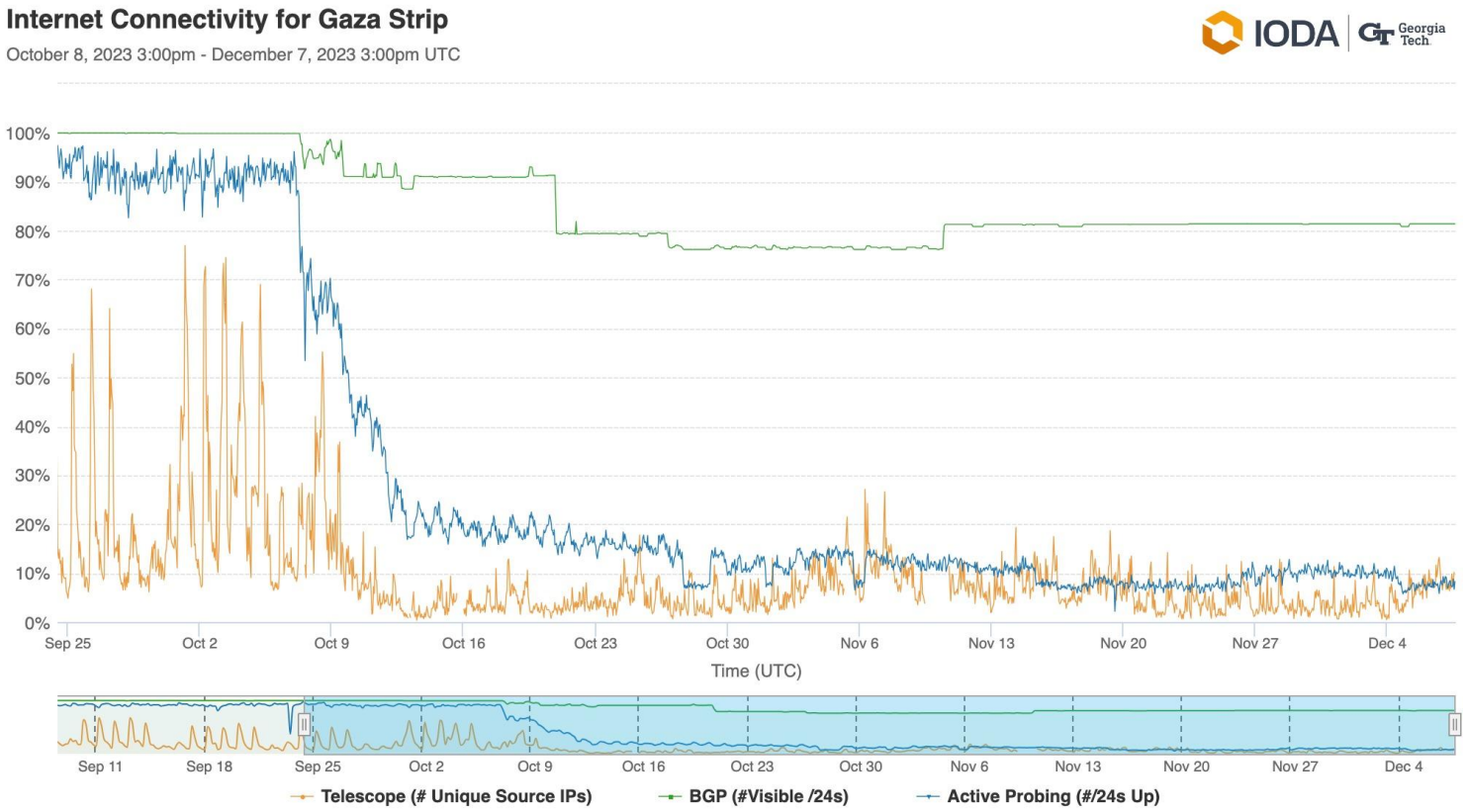
Outage Detection	Definition	Data
Alerts	IODA detects that a signal demonstrates an abnormal drop or recovery	Time, signal, actual value, base value
Events	IODA summarizes alerts into an outage event with a severity score	start. end, duration, score
Overall Outage Scores	Events are summarized at the country, region, or AS/ISP level and visualized on a map or time series.	overall outage score, signals associated with the outage, signal level outage score

Let’s take a look

IODA

Georgia Tech

How to identify an outage in IODA

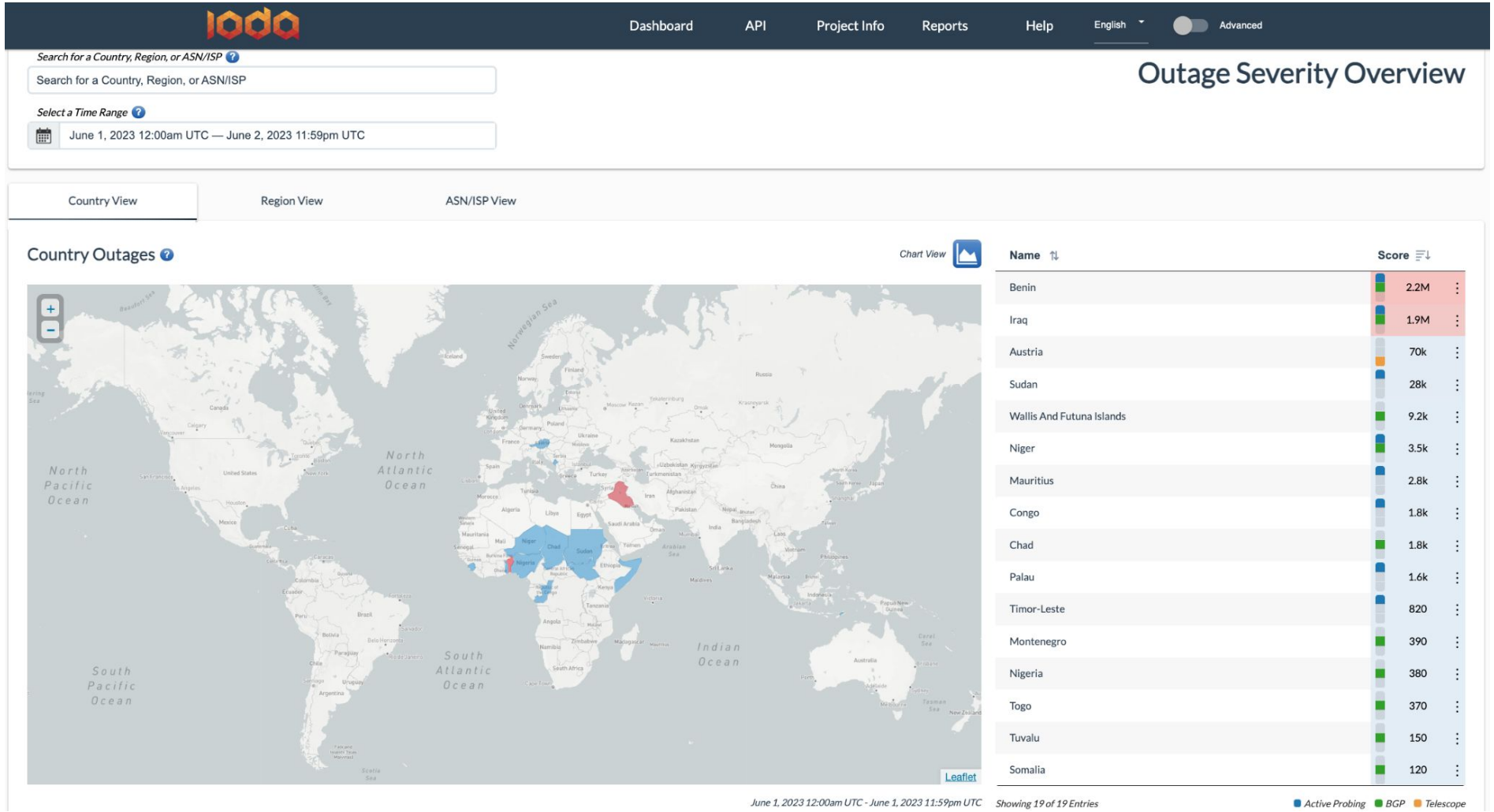


- Outages are **abnormal**, **simultaneous** drops in **2 or more** signals
  - 2 or more IODA signals
  - 1 IODA signal and 1 external source confirming an outage (e.g. Cloudflare, on the ground reporting)

IODA

Georgia Tech

Demo: How to identify an outage in IODA



IODA

Georgia Tech

An Internet Shutdown Rapid Response Protocol

Preliminary Shutdown Evidence

- An alert is triggered on a measurement dashboard that shows a disruption (e.g., IODA or Cloudflare)
- A partner organization identifies a censorship event (e.g., Access Now, Miaan Group)
- A censorship event is expected due to an upcoming political event: mobilization, election, coup, etc.

Verification and Confirmation

- Measurement team investigates their data for scope of outage (duration, geography, ISPs)
- If measurement data demonstrates disruption, data is shared with partner organizations for validation (Measurement groups and CSOs) via Signal, Slack, Email
- Gather socio-political and measurement details for confirmed disruption details

Circulation of Confirmed Information

- Share with Internet Freedom Community and broader public via social media, secure messaging, Slack, KIO listserv

Circumvention Analysis

- Determine which ASes are affected, and which are not by disruption/ censorship
- Repeat analysis as necessary based on evolving censorship practices

IODA

Georgia Tech

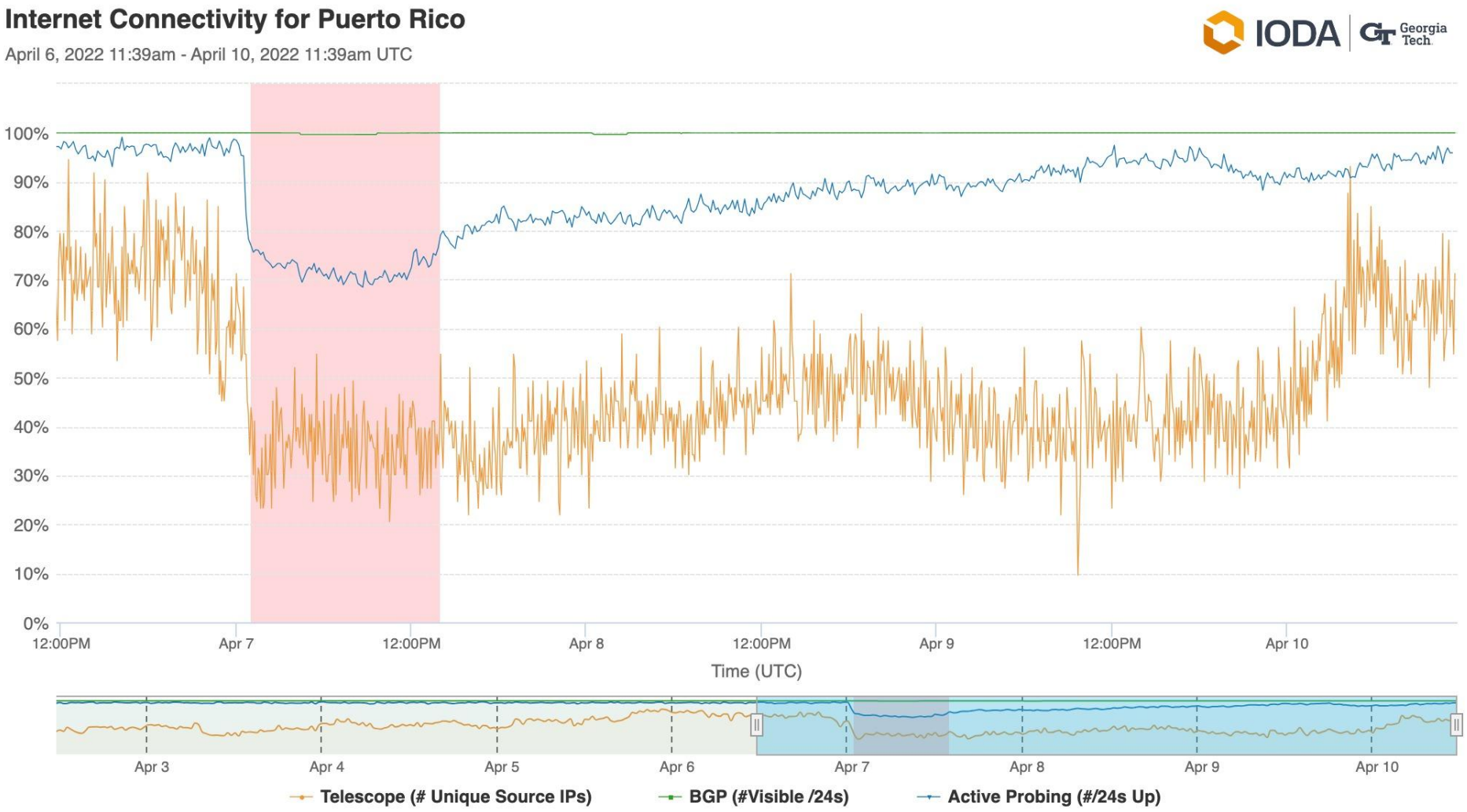
Limitations of IODA

- IODA relies on geolocation datasets that can be inaccurate/ outdated
- Limited to IPv4 (no IPv6)
- Less visibility into countries that heavily use private IP addresses (NAT)
- Less visibility into mobile networks
- IODA cannot tell the cause of a disruption

Recent and Ongoing Research

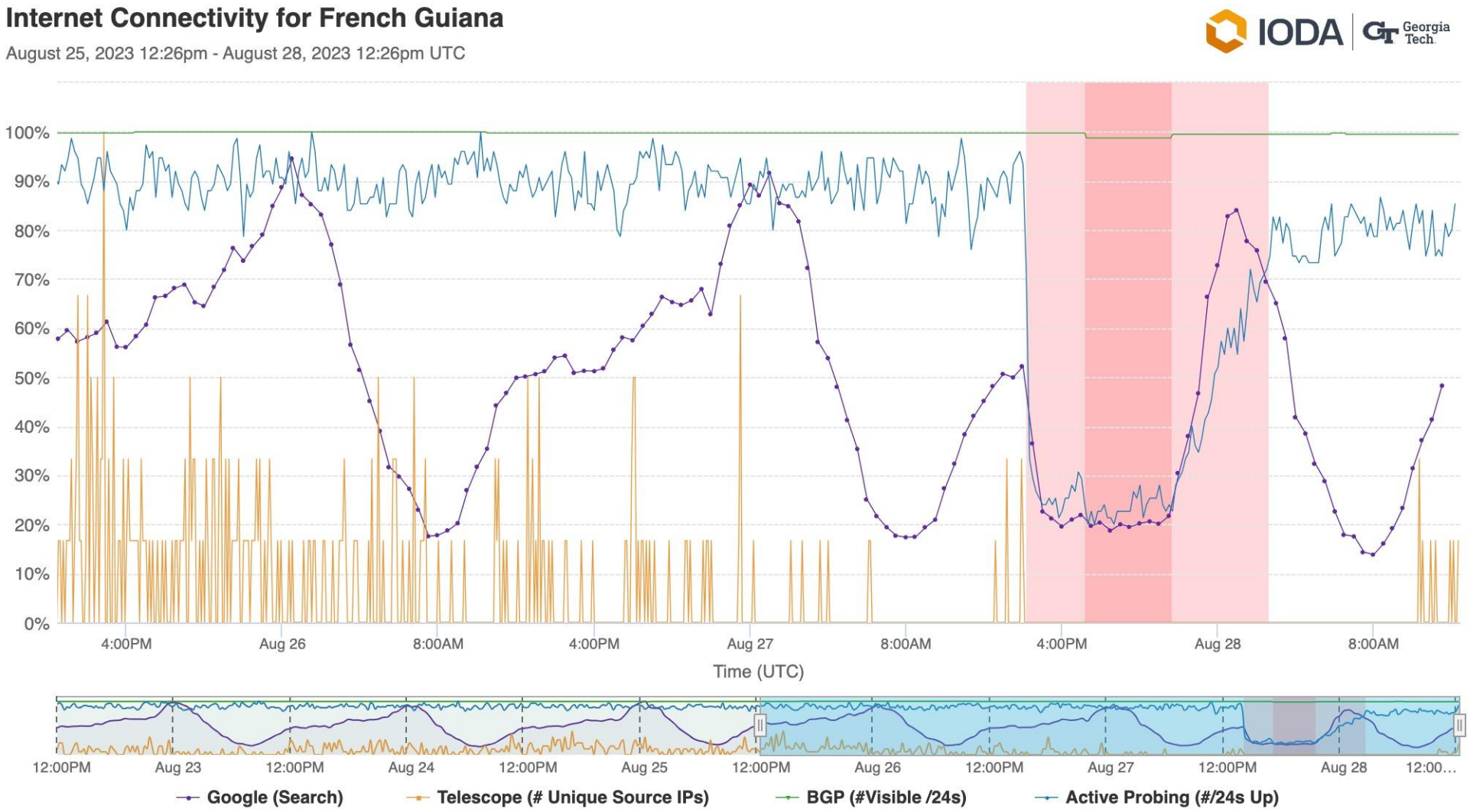
- Signatures of shutdowns vs spontaneous outages
- Connectivity during ongoing conflict
  - Handling a combination of short and long duration drops
- Developing a technique to detect throttling / route changes

Spontaneous Outage



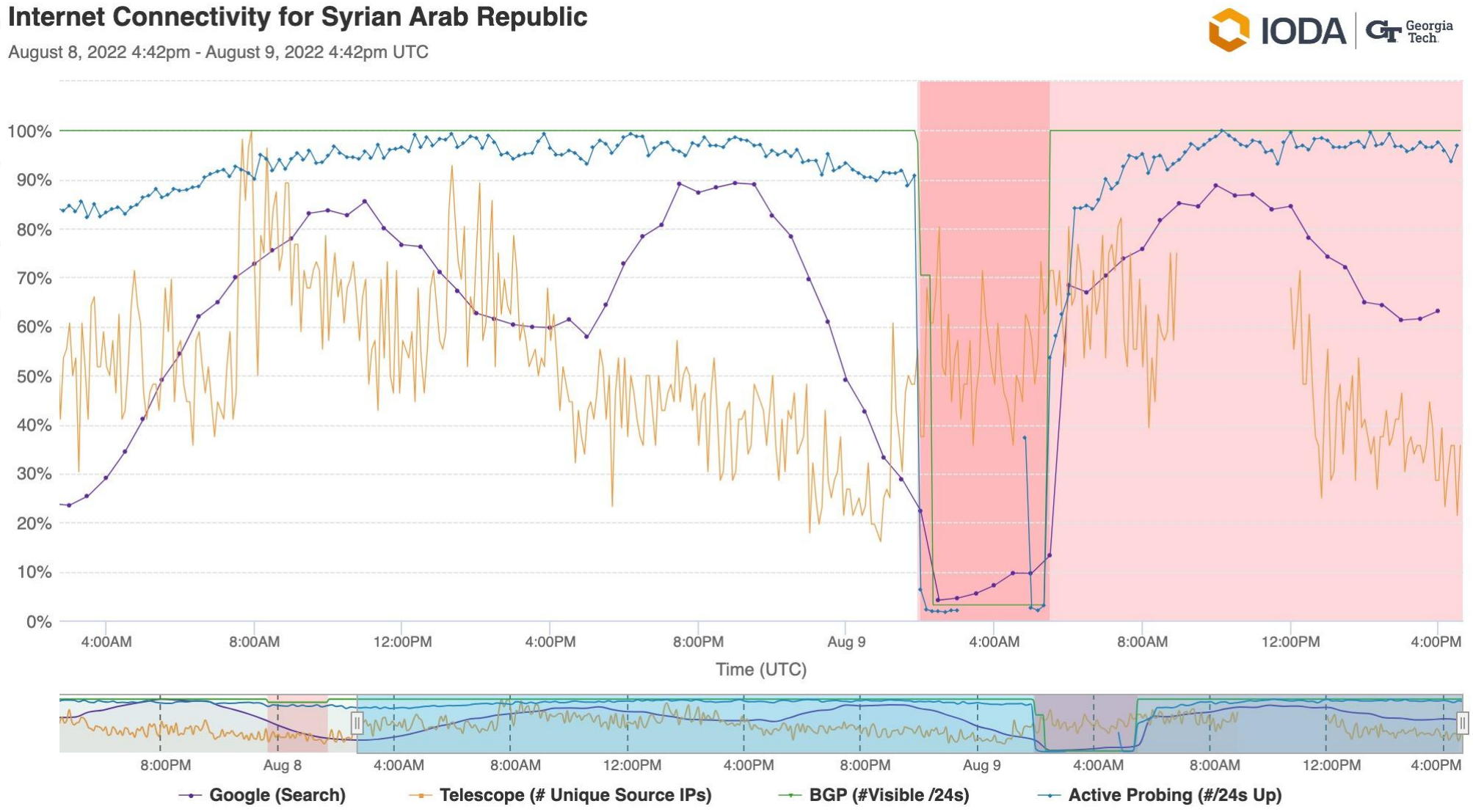
Georgia Tech

Spontaneous Outage



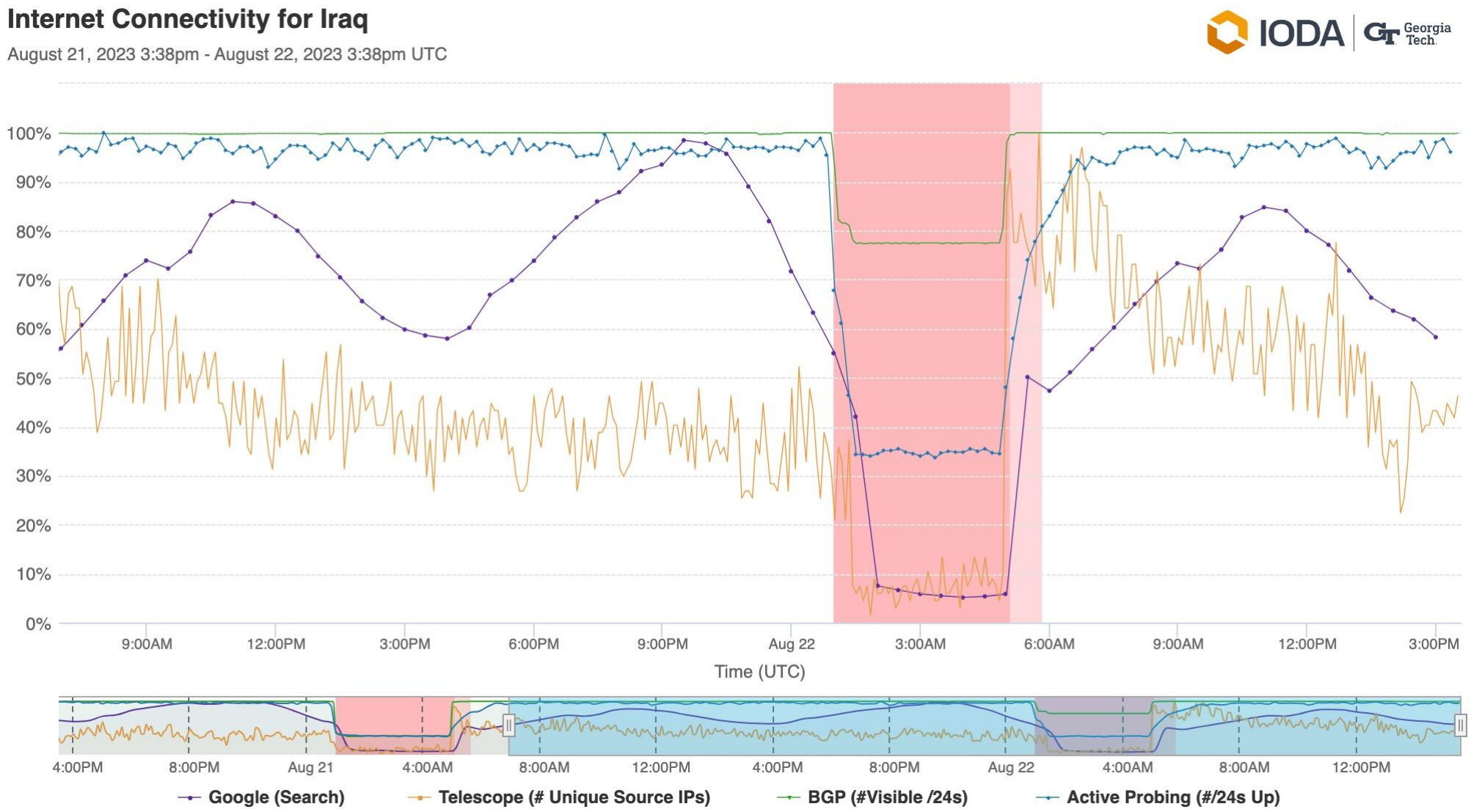
Georgia Tech

Full Network Shutdowns



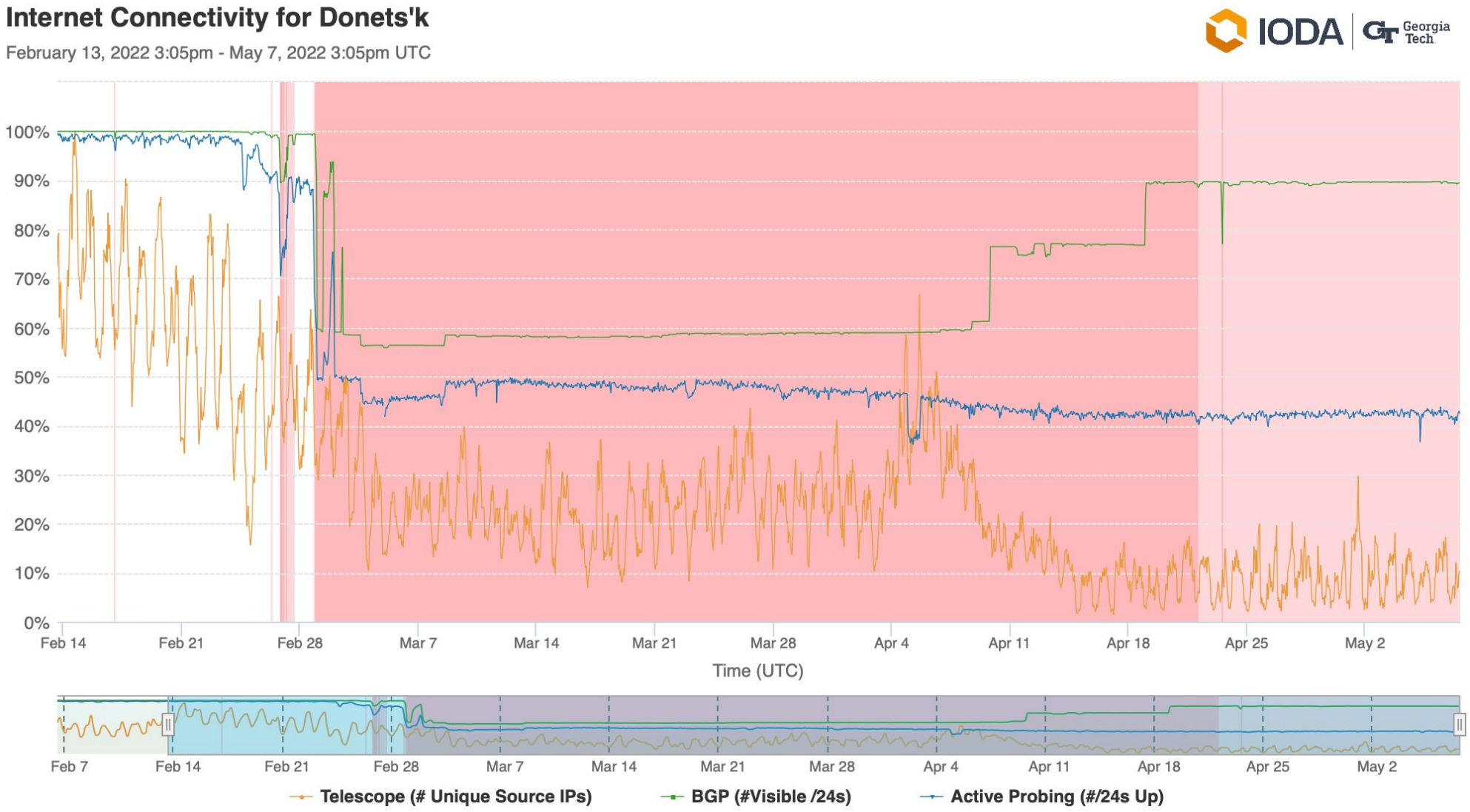
Georgia Tech

Full Network Shutdowns



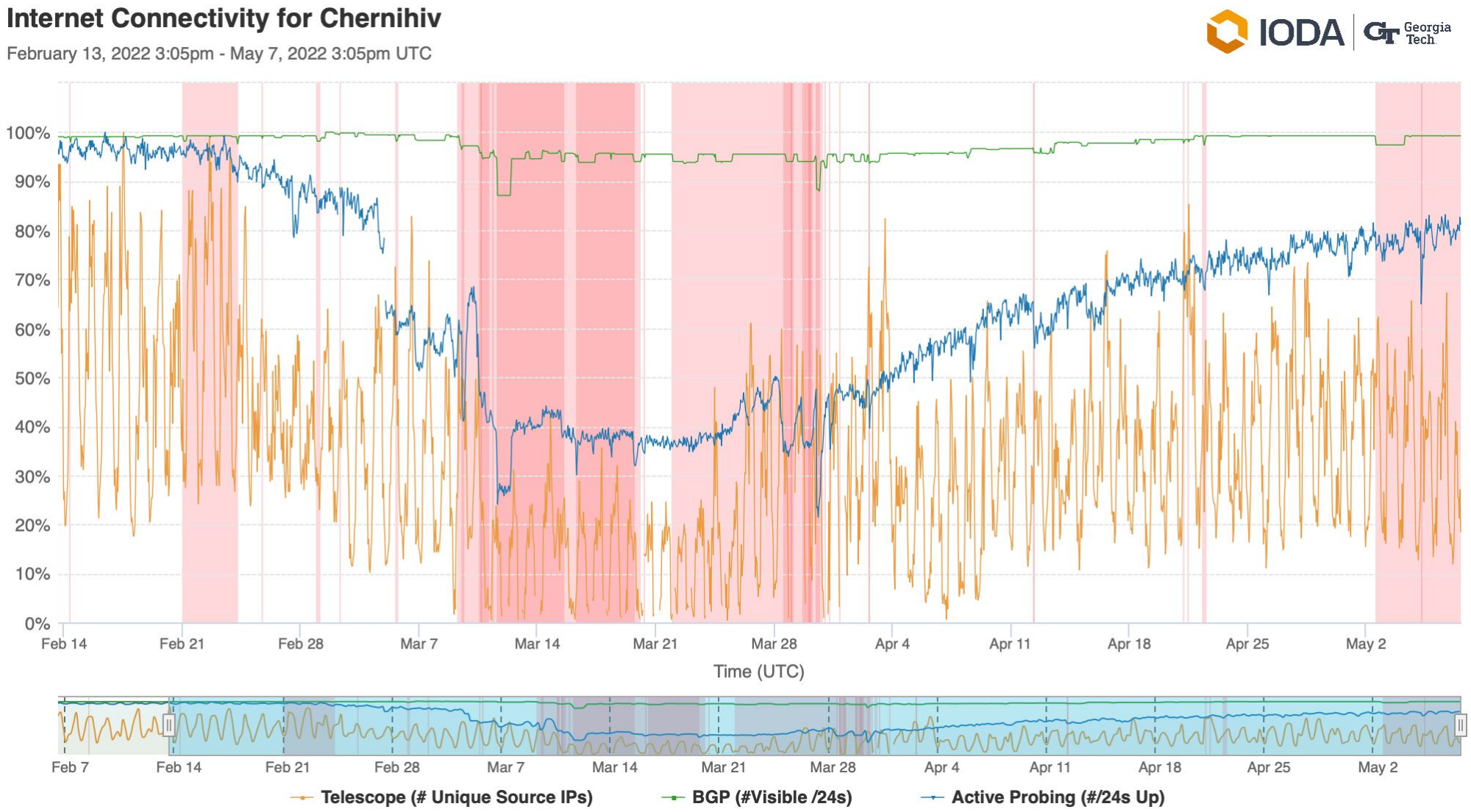
Georgia Tech

Connectivity During Conflict: Ukraine



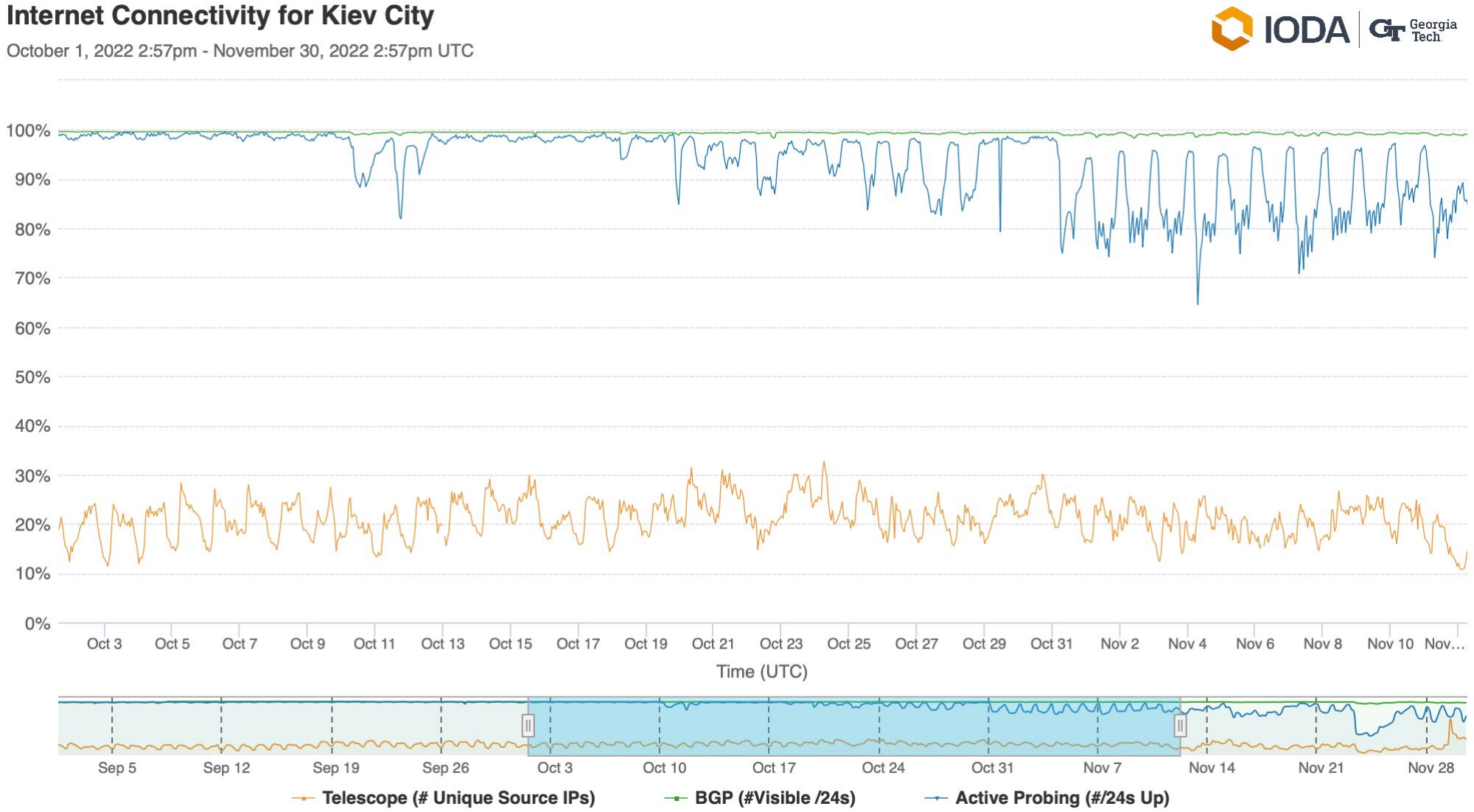
Georgia Tech

Connectivity During Conflict: Ukraine



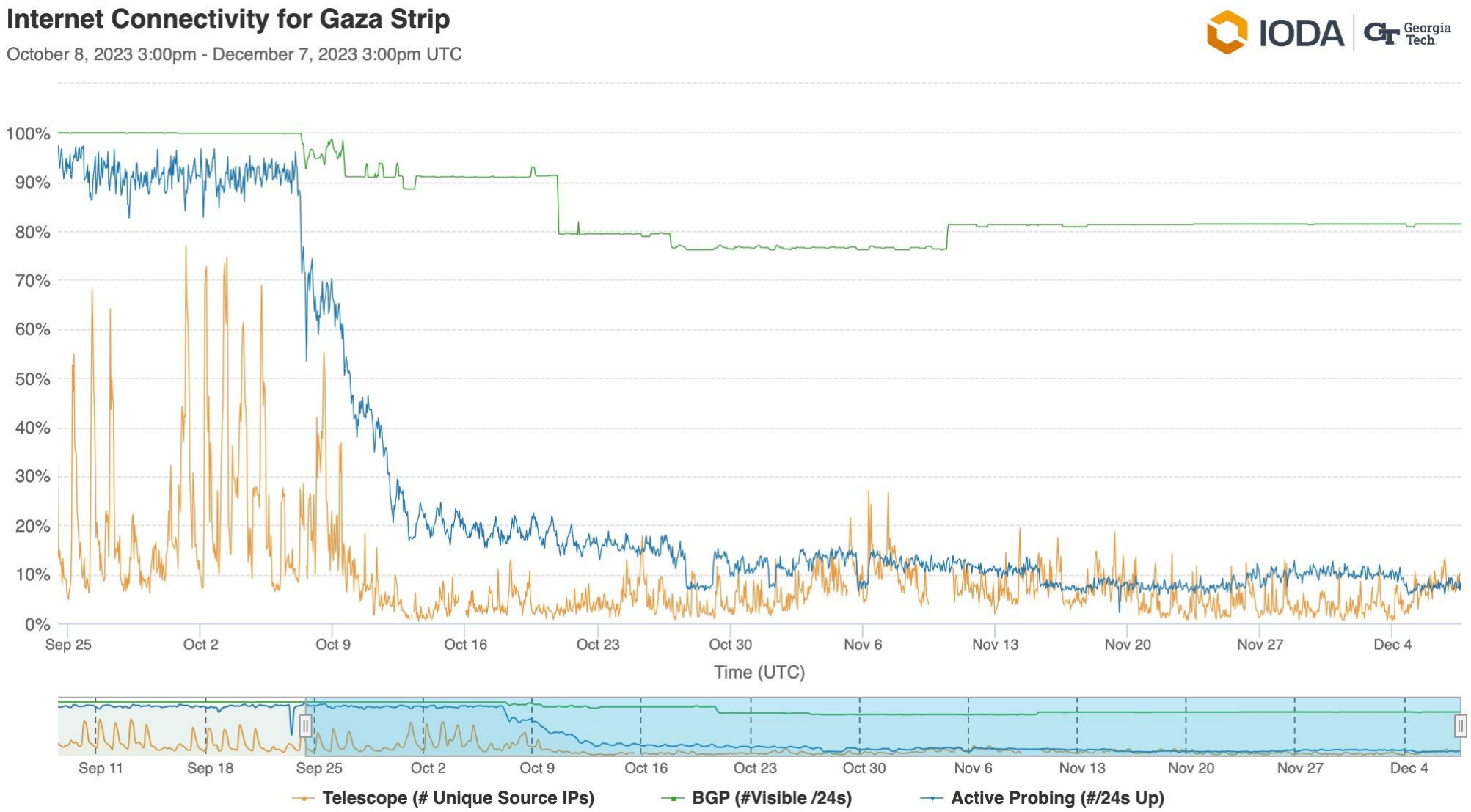
Georgia Tech

Connectivity During Conflict: Ukraine



Georgia Tech

Connectivity during Conflict: Gaza Strip



Georgia Tech

Signatures of a Country-wide Shutdown

- **Countries with shutdowns are the most autocratic scoring countries in the dataset.** However, countries that experience spontaneous outages also score more autocratic than countries that experience neither.
- **Internet shutdowns are significantly more likely to occur on days of political mobilization.**
  - Shutdowns are 9 times more likely to co-occur with protests
  - 16 times more likely to co-occur with elections,
  - 286 times more likely to co-occur during coups. Outages are not significantly more likely to occur on days of political mobilization.
- **Spontaneous outages tend to have shorter durations** compared to shutdowns.
- **Shutdowns are significantly more likely to start on the hour** compared to spontaneous outages.
- **Shutdowns are likely to occur precisely 1, 2, 3, or 4 days after a previous shutdown**

Georgia Tech

Questions?