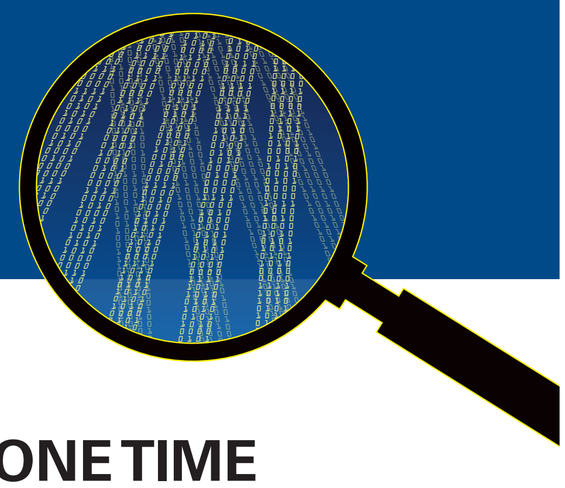
# FloCon®2014



# The Routing Table Tool Suite (RT-Tools)

## MAPPING THE INTERNET ONE ROUTE AT A TIME OR ALL ROUTES AT ONE TIME

## Base Capabilities

The RT-Tools suite displays Autonomous Systems (AS) Network traffic based upon the path analysis of aggregate routing tables. The routing tables are built from data acquired from open source resources located at Oregon University and RIPE. The analysis tools provide a method to make a group of complex relationships more manageable.

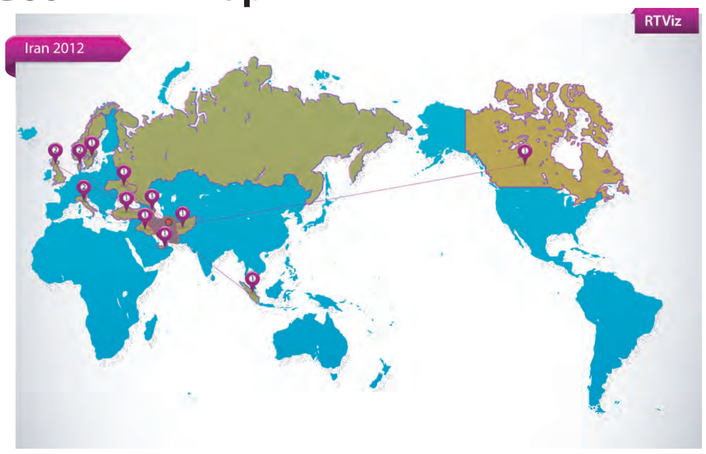
RT-Tools can provide insights into organization characteristics such as

- Geopolitical Affiliation and Stability
- Business Relationships
- Asset Valuation
- Resource Dependence
- Proxy or Filtering Chokepoints

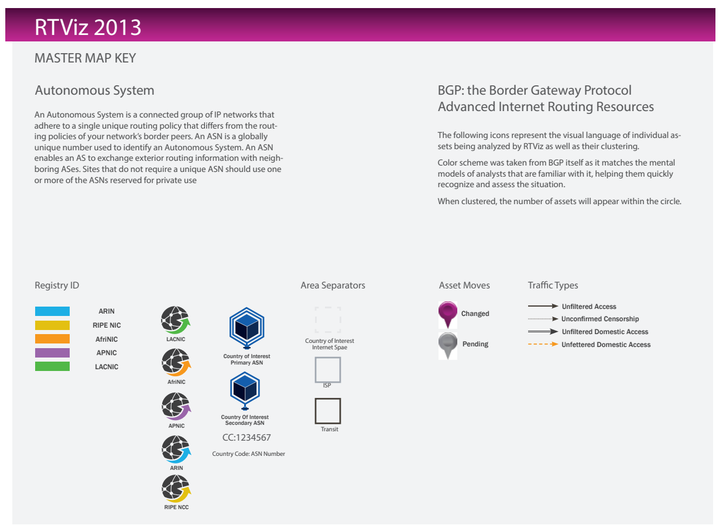
## Differentiators

- Analysis comes from tracking data points over time
- Can be configured to view data comparisons
- Allows for pivoting against different data sources to enrich understanding
- Analyze several routing tables sources concurrently
- Work product shows enriched aggregate consensus

## Geo RTViz Map




## Master Map Key



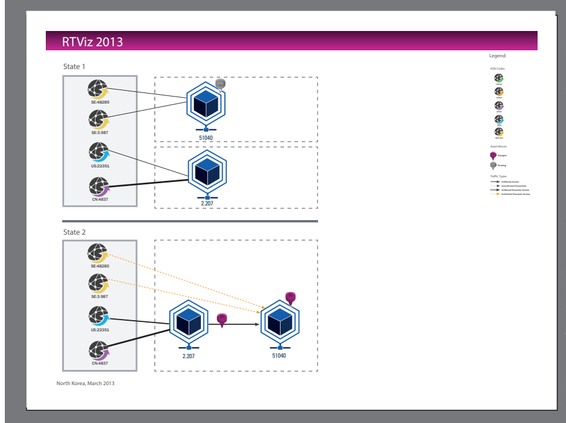

## Data Fusion

RT-Tools integrate data from various sources so that the final product is greater than the sum of its parts. The tools combine information from routing tables with resources that provide entity identification and attribution. This approach establishes a framework that makes patterns more avilable to analysts.

## Future Plans

We are designing RT-Tools to allow external data sources to add greater context. The resulting RTViz map can provide dynamic access to additional data sources to promote real-time analysis that can track historical changes in a single unified interface.

## RT-Tools Visualization

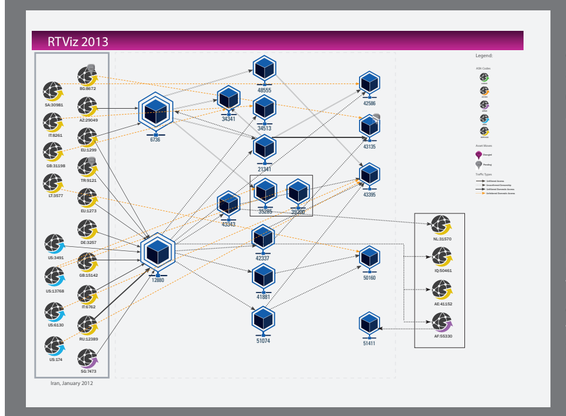



### North Korean Internet Outages in March 2013

Recently North Korea (Democratic People's Republic of Korea) has been in the news for a variety of reasons. There was a widely spread rumor that North Korea had extended an offer to host the Bit Torrent site "The Pirate Bay". There are also numerous legitimate news outlets publishing stories that indicate North Korea is attributing issues with Internet connectivity to acts of aggression from either the United States or South Korea (Republic of Korea).

Contrary to these reports, public routing data is telling us an entirely different story. AS2.207 is routing all North Korean IP addresses through two routes. AS4837 provides terrestrial routing via China, and AS22531 provides an alternate path through Intelsat. AS2.207 hosts only 1,024 IP addresses and all are routed out AS4837, with only 256 being routed out the Intelsat link as well. On March 5, 2013 AS2.207 started advertising AS51040, "The Pirate Bay" AS, and its address space through AS22531. "The Pirate Bay" is a very popular site and the traffic is considerable.

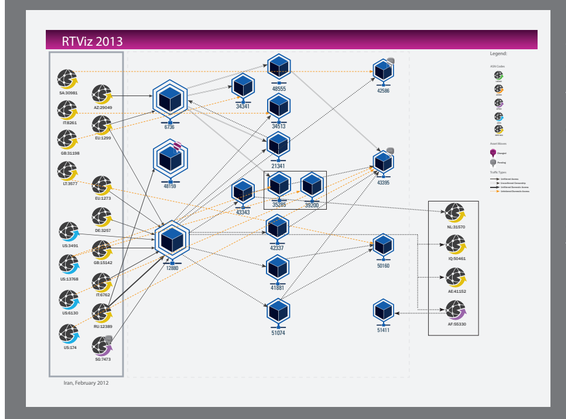
These facts indicate an alternate explanation to the North Korean accusations. The sudden uptick of traffic to the Pirate Bay on the North Korean infrastructure could appear to be a DDoS. Additionally, a large number of well-connected Internet users happen to reside in both the United States and South Korea. However, this traffic increase should not be attributed to the United States or South Korean governments, it is more likely a self-inflicted artifact of hosting the Pirate Bay.




### Iran Internet Routing Changes January 2012

An investigation of the global BGP routing tables presents a country of interest, in this case Iran, as being a very complex series of relationships. By removing the ASNs that are not directly touching the outside or providing alternate access to the outside we get an interesting view of information.

This visualization from January 1, 2012, of the internet perimeter shows that two primary routing chokepoints exist in Iran: AS12880 generally provides high-speed Internet access for over four million IP addresses, while AS6736 likely serves academic needs for over three hundred thousand IP addresses. Many networks connect through both AS's. The Open Net Initiative reports that strict content management is enforced in Iran, and it has been asserted elsewhere that filtering occurs as traffic passes through AS12880, but content management through AS6736 is unknown. The Islamic Republic of Iran Broadcasting (IRIB) AS42586 has a standing alternate satellite connection which bypasses both of these chokepoints. By looking at the routing table snapshot for a single time period we can find which ASNs are dependent on other ASNs for Internet access and which organizations leverage path diversity to assure resilient network access. Some resources are important and require alternate paths for access in the case of a service disruption.

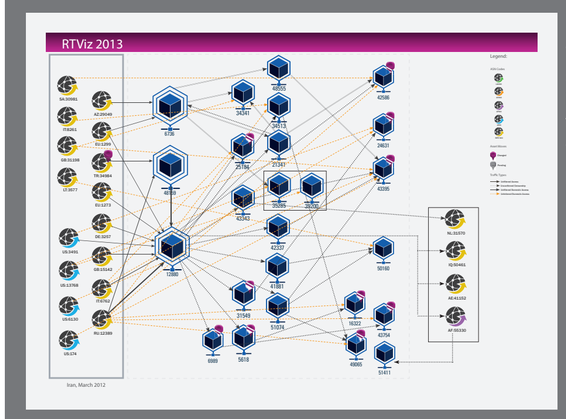



### Iran Internet Routing Changes February 2012

The visualization from February 1, 2012 is missing AS43135; it did not disappear from Iran's communication infrastructure, but it did lose its directly connected route to the outside world. What did disappear from the perimeter of the country of interest are external service providers AS9121 and AS8672.

A significant addition in late January shows up on the February 2013 routing visualization AS48159, becomes visible and is directly attached to the outside without being behind either chokepoint.

Other observed ASN that highlight interesting behavior are those that appear to be Tier 2 service providers, like AS51074, or are highly connected as previously mentioned AS42586 or AS43135, AS43395, and AS50160. If the assertion that AS12880 provides internet filtering or acts as a proxy, any connection that routes around the chokepoint is potentially significant.




### Iran Internet Routing Changes March 2012

The routing visualization from March 1, 2012 shows decidedly more activity with regards to the directly connected ASN. AS48159 is connected to another external peer that was not previously visible. Multiple inside ASN present connections to the Internet: AS16322, AS24631, AS25184, AS43754, AS49065. None of these ASNs are new but their connections directly to the Internet are.

The newly visible ASNs are not connecting through a new external service provider; they were previously routed from the inside to the Internet through AS12389. What has changed is that they now have routing that bypasses internal transit hosts and become visible in this representation.

http://www.cert.org/flocon

**CERT/CC-2013-72**

©2013 Carnegie Mellon University

CERT | Software Engineering Institute | Carnegie Mellon University