Censorship

- **Egypt**
  - Start on January 25th, 2011
  - January 27th, 23 million Internet users gone - complete shutdown
  - Total of 5.5 days

- **Libya**
  - Start on February 17th, 2011
  - Three major Internet access disabled:
    - Feb. 18th, 19th, March 3rd
Censorship

- Egypt
  - Prone to manipulation
  - Internet Infrastructure dominated by state ownership
  - Small number involved in international connectivity

- Libya
  - Internet Infrastructure dominated by single state owned AS (12 of 13 IPv4 prefixes)
  - Only two submarine cables with international connectivity
Main Source of Measurements

- **BGP Data**
  - RouteViews
  - RIPE NCC's Routing Information Service (RIS)

- **Unsolicited One-way Internet Traffic**
  - Internet Background Radiation (IBR)
  - Traffic to Unassigned Address Space
  - UCSD Network Telescope

- **Active Traceroute Probing**
  - Archipelago Measurement Infrastructure (Ark)
Data Sources
IP Addresses, BGP Prefixes, AS numbers

- IP Address Ranges geolocated to Egypt or Libya
  - Regional Internet Registries - AfriNIC
  - MaxMind GeoLite Country Database

<table>
<thead>
<tr>
<th></th>
<th>Egypt</th>
<th>Libya</th>
</tr>
</thead>
<tbody>
<tr>
<td>AfriNIC delegated IPs</td>
<td>5,762,816</td>
<td>299,008</td>
</tr>
<tr>
<td>MaxMind GeoLite IPs</td>
<td>5,710,240</td>
<td>307,225</td>
</tr>
</tbody>
</table>

- With given IPs, Mapped to BGP-announced Prefixes and ASes
BGP: Reachability

- BGP Updates & RIB Tables - granularity
- Prefix marked disappeared = withdrawn in routing history, i.e. no longer observable from any route collector peer
BGP: Reachability
BGP: Reachability
Internet Background Radiation

- Network Telescopes: unused IP addresses
  - Conficker
  - Backscatter
  - Other
Internet Background Radiation

- **Conficker**
  - Computer Worm, TCP SYN packets with destination port 445, packet size 48 bytes
  - assumption: Such packets generated by infected systems looking for new victims
  - Source IP addresses not spoofed, geolocation meaningful
Internet Background Radiation

- **Backscatter**
  - Source IP Addresses randomly spoofed
  - Response packet (ex. SYN-ACK) produce backscatter

- **DoS**
Internet Background Radiation

- **Other**
  - Other worms
  - TCP/UDP Scanning
  - Probing activity
  - Misconfigurations
- **More traffic than before blackout**
  - Large TCP/UDP Scan (Jan 31st) resumed (?)
Internet Background Radiation
Active Traceroute Probing

![Graph showing percentage of Ark traceroutes terminating in Egypt over time. The graph indicates a significant drop in January and February, with a notable increase in March and April.]
Libya
Conclusion

- Use of BGP information
- Darknet/Telescope Data
- Traceroute