



Bad guys are everywhere,  
good guys are somewhere!

NSA/CSS Threat Operations Center (NTOC)

NTOC Technology Development



# (U) NTOC



- (U//FOUO) Operates under *both* SIGINT and Information Assurance authorities
  - Leverage SIGINT, IA, OSINT
- (U//FOUO) Coordinates Integrated Cyber Operations
  - V2: Analysis
  - V3: Operations
  - V4: Technology Development Support
    - V45: Technology Development Division



## (U) V45 - Projects



- (U//FOUO) TREASUREMAP
  - Massive Internet mapping, exploration, and analysis engine
- (U//FOUO) PACKAGEDGOODS
  - Globally dispersed traceroute generators
- (U) Other Projects





# (U) What is TREASUREMAP?



(U//FOUO) Capability for building a near real-time, interactive map of the global internet.

Map the entire Internet – Any device\*, anywhere, all the time

(U//FOUO) We enable a wide range of missions:

- Cyber Situational Awareness – *your own network plus adversaries'*
- Common Operation Pictures (COP)
- Computer Attack/Exploit Planning / Preparation of the Environment
- Network Reconnaissance
- Measures of Effectiveness (MOE)

(\* limited only by available data)



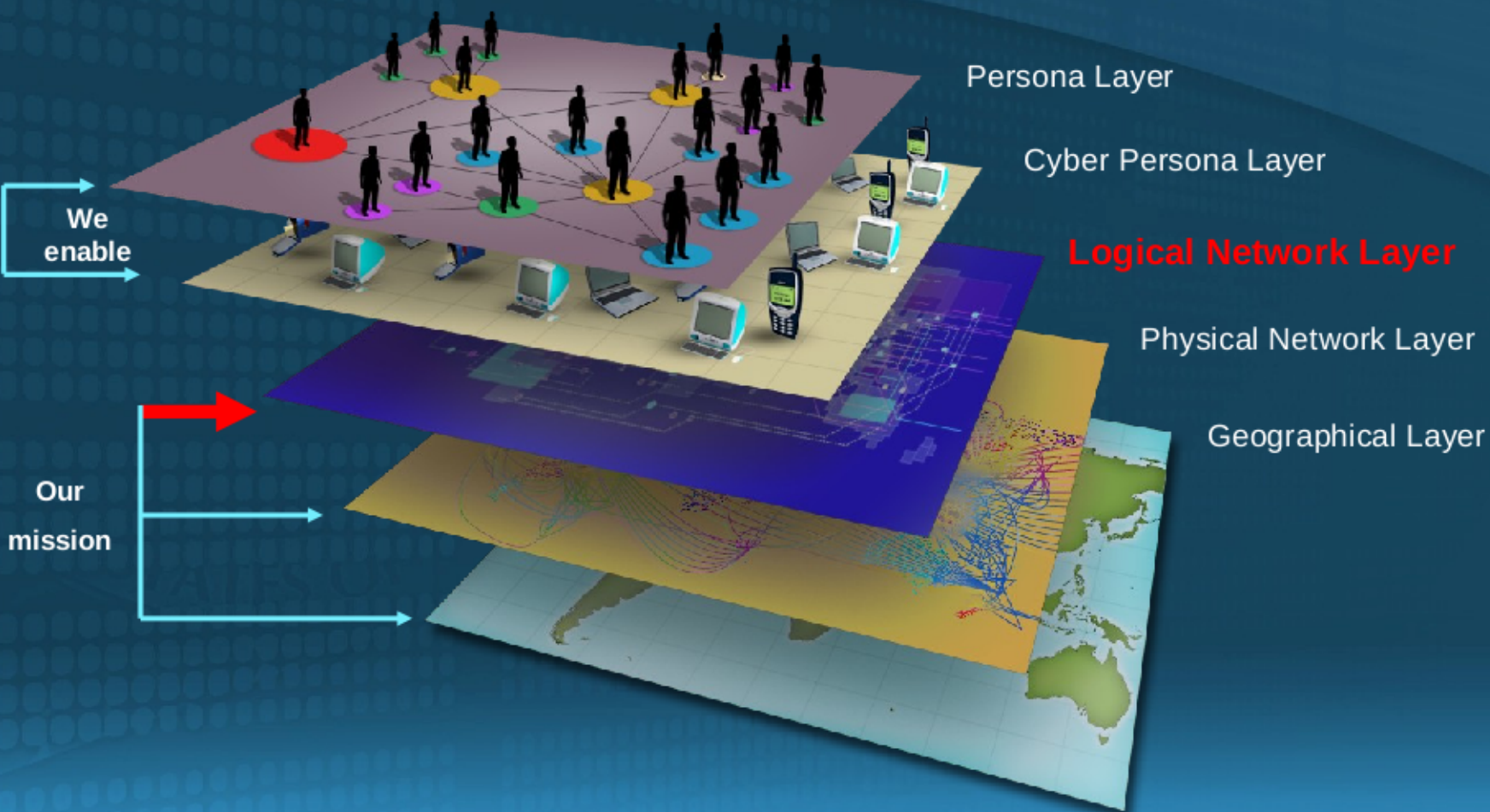
# (U) TREASUREMAP



- (U//FOUO) **Continual generation** of global Internet map, IPv4 and IPv6 (limited)
- (U//FOUO) Focus on logical layers (router and autonomous system), but touches physical, data link, and application layers
- (U) Its Huge.



# (U) TREASUREMAP as an Enabler





## (U) Current State



- (U//FOUO) Data Sources
  - *Open Source Intelligence (OSINT) \* & Academic*
  - *Commercially Acquired*
  - SIGINT
  - Information Assurance
- (U//FOUO) Available on multiple networks to many user groups
  - NSAnet – TREASUREMAP (TM)
    - 5-Eyes partners
    - JWICS users - USG IC
  - SIPRNet – USG IC /DoD – TREASUREMAP-SIPR (TM-S)
- (U) New capabilities delivered every 90 days
- (U) 30+ Gigabytes of additional data added and replaced per day

(\* OSINT – Open Source / Publicly available Internet Meta-Data)



## **(U) Data Sources**

Feed the Machine





# (U) OSINT, Commercial & Academic



- (U//FOUO) BGP
  - Gives the 300,000 foot view of the Internet
  - Defines routing across Autonomous Systems (AS)
  - Origination of IP address spaces (Prefixes) to AS
  - How the Internet gets knowledge of itself (IP address space)
  - Commercially purchased Data Sources
    - Akamai, SOCIALSTAMP, SEASIDEFERRY
  - Open Source
    - Public BGP, IXP (RIPE), APNIC, ROUTEViews, CERNET



## (U) OSINT, Commercial & Academic

- (U//FOUO) Traceroutes
  - Router –to- router links to targeted IP addresses
  - Creates links between networking devices (routers)
  - TM ingests approx. ~16–18 million traceroutes daily
  - Gives the 300 foot view, router-to-router infrastructure
  - Data Sources
    - ARK – CAIDA’s Archipelago Project \*
    - PACKAGEDGOODS \*
    - SOCIALSTAMP
    - RUSTICBAGGAGE
    - User Input



## (U) OSINT, Commercial & Academic

- (U) Registries - Information on netblock and AS ownership
- (U) DNS - IP address to domain name matching
- (U) Operating System (OS) Fingerprints
  - Software and Operating System characteristics of networked devices
  - ~30-50 million unique IP addresses represented per day



# (U//FOUO) Traceroutes: **PACKEGEDGOODS**



- (U//FOUO) Collects “network measurement” data, on public internet
- (U) Random traceroutes and user requested
- (U//FOUO) **PG-GTR**
  - Currently using ~700 public traceroute sites to perform operations
  - High target (full IP addresses)
  - Capable of ~4K IPv4 and IPv6 traceroutes daily
- (U//FOUO) **PG-Server**
  - High volume: ~6.5 million traceroutes per day
  - Low targeting: IPv4 /24 netblocks or higher
  - Can do whole ASes, Country, Netblocks
  - 13 covered servers in unwitting data centers around the globe
    - **Asia:** Malaysia, Singapore, Taiwan, China (2), Indonesia, Thailand, India
    - **Europe & Russia:** Poland, Russia, Germany, Ukraine, Latvia, Denmark
    - **Africa:** South Africa
    - **South America:** Argentina, Brazil



## (U) Coming Soon!



- (U//FOUO) **PG-Server 2.0**
  - Tasking of full IP address
  - Choice of traceroute types:
    - ICMP
    - ICMP Paris
    - TCP
    - UDP
  - Choice of PG-SVR (for source of traceroute)
  - Auto-refresh



## (U) Traceroutes - CAIDA



- (U) University of California, San Diego
  - Cooperative Association for Internet Data Analysis
  - Archipelago measurement platform
- (U//FOUO) TM data source: ARK
- (U) High volume: ~10 million traceroutes per day
- (U) Random targeting (/24 netblock, BGP advertised)
- (U) 44 Locations: Asia (5), Europe (15), Africa (2), North America (18), South America (2), Oceania (2)



## (U) Internal Sources (Protected Sources)

- (U//FOUO) **PACKAGEDGOODS** - **NTOC**
  - (S) Clandestine traceroute and DNS processor
- (S//SI//REL) **BLACKPEARL** – **NAC**
  - SIGINT session 5-tuple, identified routers, routing protocols, SIGINT access points, (inferred SIGINT access points)
- (S//SI//REL) **LEAKYFAUCET** – **NAC**
  - Flow repository of 802.11 WiFi IP addresses and clients via STUN data
- (S//SI//REL) **HYDROCASTLE** – **NAC/INSCOM**
  - 802.11 configuration data extracted from CNE activity in specific locations
  - (Requires HYDROCASTLE account)
- (S//SI//REL) **MASTERSHAKE** – **NAC**
  - FORNSAT and WiFi collection data
- (S//SI//REL) **S-TRICKLER** - **NTOC**
  - IP address fingerprints and potential vulnerabilities from FORNSAT collection



## (U) Internal Sources (Protected Sources)

- (S//SI//REL) **TOYGRIPPE** - **NAC**
  - Repository of VPN endpoints
- (S//SI//REL) **DISCOROUTE**– **NAC/GCHQ**
  - Router configuration files from CNE and passive SIGINT
  - NAC's DISCOROUTE repository
- (TS//SI//REL) **VITALAIR2** – **TAO**
  - Automated scanned IP addresses for TAO known vulnerabilities
- (U//FOUO) **IPGeoTrap** - **NAC**
  - Provides geolocation services for IP addresses/ranges
- (TS//SI//REL) **JOLLYROGER** – **SSG/TAO**
  - Provides metadata that describes the networking environment of TAO-implemented Windows PCs
  - (Requires JOLLYROGER account)
- (U//FOUO) **TUTELAGE** – **NTOC**
  - Specific alerts from intrusion detection sensors
  - (not currently active)

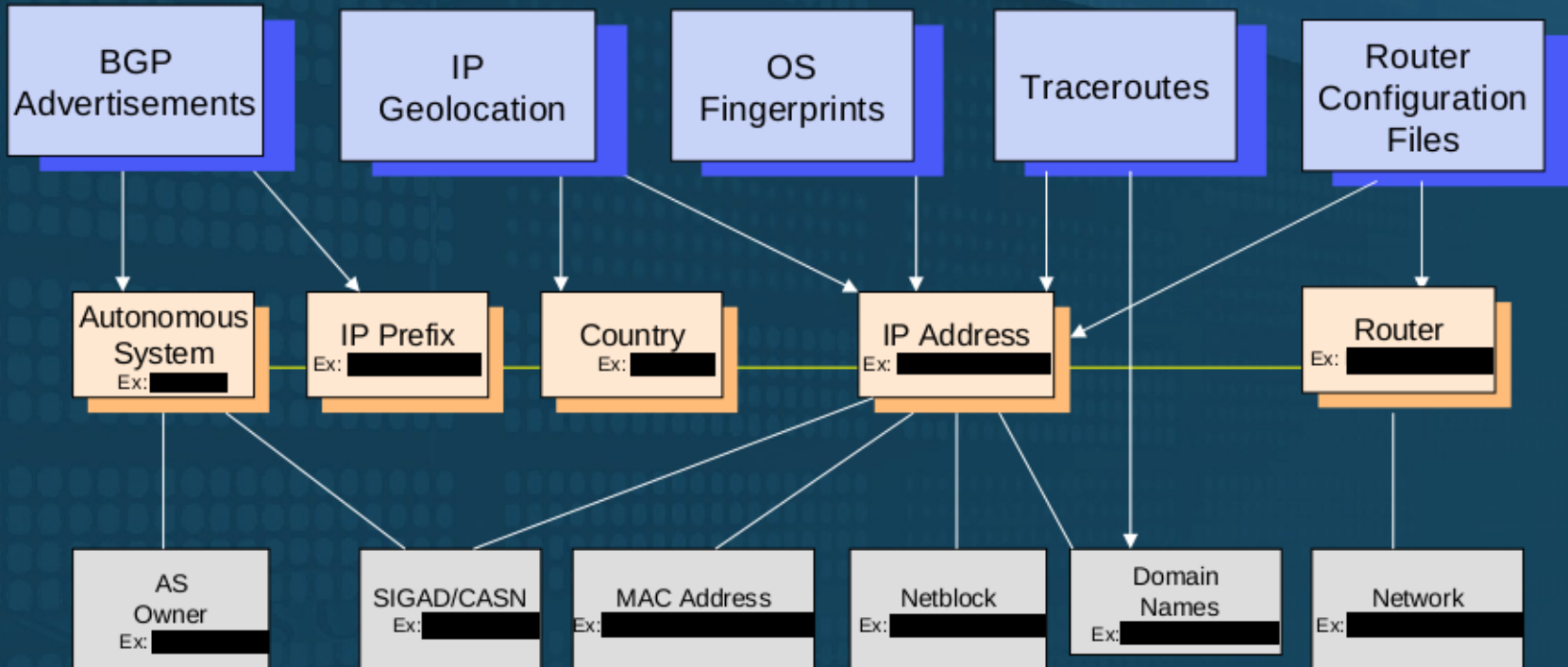




(U) The Whole is Greater  
than the Sum of the Parts



# (U) Data Relationships

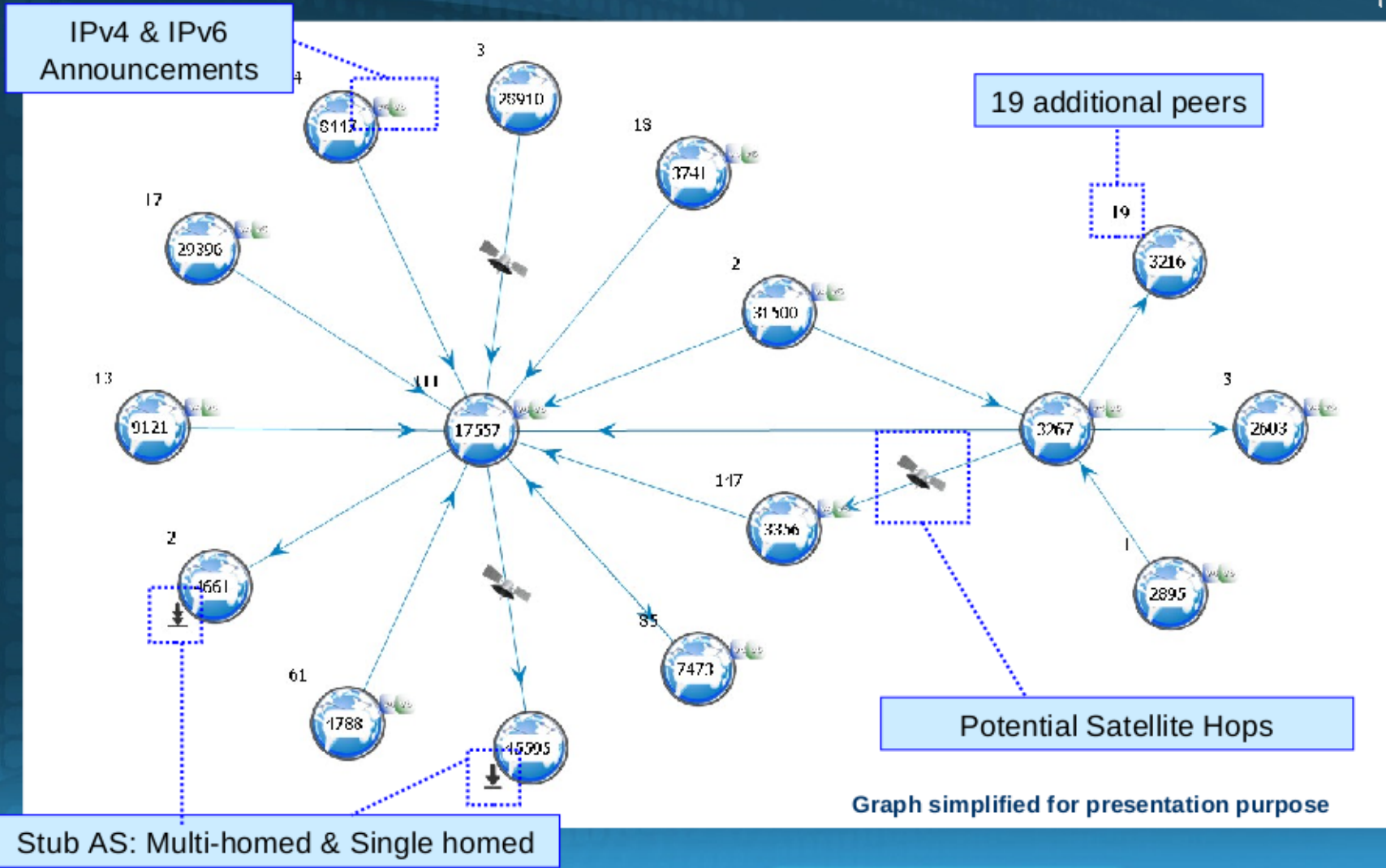


**Yellow** links denotes direct relationships between data types.

For example, we know which AS contains a router because we can relate a router to IP Addresses, IP Addresses to IP Prefixes, then IP Prefixes to an AS.

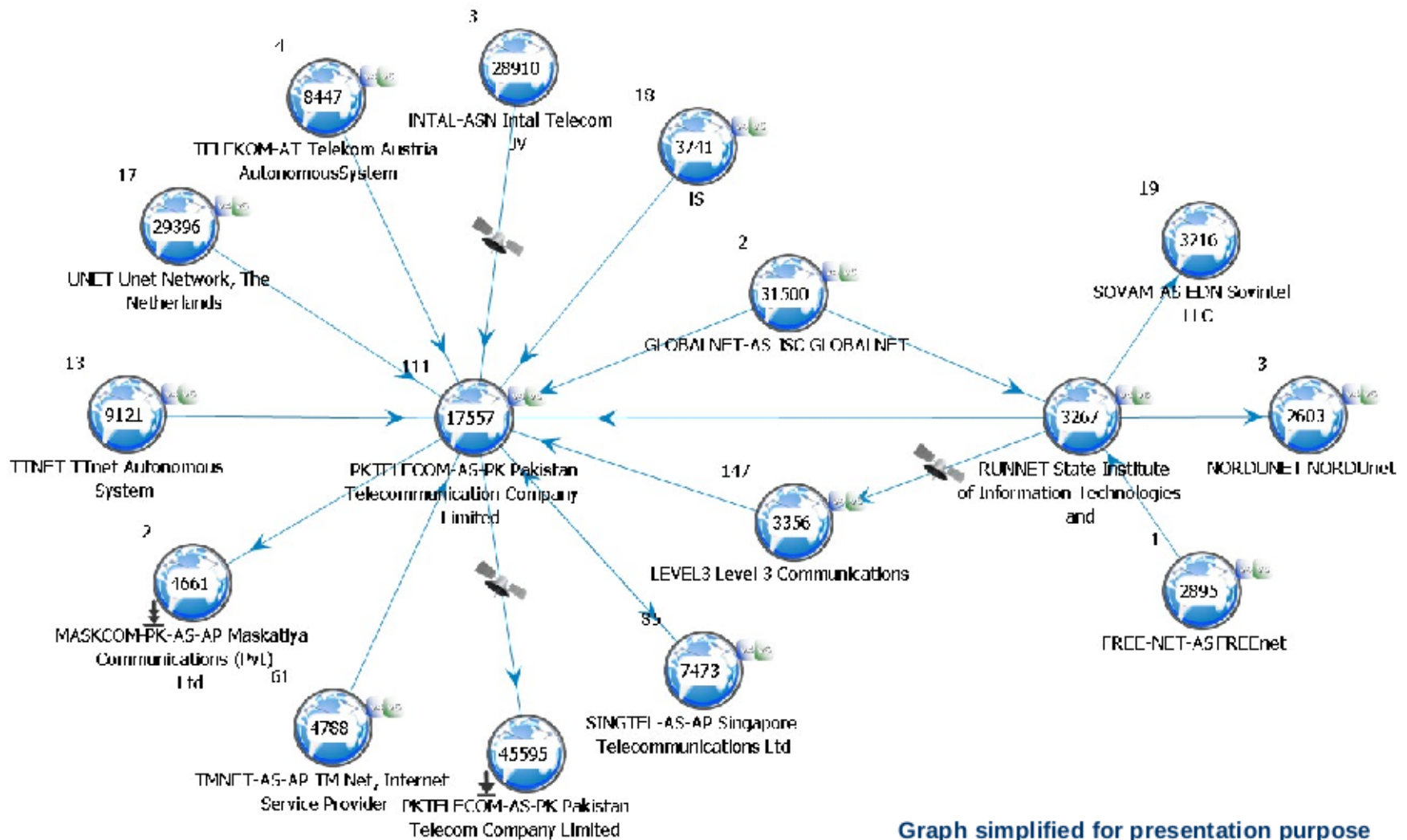


# (U) Autonomous System Peering - BGP



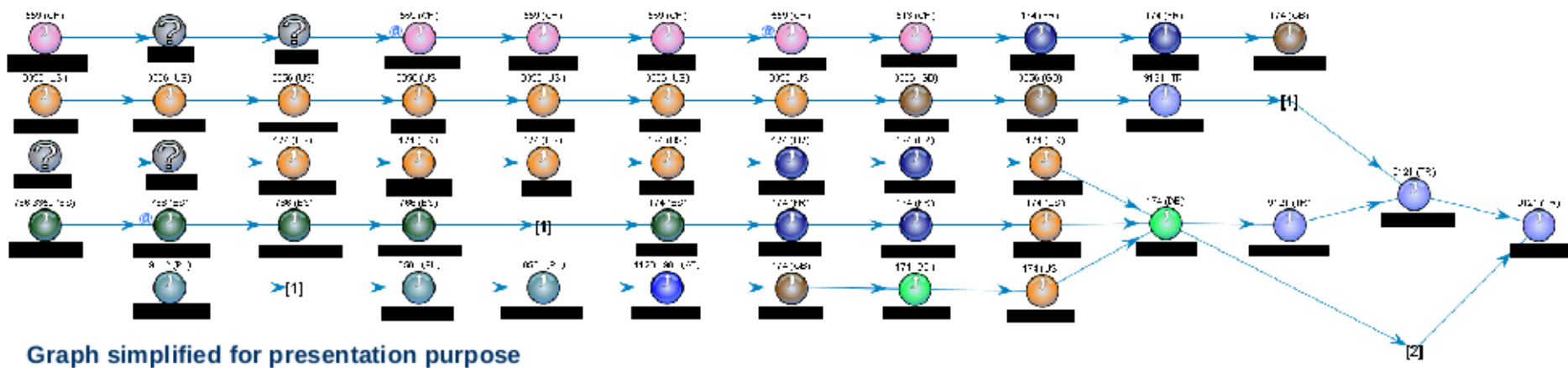


# (U) ... and Registries





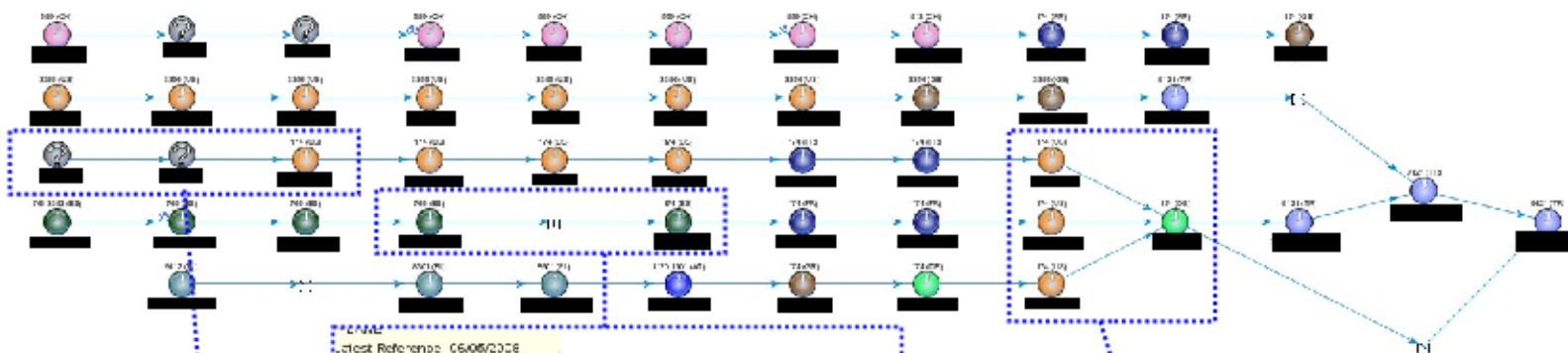
# (U) Internet "flow" to a "Network"



They're color-coded by country. Big deal.



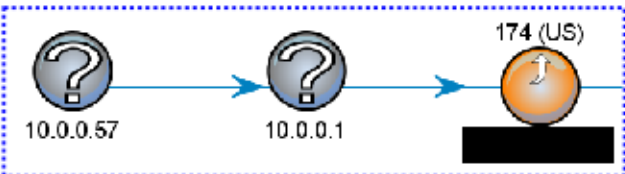
# (U) With Traceroute...



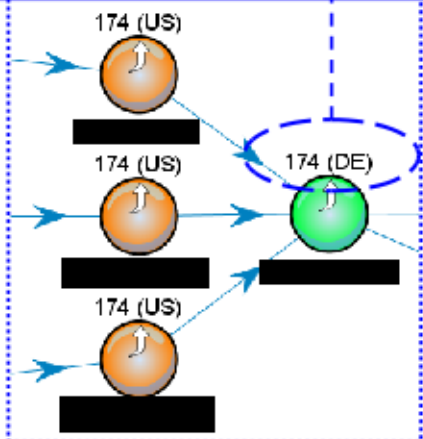
Correlation of IP Address with AS & Country



Missing Hops



RFC1918 Addresses  
(private IP address space)

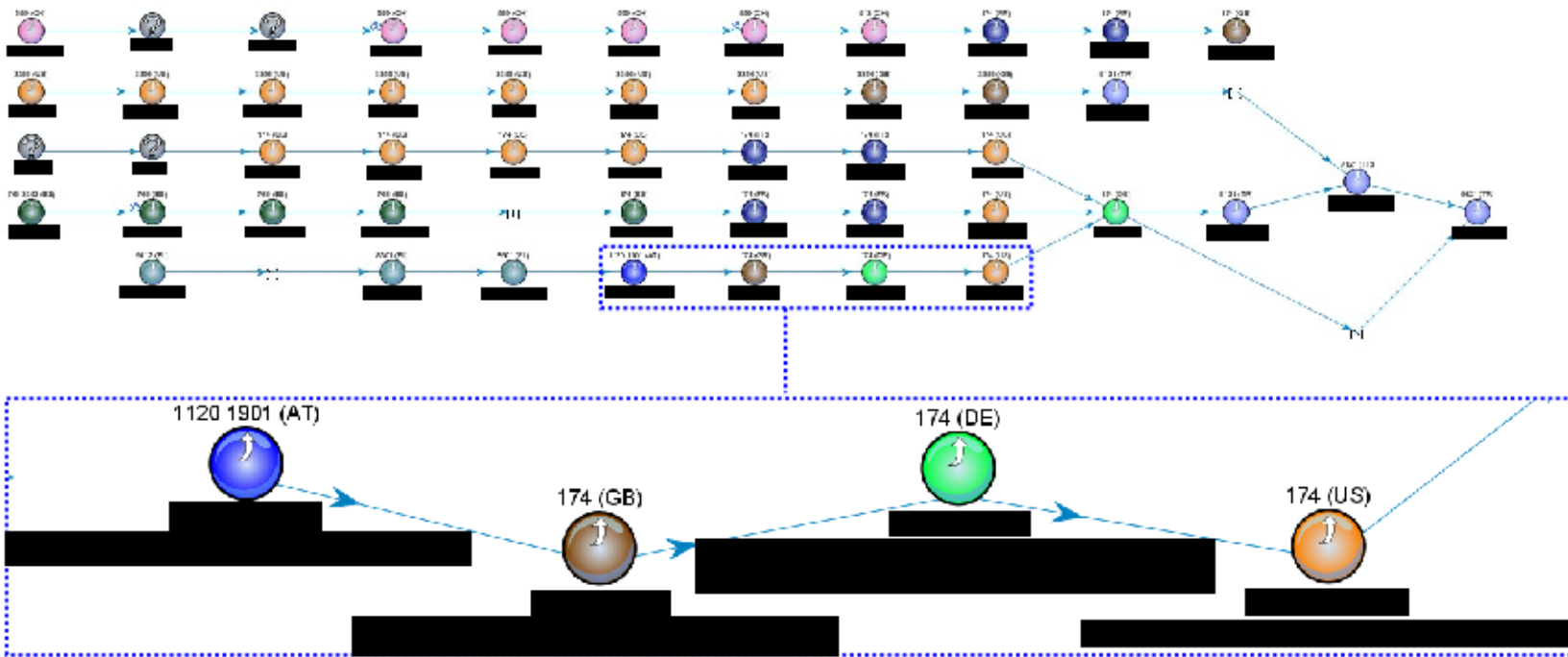


Network Bottlenecks

Graph simplified for presentation purpose



# (U) ... and DNS



Graph simplified for presentation purpose







## (U) Seeing Red

**SIGINT** in the Water





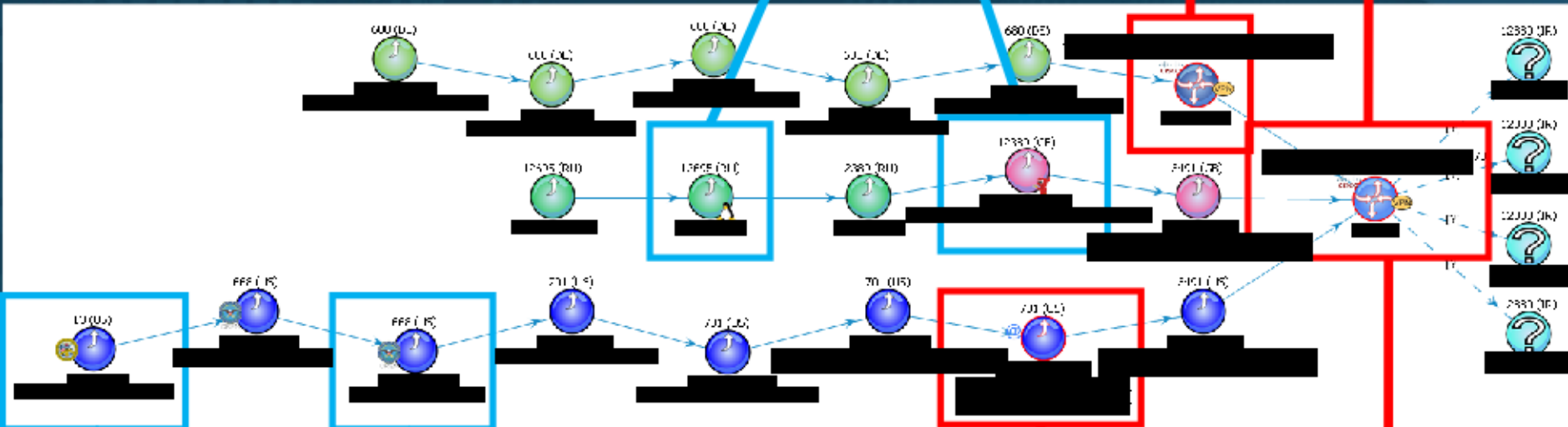
# (S//SI//REL) Traceroute – overlaid with SIGINT and other



TOYGRIPPE (VPN)

Router Configuration  
Router Vendor: Cisco

OS Fingerprints



DoD Shields: DoD IP Addresses

Node Referenced in SIGINT

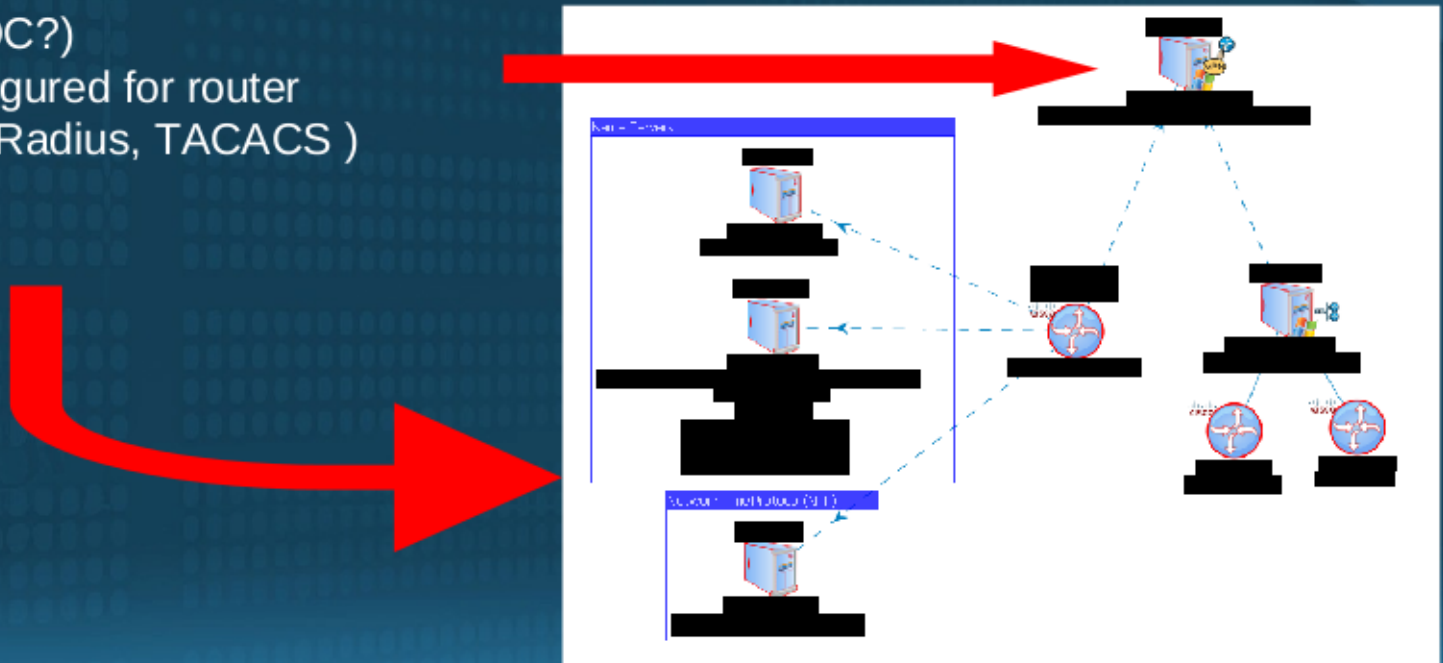
Underscore AS: "Operational" AS =  
12880



# (S//SI//REL) Known Devices



- (S//SI//REL) Sources: DISCOROUTE (NAC router configuration repository)
- (S//SI//REL) Display supporting infrastructure, as configured in router configuration files
  - Where router accessed from (possible NOC?)
  - servers configured for router (NTP, DNS, Radius, TACACS )







# (S//SI//REL) Cisco Discovery Protocol (CDP)



(NO)  
 cisco  
  
 89.254.60  
 SLB-SIN-SW01

CDP Router Report: SLB-SIN-SW01

```

---
Date:                05/04/2010
Device Name:         SLB-SIN-SW01
Model:               cisco WS-C2960-24TC-L
Capabilities:        Performs Level2 Switching
                    L2MP Flag Set
Software Version:    12.2(25)SEE2
Network Prefixes:   -
Duplicate Ports:     -

Physical Port  Address      Protocol  AS  Country  Data Sources
FastEthernet0/6  89.254.60  IP        N/A  NORWAY   BP_IRL [05/09/2010 20:00:00]
  
```





## (U) Communities



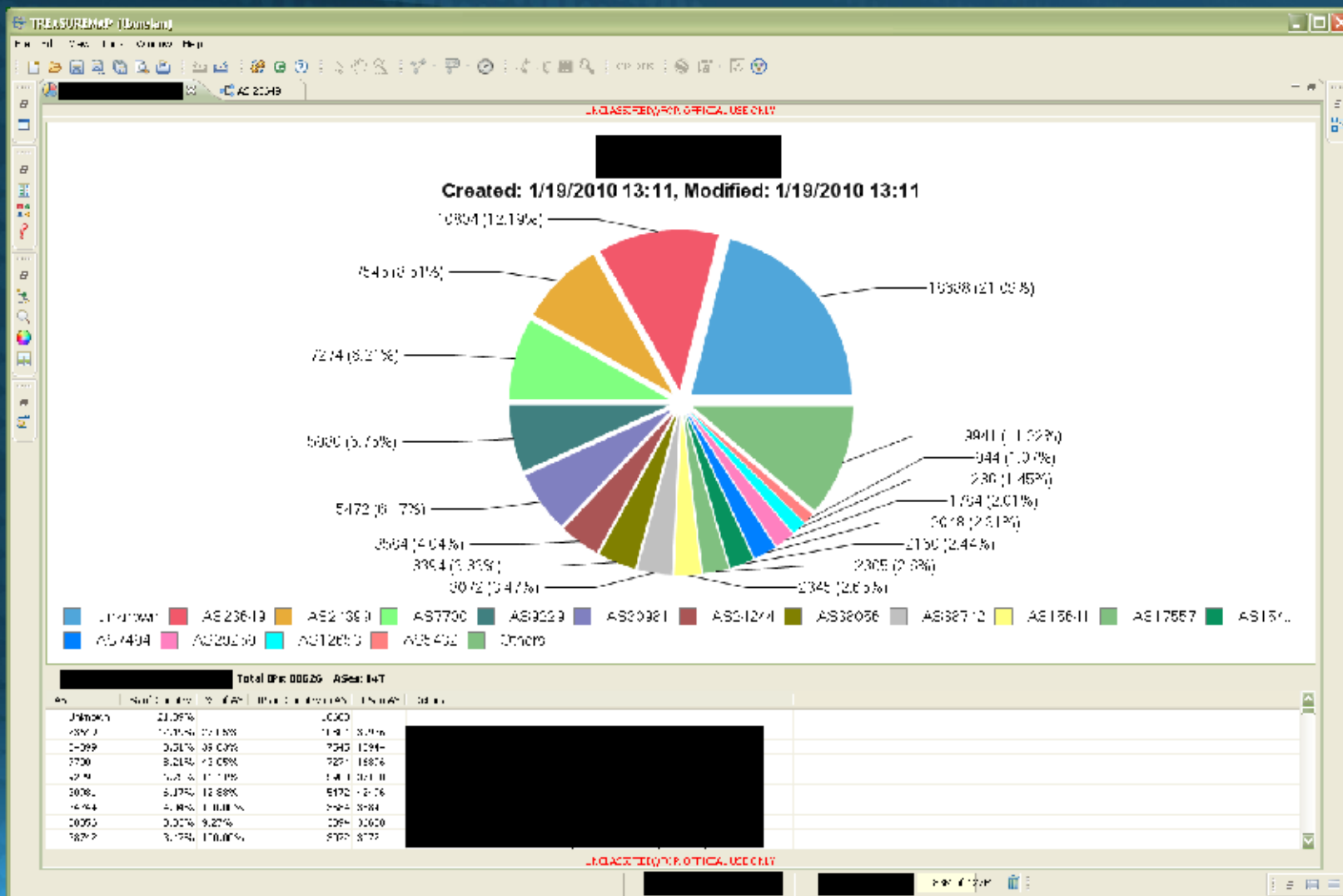
- (S//SI//REL) Individual IP addresses related by a common attribute
  - TOR router
  - Servers (DNS, NTP, SNMP, TACACS, RADIUS)
  - Hide IP NG Proxy Servers
  - BYZANTINE HADES Infrastructure hosts/infected hosts
- (S//SI//REL) Sources: (Varies)
  - Currently TOR router advertisements
  - router configurations
  - XKEYSCORE







# (U) Country (AS Presence)





## (U//FOUO) TREASUREMAP Workspace

- (U//FOUO) **Toolbar**: Offers access to a variety of commonly used functions
- (U//FOUO) **Search Pane**: Input search parameters
- (U//FOUO) **Advanced Search Options**: Preferences for searches
- (U//FOUO) **Release my search to PG**: Requesting traceroutes for target IP addresses
- (U//FOUO) **Other Searches**: Includes Router, DNS, Batch IP/MAC and JOLLYROGER
- (U//FOUO) **Legend**: Contains all of the icons and decorations as seen in an active graph
- (U//FOUO) **Send Feedback**: Provides a way to communicate questions, comments or problems to the TREASUREMAP team.



## (U//FOUO) TREASUREMAP Search Items

1. (U//FOUO) IP Address
2. (U//FOUO) Routers
3. (U//FOUO) DNS (FQN)
4. (U//FOUO) MAC address / 802.11 BSSID / 802.11 SSID
5. (U//FOUO) IP Prefix / Range (CIDR Notation)
6. (U//FOUO) Registry Netblock
7. (U//FOUO) SIGAD and/or Case Notation
8. (U//FOUO) Country / IP Country Code
9. (U//FOUO) Autonomous System (AS) Number
10. (U//FOUO) Free Text

# (S//SI//REL) User Interface: NAVS



The screenshot displays the NAVS interface with several key components:

- Traceroute routing infrastructure:** A network diagram showing nodes (routers) and links (connections) between them, color-coded by path.
- Node detail pop-ups:** A callout box pointing to a specific node in the network diagram.
- Node Clustering:** A callout box pointing to a group of nodes in the network diagram.
- Summary Information:** A callout box pointing to a table at the bottom of the interface.
- Tabular data:** A callout box pointing to the data rows in the summary table.


The summary table at the bottom is titled "Traceroutes Summary" and contains the following columns:

Date Source	Trace Target	Trace Network	Trace AS	Trace Country	Trace Path	Origin Location	Origin AS	Origin Country	Trace ID
									04/06/20
									UNUS-23
									04/06/20
									UNUS-23
									04/04/20
									UNUS-23
									04/04/20
									UNUS-23

# (UFOUO) User Interface: Website



Dynamic Page - 3/26/2008 1:54:06 PM - TS//SI//REL TO USA, FVEY



[Home](#) | [FAQ](#) | [Help](#) | [Privacy](#) | [Terms](#) | [Feedback](#)

[HOME](#) | [QUERY](#) | [USERS](#) | [PACKAGEDGOODS](#) | [DATA](#) | [TOOLS](#) | [GALLERY](#)

**UPDATE** On Friday, 06 February 2008 at approximately 1600 EST, TREASUREMAP deployed an update to the system. If running a shared installation (please contact your system administrator). To continue with the new version, select "Proceed with Update" when prompted. If you have a shared installation and/or are encountering, to continue using the current version select "Work Offline without Update" until your system administrator can update you to the current version.

**Share URLS ONLINE!**

(SMALL) The TREASUREMAP system provides a near real time, interactive map of the global internet. By using public domain, commercial, BGP/AS, and IAS data, the TREASUREMAP system provides a more relevant view of the broader internet, including new links between advertisers and their target manufacturers. Selected intelligence information, such as data centers, public domain names, countries, operating systems, and ISPs, is reflected in various, automatically generated, online search results data and overlaid on the network topology maps, giving users a powerful network analysis tool.

**TREASUREMAP on Twitter** - [http://twitter.com/treasuremap](#)  
**TREASUREMAP on SIPR** - [http://sopr.com/treasuremap](#)  
**TREASUREMAP on YouTube** - [http://www.youtube.com/treasuremap](#)

**TREASUREMAP Help Desk**

- [Home](#)
- [FAQ](#)
- [Help](#)
- [Privacy](#)
- [Terms](#)
- [Feedback](#)


Government Level: [\[Redacted\]](#)  
Customer Service Team: [\[Redacted\]](#)

**Small text-based queries**

Advanced

Enter:

**Download TREASUREMAP**



Supports all NRA, 2nd Party, and Third Party Users

[Other Install Files](#) [Installation](#)

**TREASUREMAP 3.1 New Features**

- New data sources to access network analysis and the backbone and ISP's data.
- New capability to Show US Show Fingerprints Data Records from the new, dynamic, Dynamic ASB.
- New functionality to Show Recently Closed Circles.
- New capability to View and Export Top of Mapped Domains to CSV format.
- New functionality within the Topology View function.
- New ability to Identify Node Density on a graph to more easily identify critical nodes/poits.
- Improved Sorting capabilities.
- New IPv6 Network Search capabilities.
- New and improved Look and Feel of the TREASUREMAP Website.
- New Search functionality to search the TREASUREMAP Website and help contents and quickly find what you need.
- Enhanced Chatting capabilities.
- TREASUREMAP Client Calculation now supports IPv6 protocols.
- New Slide Animation to assist in navigating around node

**Video Tutorials**

Click on the links below to view the tutorial:

- ▶ [First Time Full Tutorial](#)
- ▶ [How to Use the Search](#)
- ▶ [How to Use the Topology](#)
- ▶ [How to Use the IP Search](#)
- ▶ [How to Use the AS Search](#)
- ▶ [How to Use the Country Coverage](#)
- ▶ [How to Use the Country Coverage](#)
- ▶ [How to Use the Country Coverage](#)
- ▶ [How to Use the Country Coverage](#)
- ▶ [How to Use the Country Coverage](#)
- ▶ [How to Use the Country Coverage](#)
- ▶ [How to Use the Country Coverage](#)

**Getting Started**

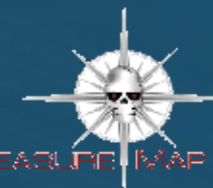
1. Click Download TREASUREMAP below, and log.
2. Execute the installer and follow the instructions.
3. Run the application using the desktop shortcut.

© 2008 - All Rights Reserved

On-line Help

New Features Update

Video Tutorials



# (U//FOUO) TREASUREMAP Contact Info

- [REDACTED]
  - Government Lead
  - [REDACTED]
- Customer Support Team
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
- Email: DL
  - [REDACTED]
  - [REDACTED]