TREASURE MAP

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:

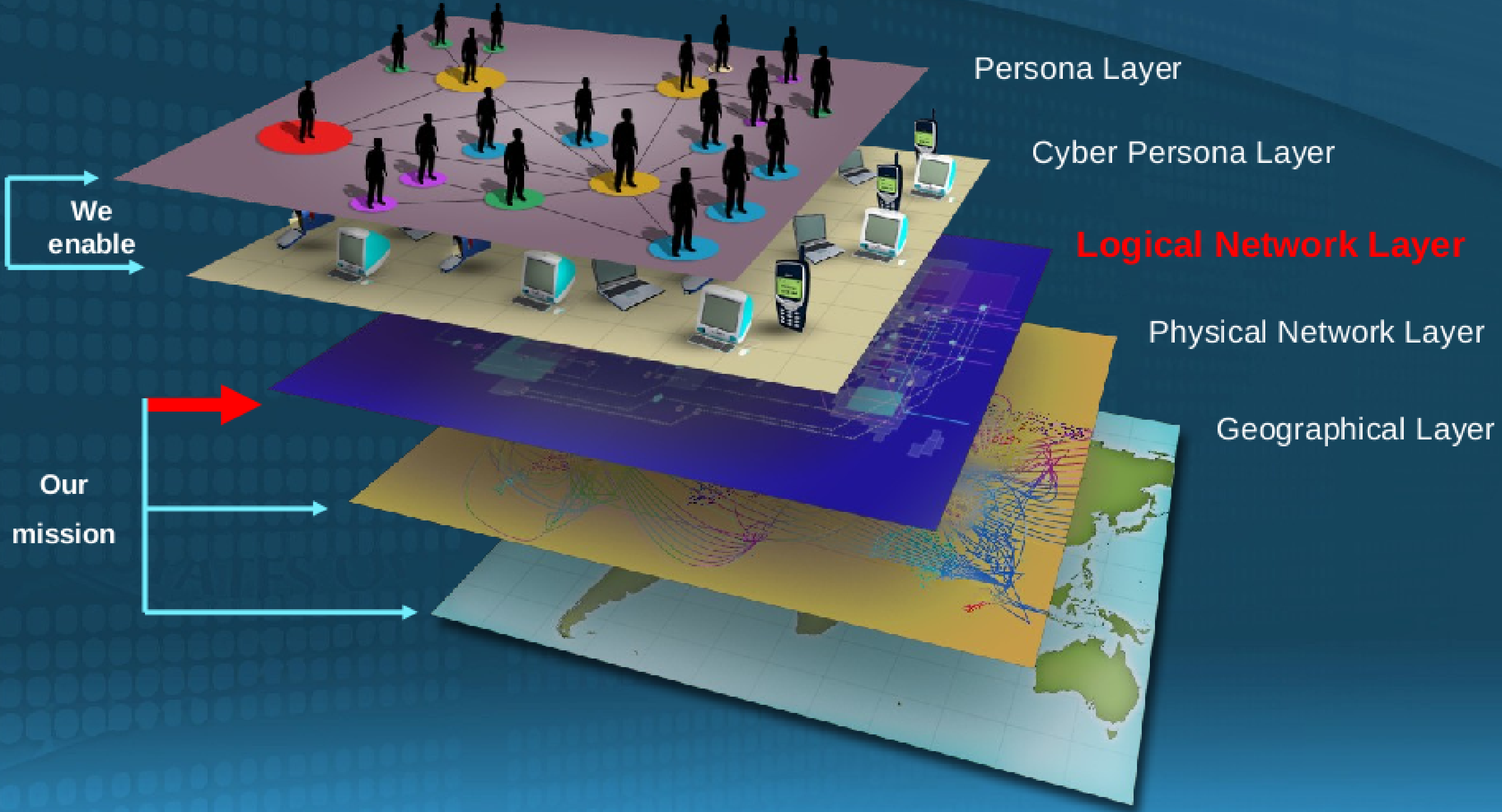
- Cyber Situational Awareness – *your own network plus adversaries'*
- Common Operation Pictures (COP)
- Computer Attack/Exploit Planning / Preparation of the Environment
- Network Reconnaissance
- Measures of Effectiveness (MOE)

(* 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)

TREASURE MAP

(U) Data Sources

Feed the Machine

(U) OSINT, Commercial & Academic

TREASURE MAP

- (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)
  - Commericaly 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

TREASURE MAP

- (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

TREASURE MAP

- (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!

TREASURE MAP

- (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: <u>~10 million</u> 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)

TREASURE MAP

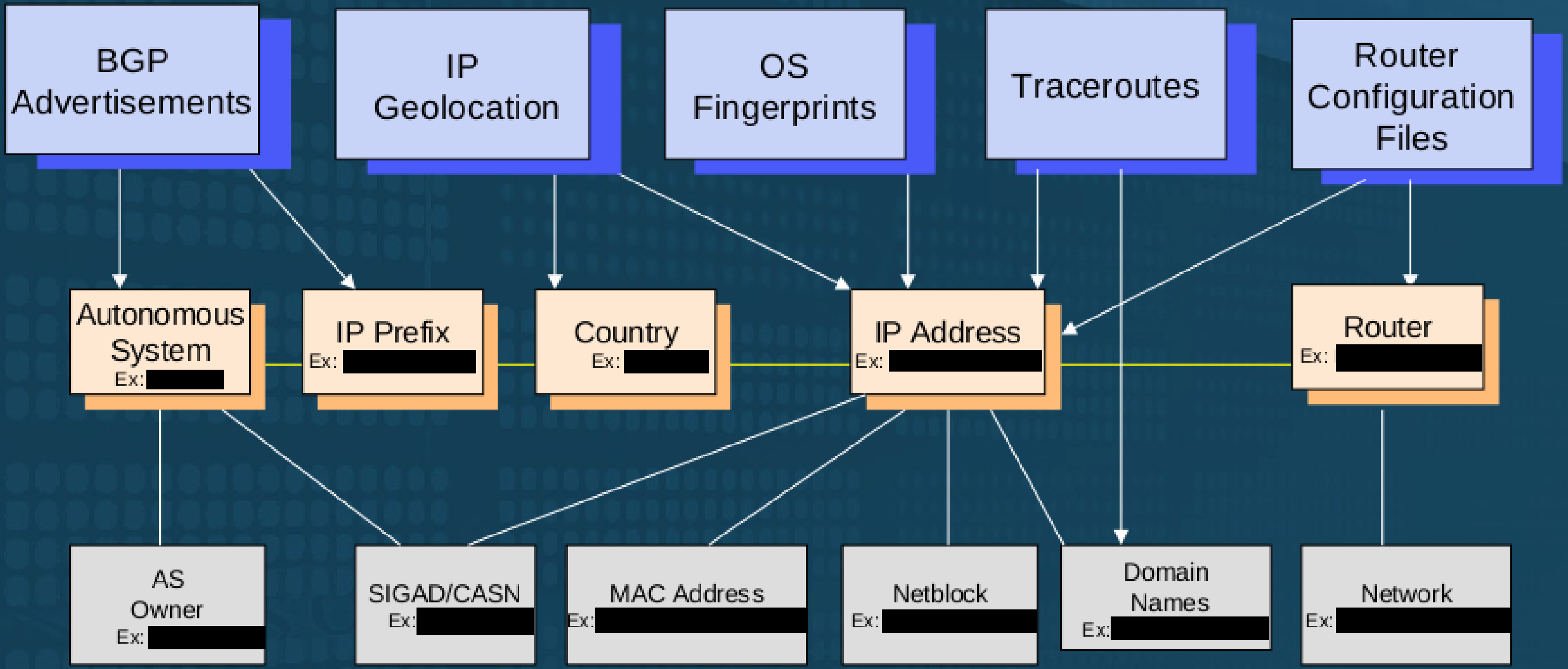
- (U//FOUO) PACKAGEDGOODS - NTOC
  - (S) Clandestine traceroute and DNS processor
- (S//SI//REL) BLACKPEARL – NAC
  - SIGINT session 5-tupel, identified routers, routing protocols, SIGINT access points, (inferred SIGINT access points)
- (S//SI//REL) LEAKYFAUCET – NAC
  - Flow repository of 802.11 WiFi 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 scaned 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-implanted 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

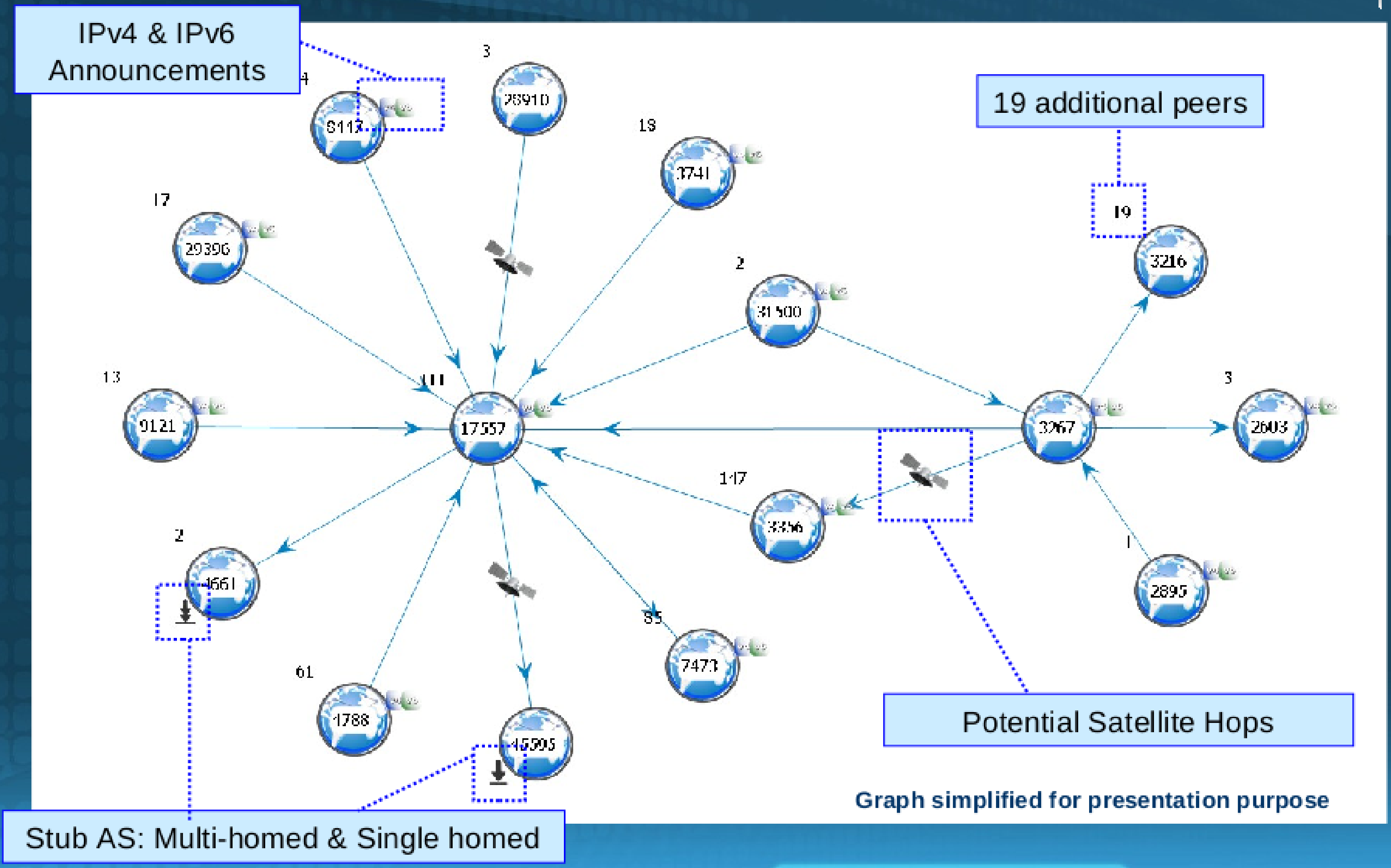
(U) Data Relationships



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



IPv4 & IPv6 Announcements

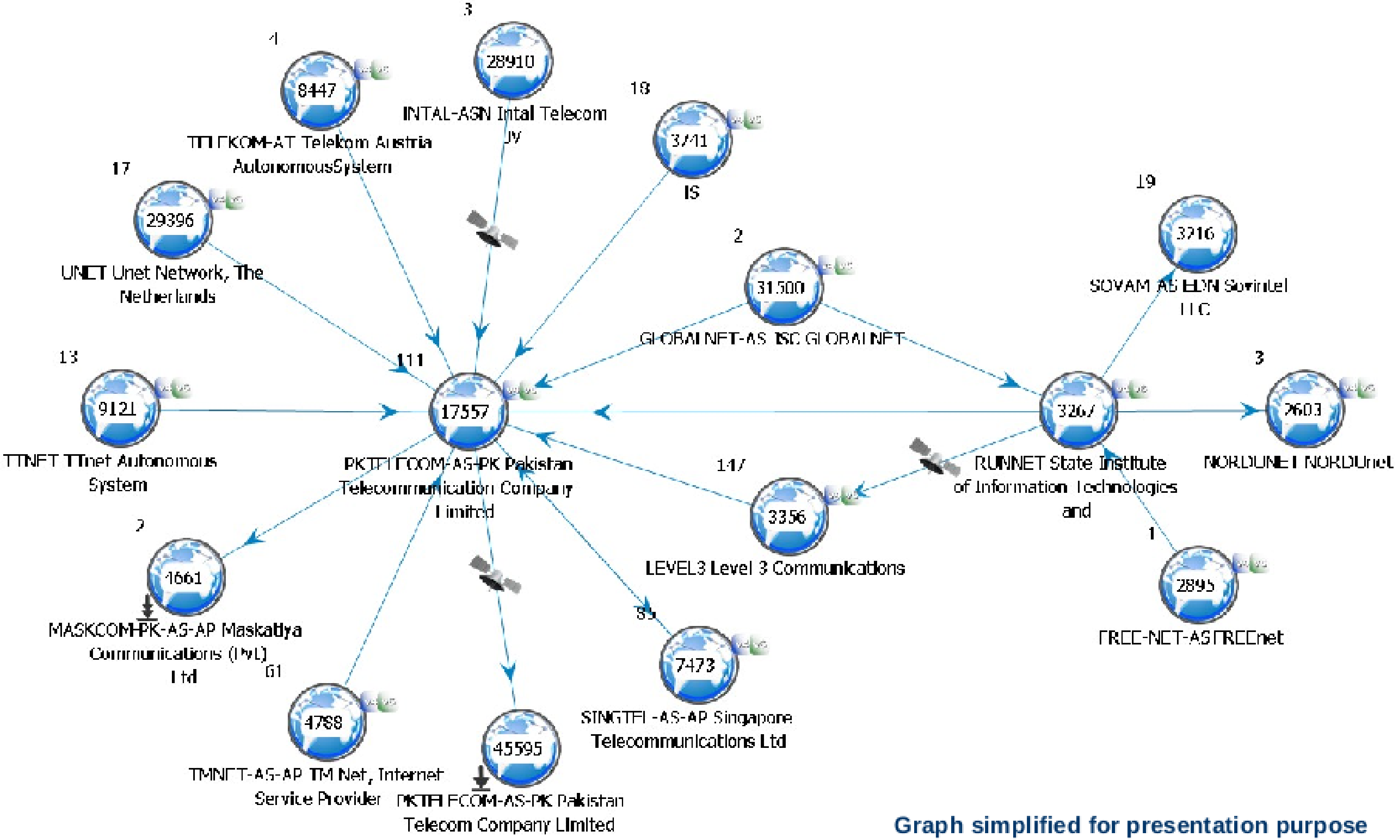
19 additional peers

Potential Satellite Hops

Stub AS: Multi-homed & Single homed

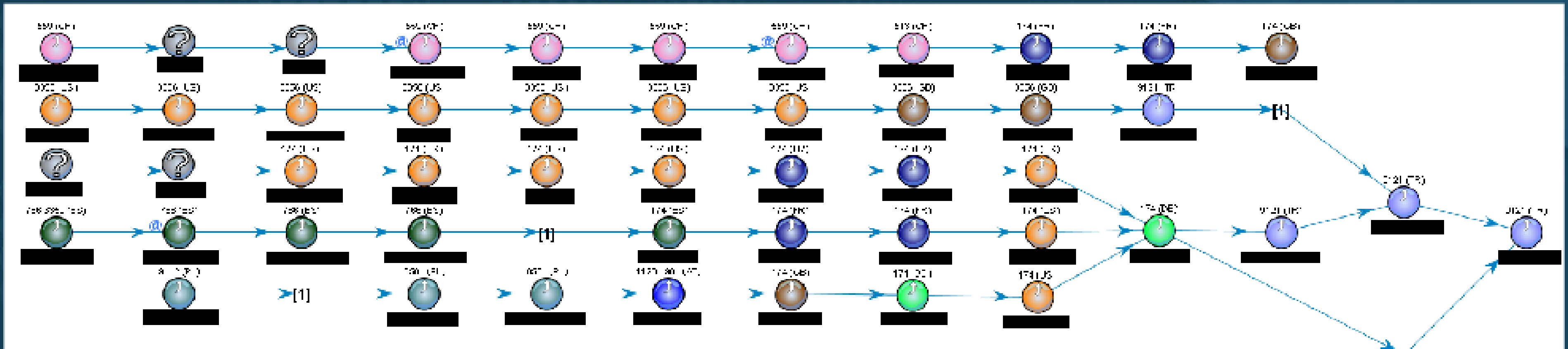
Graph simplified for presentation purpose

(U) … and Registries


3
28910
INTAL-ASN Intal Telecom JV
4
8447
TELEKOM-AT Telekom Austria AutonomousSystem
18
3741
IS
17
29396
UNET Unet Network, The Netherlands
2
31500
GLOBALNET-AS JSC GLOBALNET
19
3216
SOVAM-AS EDN Sovintel LLC
13
9121
TTNET TTnet Autonomous System
111
17557
PKTELECOM-AS-PK Pakistan Telecommunication Company Limited
3267
RUNNET State Institute of Information Technologies and
3
2603
NORDUNET NORDUnet
147
3356
LEVEL3 Level 3 Communications
1
2895
FREE-NET-AS FREEnet
2
4661
MASKCOM-PK-AS-AP Maskatiya Communications (Pvt) Ltd
61
4788
TMNET-AS-AP TM Net, Internet Service Provider
45595
PKTELECOM-AS-PK Pakistan Telecom Company Limited
85
7473
SINGTEL-AS-AP Singapore Telecommunications Ltd

Graph simplified for presentation purpose

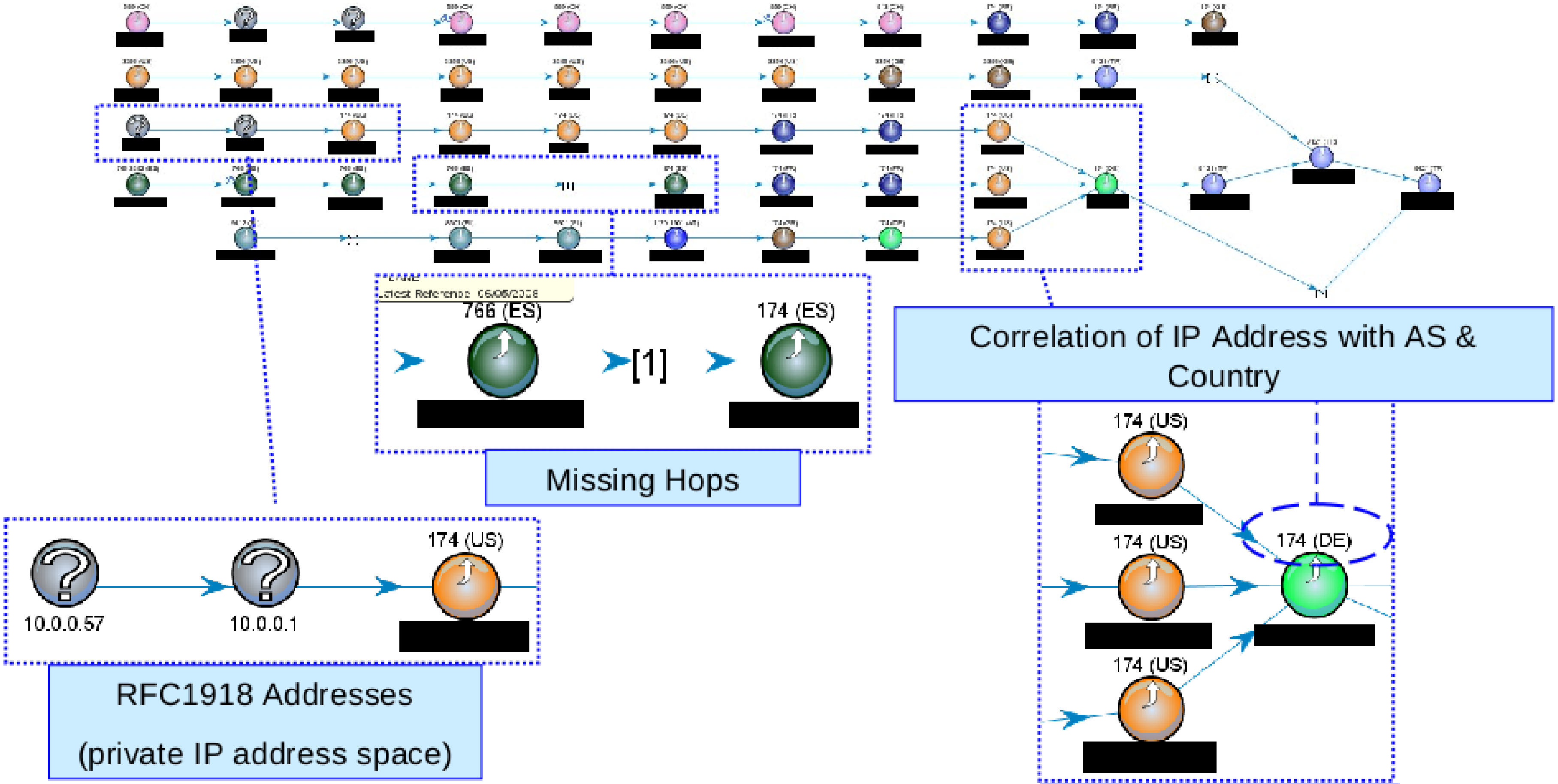
(U) Internet "flow" to a "Network"



Graph simplified for presentation purpose

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

(U) With Traceroute…



Missing Hops

Correlation of IP Address with AS & Country

RFC1918 Addresses

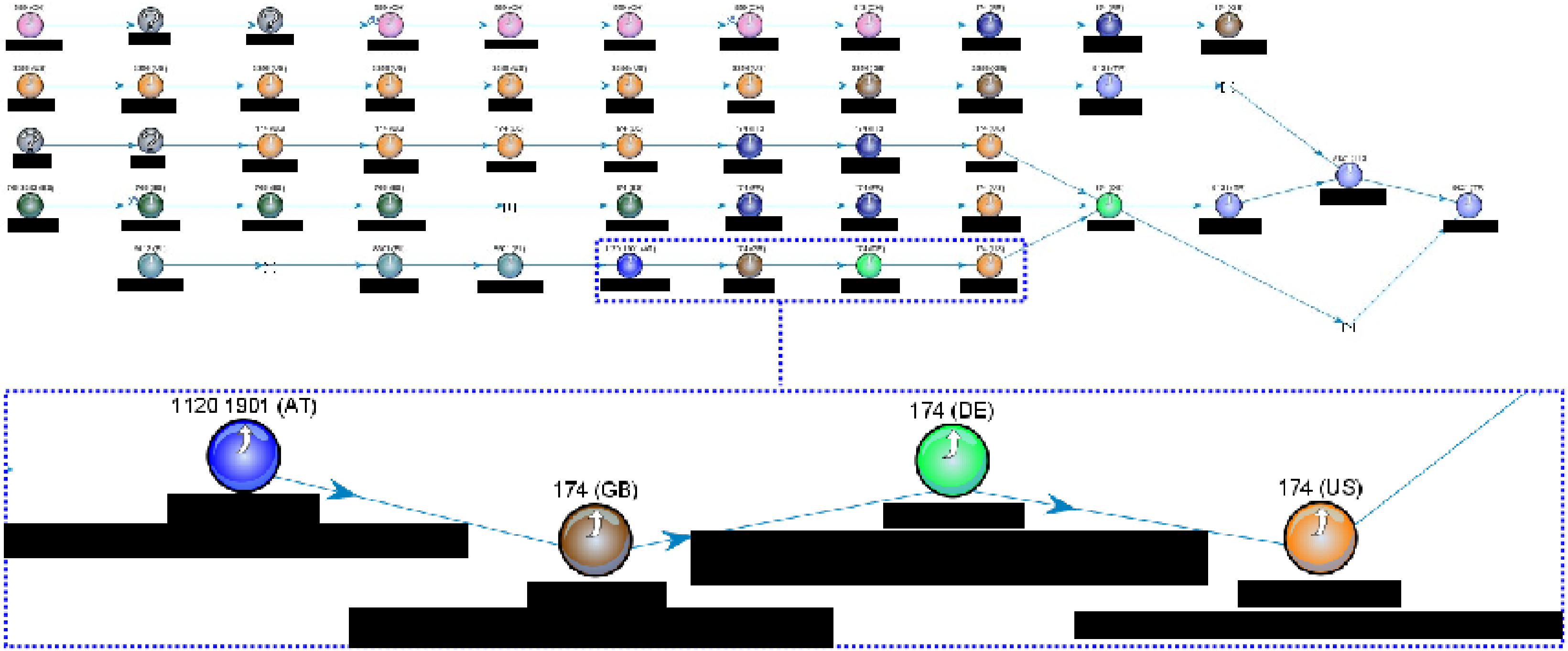
(private IP address space)

Network Bottlenecks

Graph simplified for presentation purpose

(U) … and DNS

TREASURE MAP

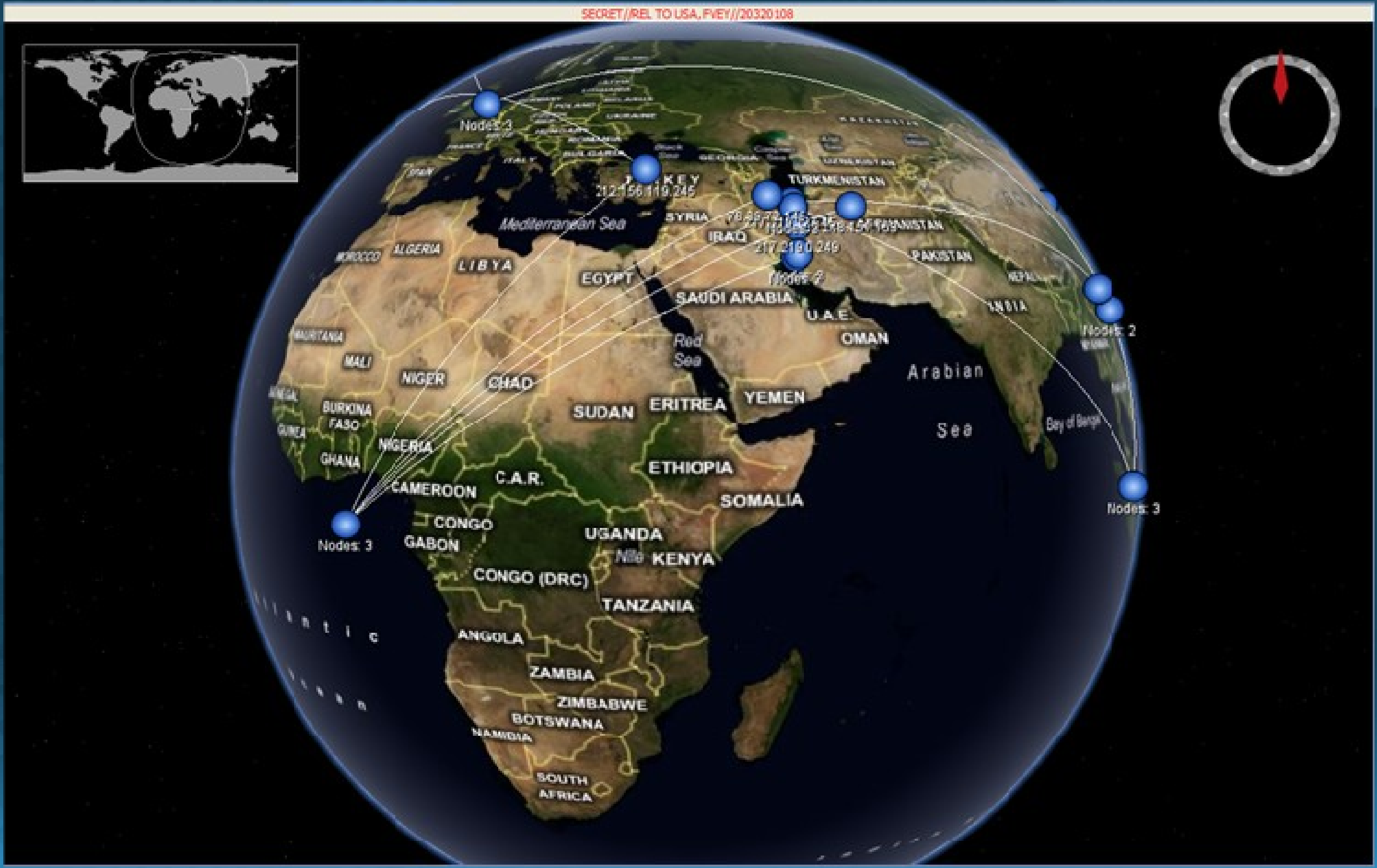


Graph simplified for presentation purpose

(U) IP Geolocation Data

TREASURE MAP

- Correlate IP addresses with country, latitude and longitude (via IPGeoTrap)



SECRET//REL TO USA, FVEY//20320108

(U) Seeing Red

SIGINT in the Water

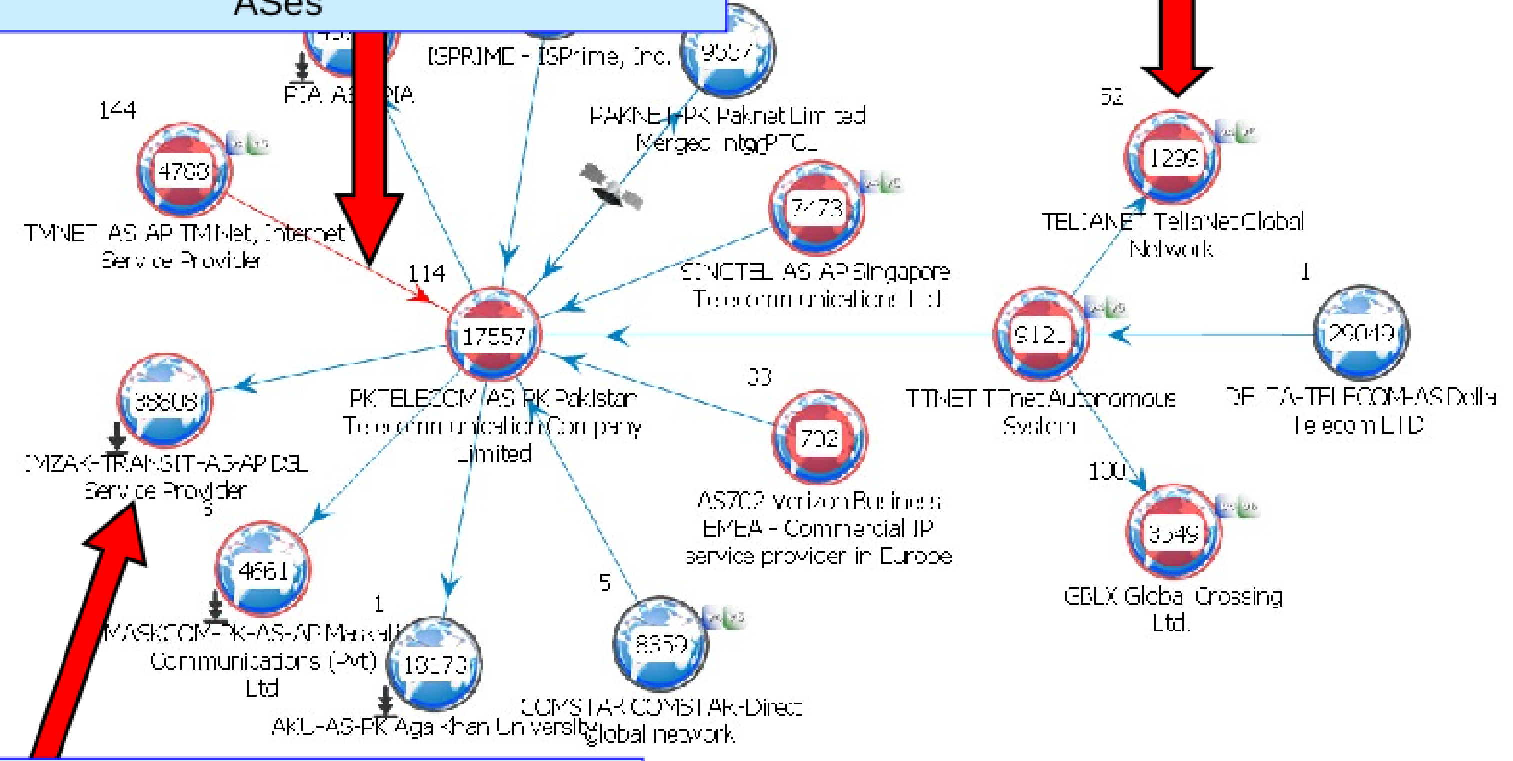
(S//SI//REL) Bring the SIGINT (AS Level)

Red Links:

SIGINT Collection access points between two ASes

Red Core Nodes:

SIGINT Collection access points within AS


PIA AS PIA
ISPRIME - ISPrime, Inc.
9557
PAKNET-PK Paknet Limited Merged into PTCL
144
4788
TMNET AS AP TM Net, Internet Service Provider
114
17557
PKTELECOM AS PK Pakistan Telecommunication Company Limited
7473
SINGTEL AS AP Singapore Telecommunications Ltd
33
702
AS702 Verizon Business EMEA - Commercial IP service provider in Europe
38608
IMZAK-TRANSIT-AS-AP DEL Service Provider
3
4661
MASKCOM-PK-AS-AP Markall Communications (Pvt) Ltd
1
18173
AKU-AS-PK Aga Khan University
5
8359
COMSTAR COMSTAR-Direct Global network
52
1299
TELIANET TeliaNet Global Network
9121
TTNET TTnet Autonomous System
1
29049
DELTA-TELECOM-AS Delta Telecom LTD
100
3549
GBLX Global Crossing Ltd.

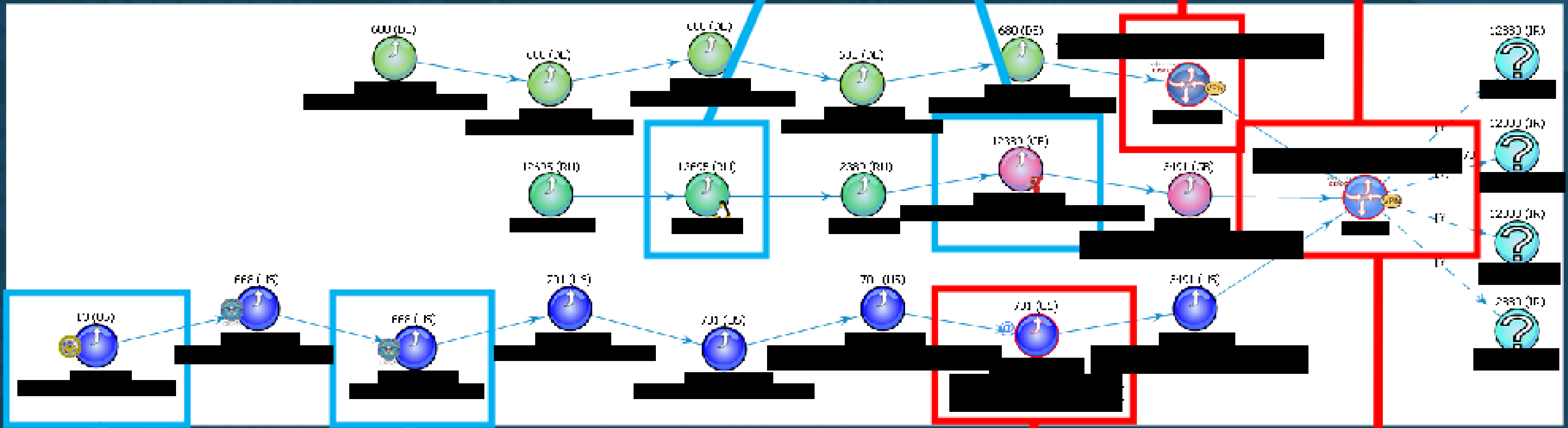
Red Ringed Node:

Nodes within AS are SIGINT Referenced

Graph simplified for presentation purpose

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

TREASURE MAP



[redacted]

TOYGRIPPE (VPN)

Router Configuration
Router Vendor:Cisco

OS Fingerprints

DoD Shields: DoD IP Addresses

Node Referenced in SIGINT

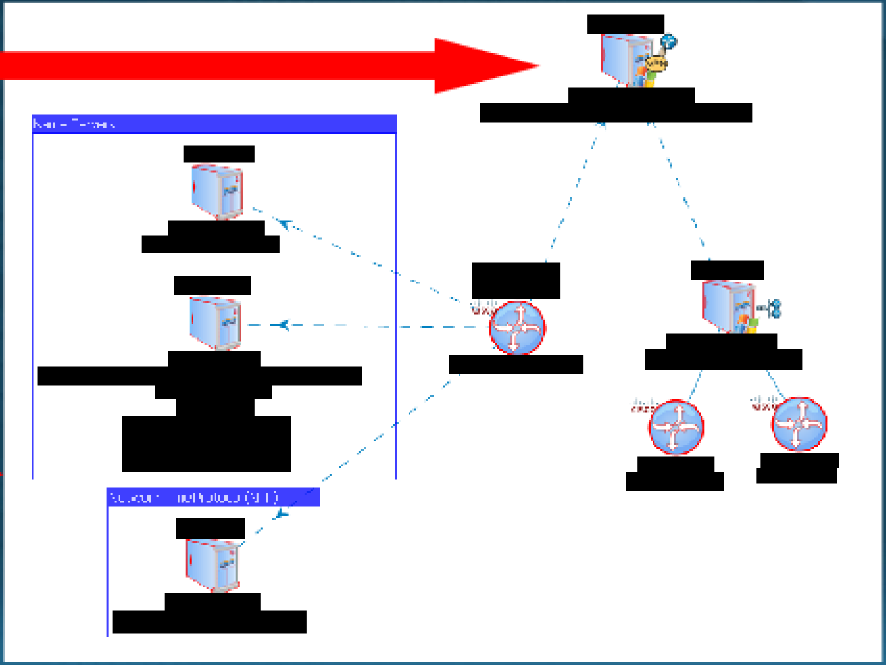
Underscore AS: “Operational” AS = 12880

(S//SI//REL) Known Devices

TREASURE MAP

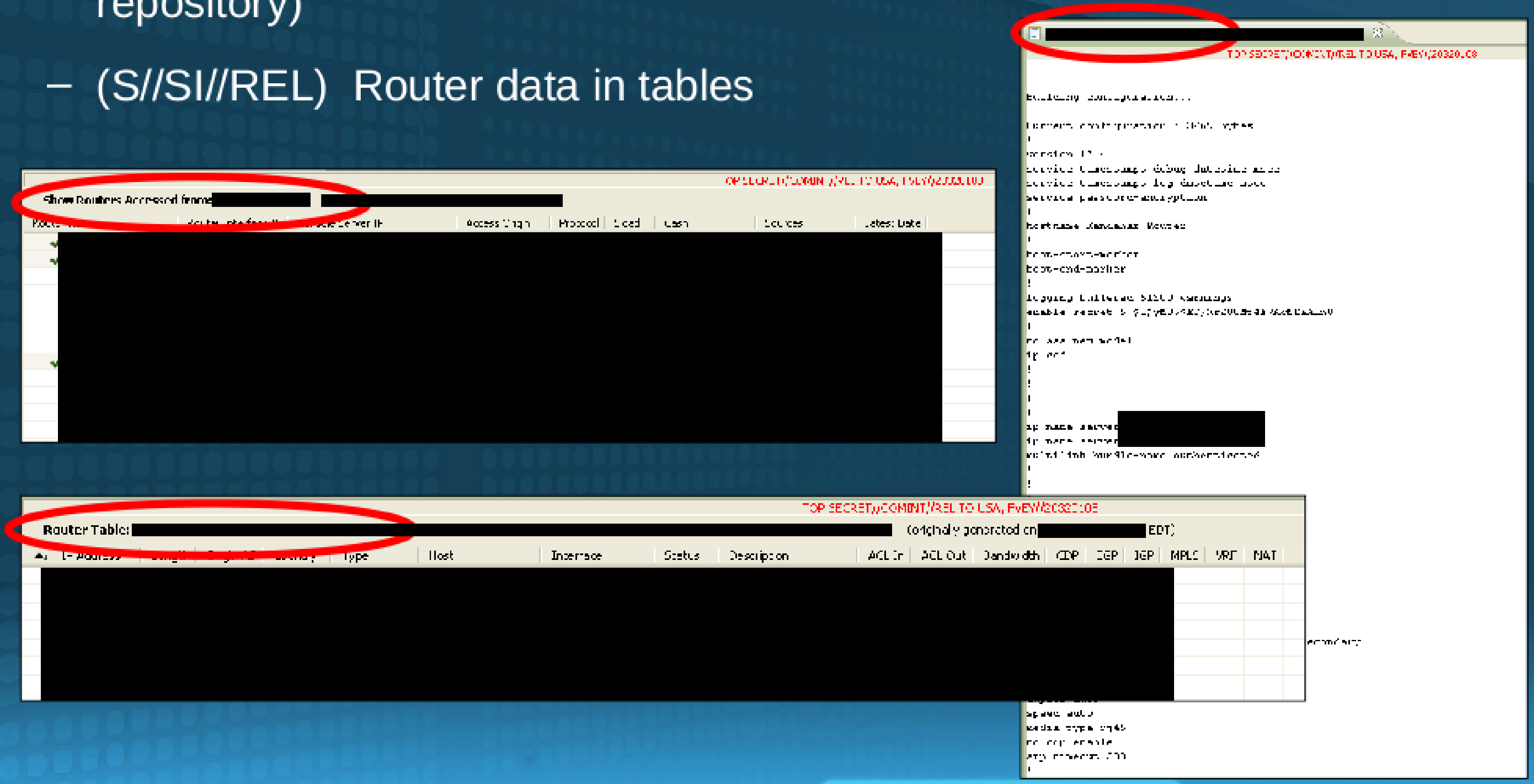
- (S//SI//REL) Sources: DISCOROUTE (NAC router configuration repository)

- (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) Known Devices

- (S//SI//REL) Sources: DISCOROUTE (NAC router configuration repository)
- (S//SI//REL) Router data in tables



TOP SECRET//COMINT//REL TO USA, FVEY//20320108

Show Routers Accessed from: [redacted] [redacted]

Router [illegible]	Router Interface	[illegible] Server IP	Access Origin	Protocol	Used	Hash	Sources	Latest Date
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

TOP SECRET//COMINT//REL TO USA, FVEY//20320108

Router Table: [redacted] (originally generated on [redacted] EDT)

IP Address	Length	[illegible]	[illegible]	Type	Host	Interface	Status	Description	ACL In	ACL Out	Bandwidth	CDP	EGP	IGP	MPLS	VRF	NAT
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		

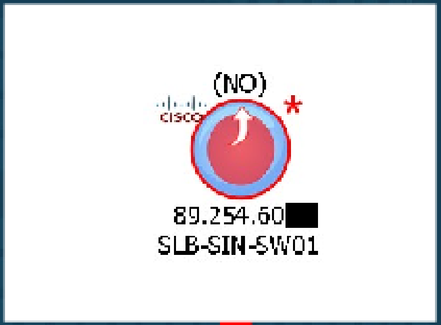
[redacted]

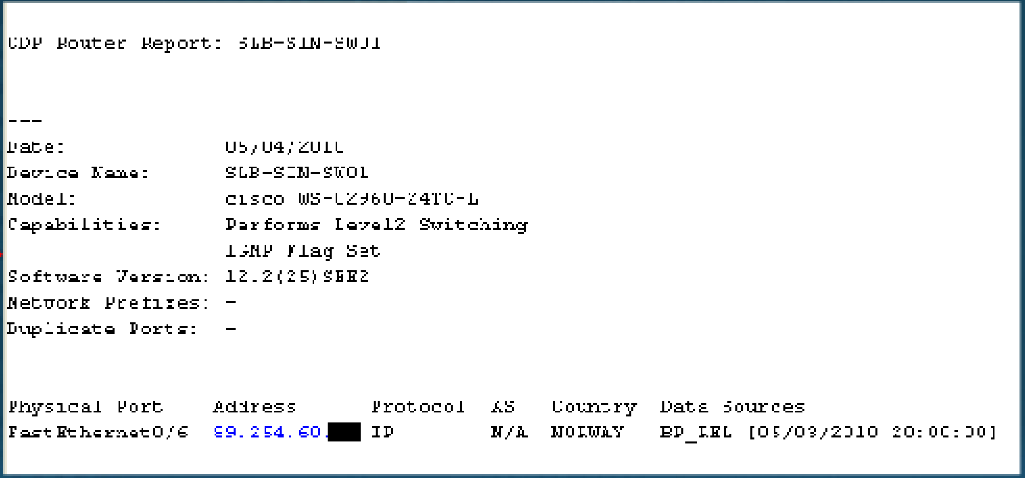
TOP SECRET//COMINT//REL TO USA, FVEY//20320108

```
Building configuration...

Current configuration : [illegible] bytes
!
version [illegible]
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname [illegible]
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
enable secret 5 [illegible]
!
no aaa new-model
ip cef
!
!
!
!
ip name-server [redacted]
ip name-server
[illegible]
!
!
[illegible]
speed auto
media-type rj45
no cdp enable
arp timeout [illegible]
!
```

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

TREASURE MAP



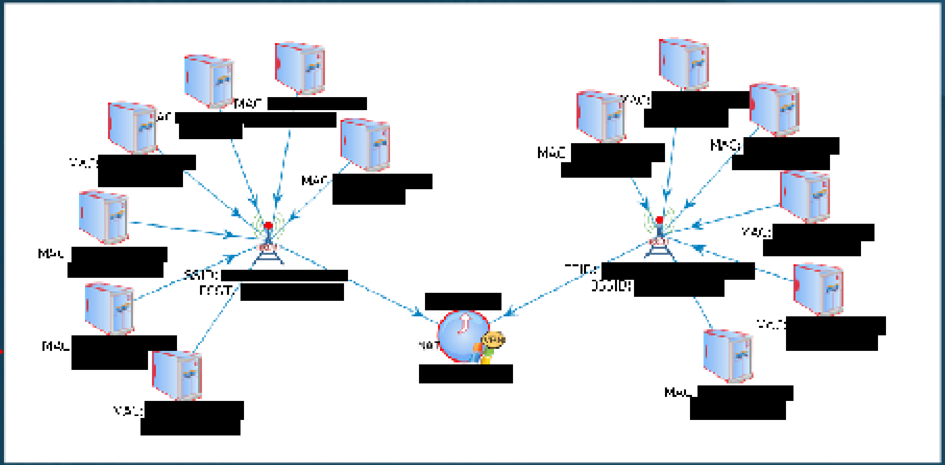


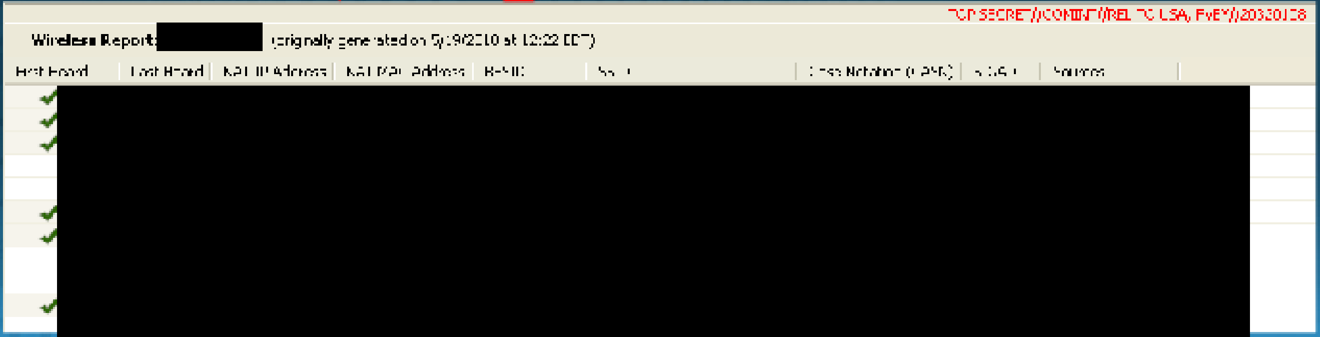
```
CDP Router Report: SLB-SIN-SW01


---
Date:               05/04/2010
Device Name:        SLB-SIN-SW01
Model:              cisco WS-C2960-24TC-L
Capabilities:       Performs Level2 Switching
                    IGMP 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.[redacted] IP     N/A   NORWAY    BP_REL [05/03/2010 20:00:00]
```

(U//FOUO) 802.11 WiFi Data

TREASURE MAP

- (U//FOUO) Display and correlation of 802.11 wireless networks and RFC1918 clients
- (S//SI//REL) Sources
  - HYDROCASTLE *
  - LEAKYFAUCET





TOP SECRET//COMINT//REL TO USA, FVEY//20320108

Wireless Report: [redacted] (originally generated on 5/19/2010 at 12:22 EDT)

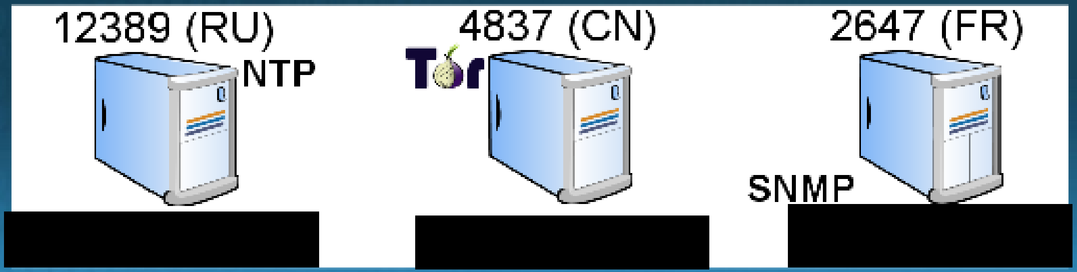
First Heard	Last Heard	NAT IP Address	NAT MAC Address	BSSID	SSID	Cross Notation (LANS)	SIGAD	Sources

[redacted]

(* HYDROCASTLE account required)

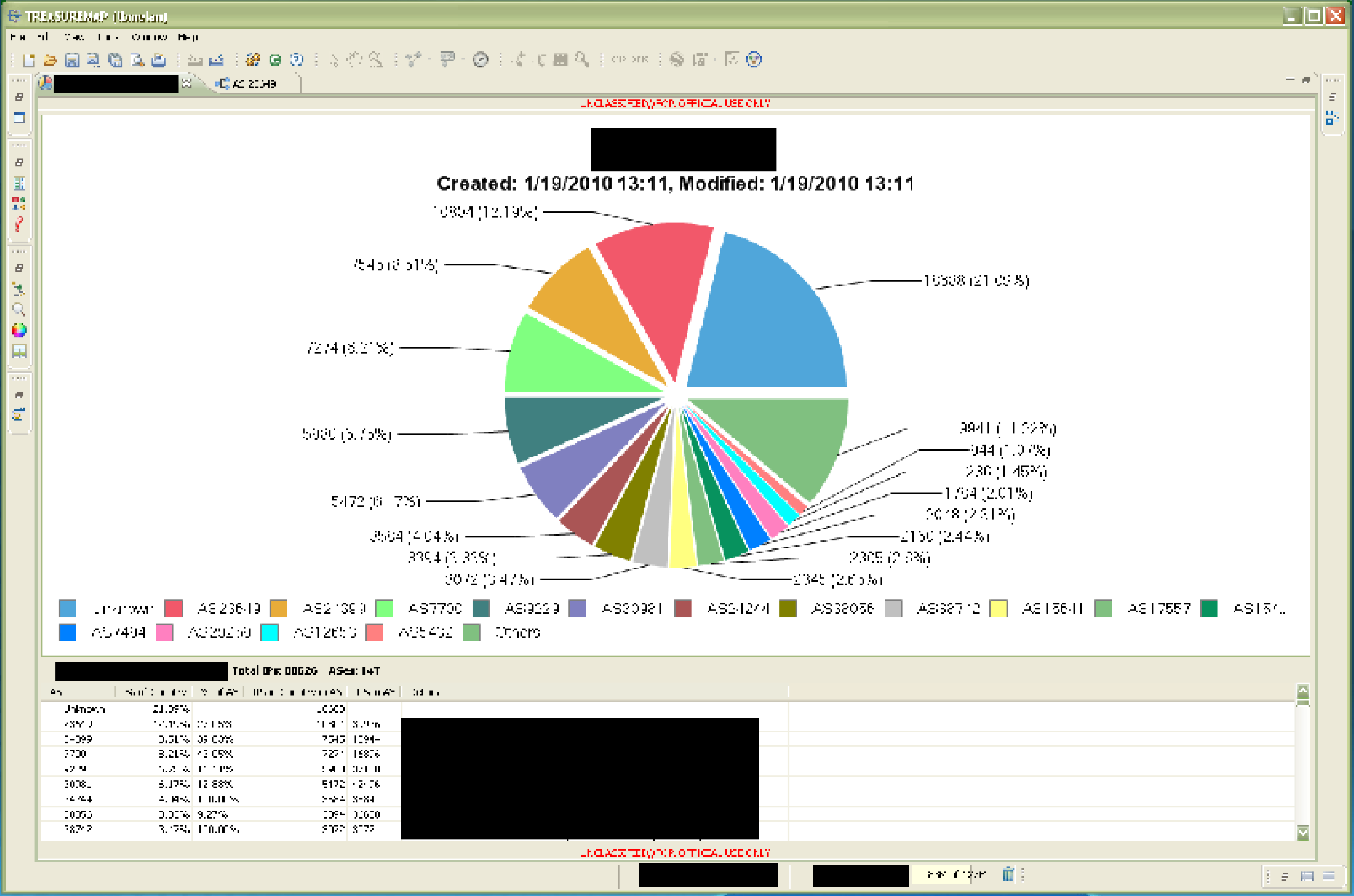
(U) Communities

- (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)

TREASURE MAP



UNCLASSIFIED//FOR OFFICIAL USE ONLY

[redacted]

Created: 1/19/2010 13:11, Modified: 1/19/2010 13:11

[redacted] Total IPs: 88626 ASes: 147

AS	[illegible]	% [illegible]	[illegible]	[illegible]	[illegible]
Unknown	21.09%		18538		
23619	12.19%	22.15%	10804	8.24%	[redacted]
21399	8.51%	39.03%	7545	10344	[redacted]
7700	8.21%	43.05%	7274	15876	[redacted]
9229	5.75%	[illegible]	5090	[illegible]	[redacted]
30981	6.17%	12.88%	5472	12476	[redacted]
24244	4.04%	[illegible]	3584	3584	[redacted]
38056	3.83%	9.27%	3394	33630	[redacted]
38712	3.47%	100.00%	3072	3072	[redacted]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

[redacted] [redacted]

TREASURE MAP

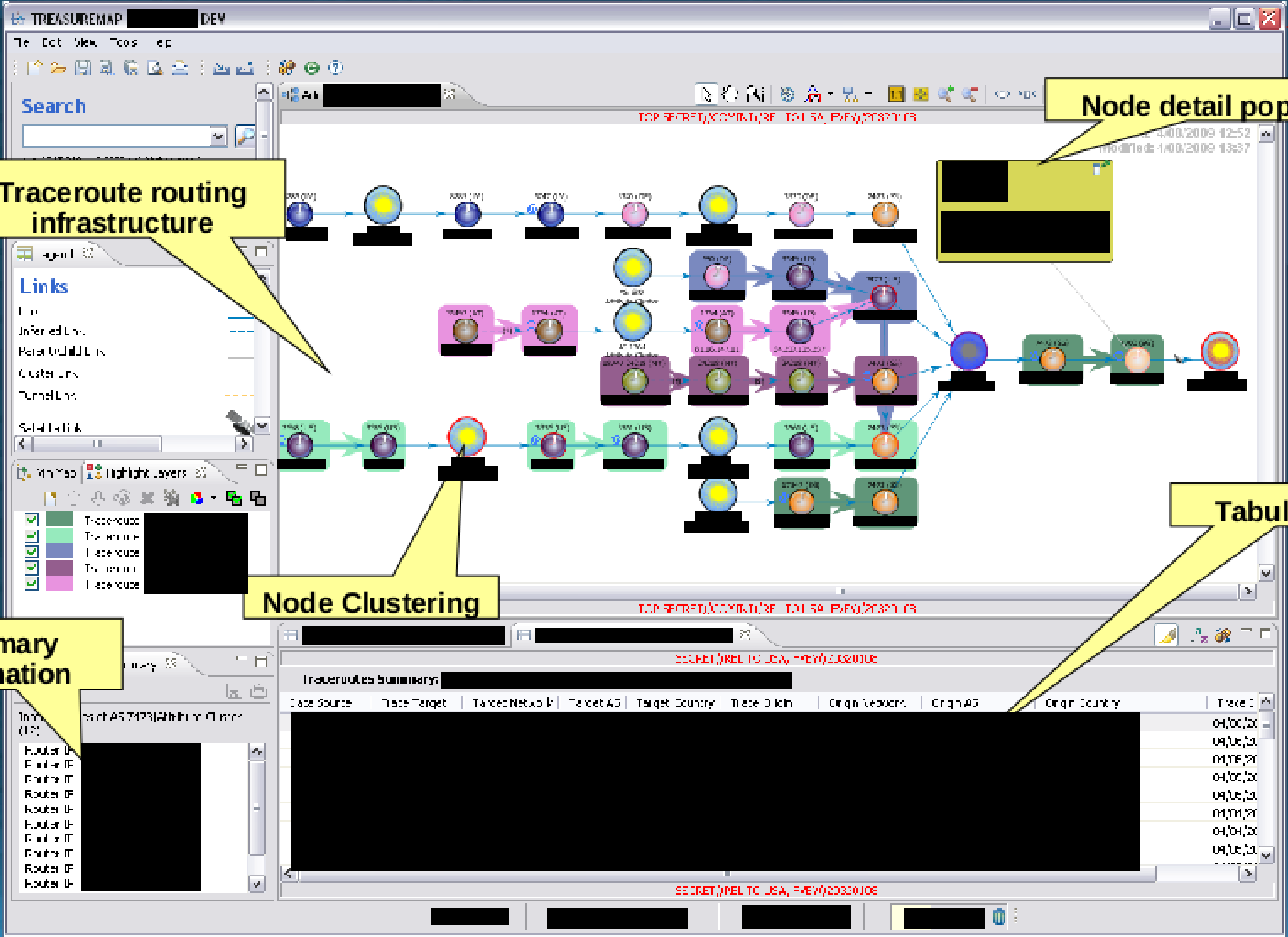
(U//FOUO) TREASUREMAP Workspace

- (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



Traceroutes Summary: [redacted]

Trace Source | Trace Target | Target Network | Target AS | Target Country | Trace Origin | Origin Network | Origin AS | Origin Country | Trace

[redacted]

SECRET//REL TO USA, FVEY//20320108

Node detail pop-ups

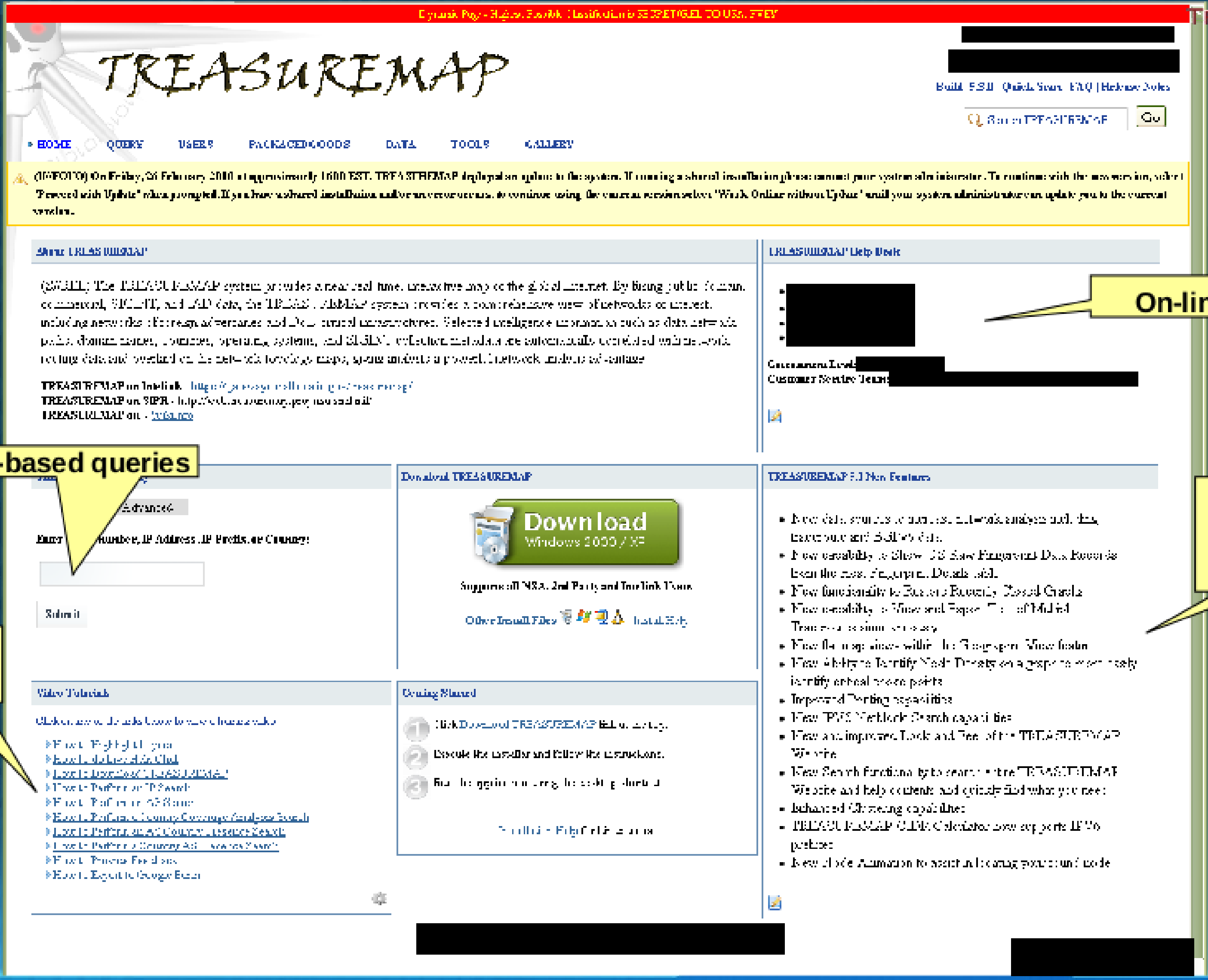
Traceroute routing infrastructure

Node Clustering

Tabular data

Summary Information

(UFOUO) User Interface: Website



Dynamic Page - Highest Possible Classification is SECRET//REL TO USA, FVEY

[redacted]

TREASUREMAP

Build [illegible] | Quick Start | FAQ | Release Notes

Search TREASUREMAP Go

HOME QUERY USERS PACKAGEDGOODS DATA TOOLS GALLERY

(U//FOUO) On Friday, 26 February 2010 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 an error occurs, to continue using the current version select 'Work Online without Update' until your system administrator can update you to the current version.

About TREASUREMAP

(S//REL) The TREASUREMAP system provides a near real-time, interactive map of the global internet. By fusing public domain, commercial, SIGINT, and LAN data, the TREASUREMAP system provides a comprehensive view of networks of interest, including networks of foreign adversaries and DoD critical infrastructures. Selected intelligence information such as data network paths, domain names, locations, operating systems, and SIGINT collection metadata are automatically correlated with the world routing data and overlaid on the network topology maps, giving analysts a powerful network analysis advantage.

TREASUREMAP on Intelink - https://[illegible]
TREASUREMAP on SIPR - http://[illegible]
TREASUREMAP on - [illegible]

TREASUREMAP Help Desk

[redacted]

Government Lead: [redacted]
Customer Service Team: [redacted]

On-line Help

Small text-based queries

Advanced

Enter [illegible] Number, IP Address, IP Prefix, or Country:

Submit

Download TREASUREMAP

Download Windows 2000 / XP

Supports all NSA, 2nd Party and [illegible] Users

Other Install Files Install Help

TREASUREMAP [illegible] New Features

- New data sources to increase network analysis including [illegible] and [illegible] data.
- New capability to Show [illegible] Raw Fingerprint Data Records from the new Fingerprint Details tab.
- New functionality to Restore Recently Closed Graphs
- New capability to View and Export [illegible] of Multiple Traceroutes simultaneously
- New filtering options within the Geographic View feature
- New Ability to Identify Node Density on a graph to more easily identify critical choke points
- Improved Printing capabilities
- New [illegible] Netblock 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 Clustering capabilities
- TREASUREMAP CIDR Calculator now supports IPv6 prefixes
- New Node Animation to assist in locating your found node

New Features Update

Video Tutorials

Click on any of the links below to view a tutorial video

- How to [illegible]
- How to [illegible]
- How to Download TREASUREMAP
- How to Perform an IP Search
- How to Perform an AS Search
- How to Perform a Country Coverage Analysis Search
- How to Perform an AS Country [illegible] Search
- How to Perform a Country AS [illegible] Search
- How to Process Feedback
- How to Export to Google Earth

Video Tutorials

Getting Started

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

[illegible] Help [illegible]

[redacted]

[redacted]

(U//FOUO) TREASUREMAP Contact Info

- [redacted]
  - Government Lead
  - [redacted]

- Customer Support Team
  - [redacted]

- Email: DL
  - [redacted]