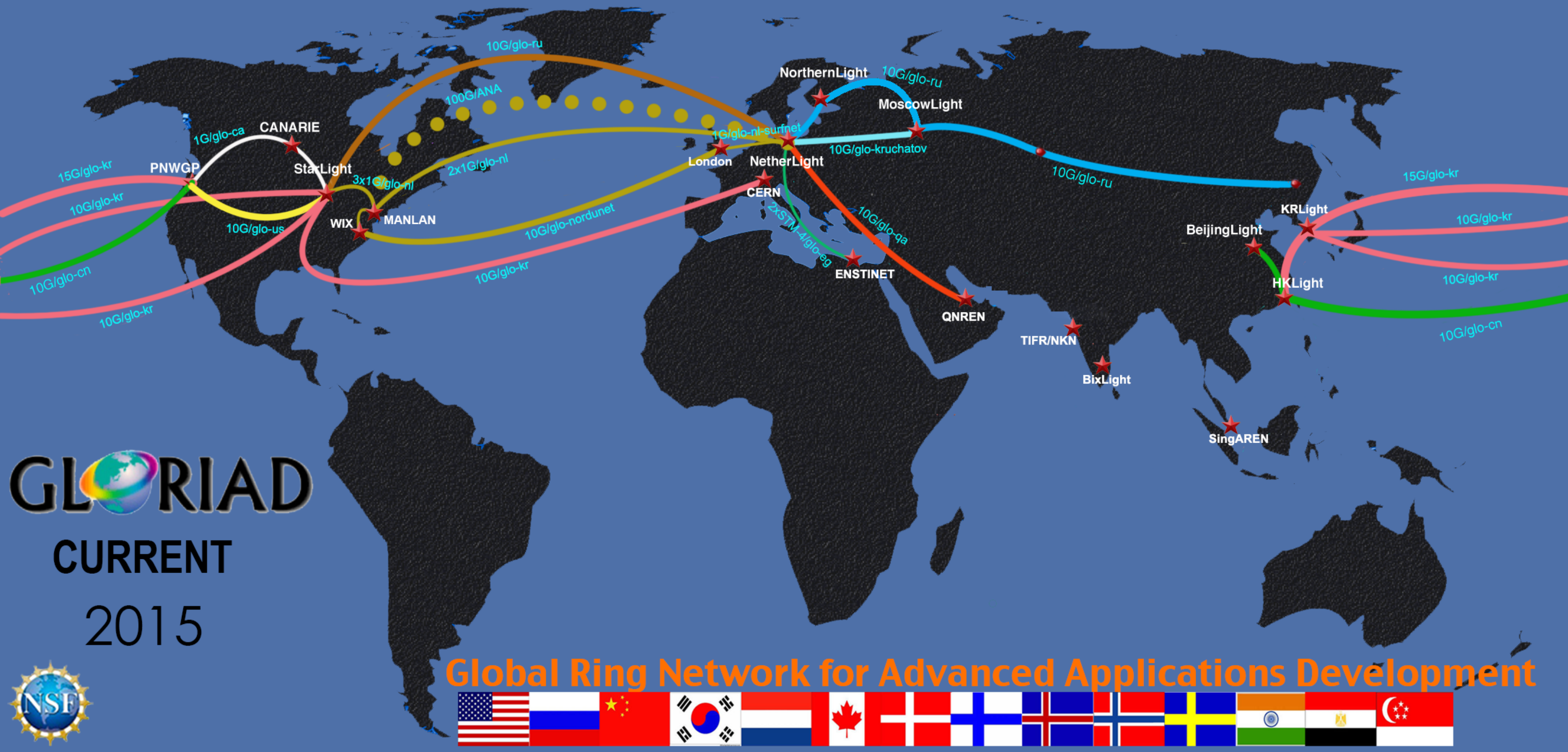
IRNC: AMI: GLORIAD/InSight

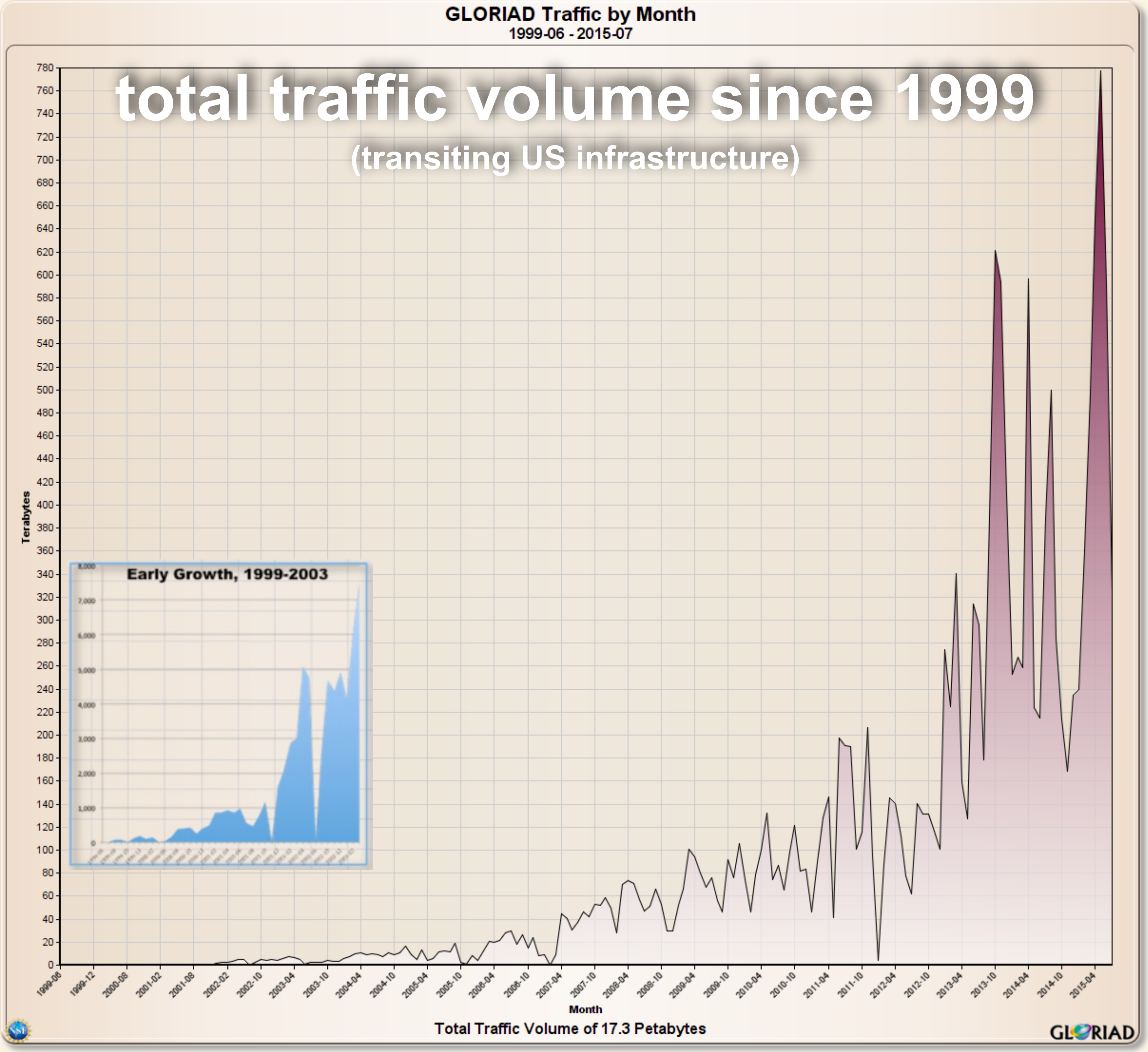
- (2 minute) GLORIAD Update
- New $1M NSF IRNC AMI award: The GLORIAD/InSight Advanced Performance Measurement System

The GLORIAD Science & Education Network

USA-RUSSIA-CHINA-KOREA-NETHERLANDS-CANADA-DENMARK-FINLAND-ICELAND-NORWAY-SWEDEN-INDIA-EGYPT-SINGAPORE



- Partners: Many!
- Sponsors: US NSF ($19.5M 1998-2015), Tata ($6M), USAID ($3.5M 2011-2013) all Intl partners (~$240M 1998-2015)
- History: (coming)



total traffic volume since 1999

(transiting US infrastructure)

2000 pages of such graphs

(2015 Annual Report to NSF)

http://www.gloriad.org/gloriad.annual.report.2015.pdfs.zip

GLORIAD History

- 1994 - Started “Friends & Partners” on-line community network
- 1995 - Started KORRnet and Russian Civic Networking Projects
- 1997 - Started MIRnet US-Russia high speed science network (6 Mbps!)
- 2001 - Moved to NCSA, University of Illinois
- 2002 - Upgraded MIRnet to 45 Mbps
- 2003 - Upgraded MIRnet to 155 Mbps
- 2004 - Added China/CSTnet! Launched “Little-GLORIAD” as first R&E network ring around the world (US-Russia-China - 155 Mbps)
- 2004 - Moved project back to ORNL/UT (JICS) with new 5-year NSF Funding
- 2005 - Added Korea (10G!), Netherlands (Europe exchange), Canada (and transit NA)
- 2006 - Added Nordic countries (re-established direct US-Nordic ties)
- 2009 - Started Taj project (Stimulus funds)
- 2010 - New 5 year NSF Funding
- 2011 - GLORIAD-Singapore Launched; New USAID Funding for GLORIAD in Africa
- 2011 - December - GLORIAD Egypt Launches
- 2012 - January - Hong Kong Workshop; June - GLORIAD India Launched
- 2012 - August - APAN - GLORIAD Agreement
- 2013 - October - Visits to UAE, Qatar and Malaysia
- 2014 - Visits to Kuwait, Oman; new 10G trans-atlantic link ready
- 2015 - 10G US-Russia links, New NSF Award for InSight Development, Visit to APAN 2015, MYREN

2015 Accomplishments (and Defeats)

2015 Accomplishments

- New 10G trans-A link (funded by NSF grant and primarily for US-Russia science) via Global Netwave/Level3
  - Establishment of the new network node in Amsterdam and direct connect to NetherLight at 10G
  - New 10 GE link to Russia (Runnet/E-ARENA) in partnership with Nordunet
  - New 10 GE link to Kurchatov Institute in Amsterdam (and layer2 circuits for KIAE for LHCONE to Internet2 and ESnet)
  - Several new peerings there including QNREN, Nordunet, Runnet, Egypt, etc
- New Qatar/QNren partners (and 10G connect to Netherlight)
- New partnership with PacWave/CENIC (also hosting GLORIAD in Seattle)
- New KISTI capacity (and to CERN)

2015 Accomplishments

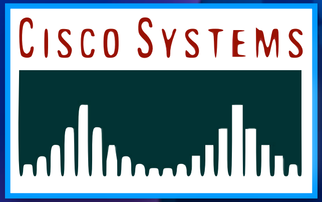
- InSight system now in production (+ new $1M Cisco-provided computational facility) Updated PerfSONAR infrastructure to 10 G
- Upgraded Knoxville-Chicago connectivity to 100G (Univ of TN and SoX-SLR)
- New CSTnet equipment and capability in US
- Redesign of backup core connectivity and switch from GE over SONET infrastructure to 100GE infrastructure
- Deployment of new BGPmon infrastructure/monitoring (+ hardening of BGP and correlation between BGP data and flow-based data)
- New backup capabilities with CANARIE and via ANA links

2015 Infrastructure

Thank you!

- CENIC/PNWG for hosting us at Seattle and providing primary path between Chicago and Seattle, and help with backup path as well,
- StarLight for hosting us and build of backup infrastructure,
- Thomas Tam, Damir Pobric and CANARIE for work on our backup circuits,
- Gerben van Malenstein, Surfnet/NetherLight, CANARIE and Internet2 for backup path between Chicago and Amsterdam,
- QNREN for the new partnership,
- Alin Pastrama and NORDUNET for help with the new Russia circuits,
- Runnet, E-Arena and KIAE for new era of connectivity to Amsterdam and on to US,
- GlobalNetwave/Level3 for primary circuit Chicago-Amsterdam,
- Vancis for Amsterdam node setup,
- CSTnet, KISTI/Kreonet, Kurchatov Institute, RUNNet, SURFnet, NORDUnet, ENSTInet/EUnet, SingAREN, MyREN, and all other peer networks for continuous support and cooperation

Thanks to some special Sponsors



QoSient, LLC

2015 News

- Current ProNET GLORIAD award no-cost time-extended through April, 2016
- $1M New NSF award for InSight Development made under IRNC program
- GLORIAD Foundation/RFC process

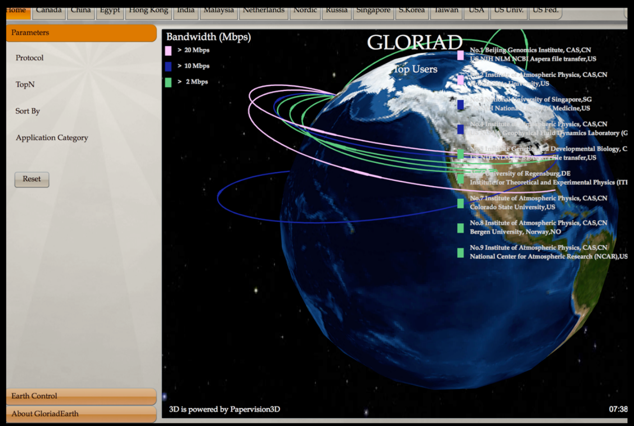
InSight Award

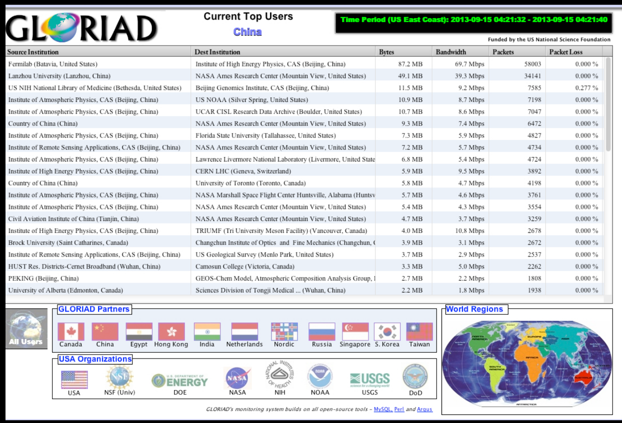
- New NSF Grant: 8/1/2015 - 1/31/2018: Open-Sourcing and Further Development of GLORIAD/InSight
  - Improving Performance Measurement
  - Crowd-Sourcing Cybersecurity
  - Young people Involvement

GLORIAD

Measurement and Monitoring System

or how do we get (meaningful/useful/actionable information) from ...





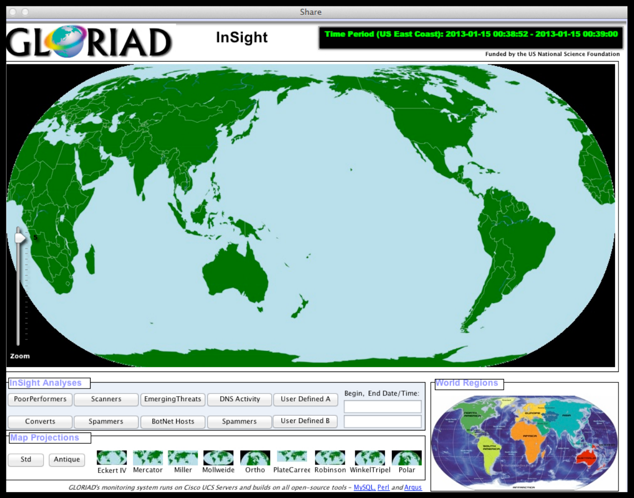
GLORIAD **Current Top Users** China

Time Period (US East Coast): 2013-09-15 04:21:32 - 2013-09-15 04:21:40

Funded by the US National Science Foundation

Source Institution	Dest Institution	Bytes	Bandwidth	Packets	Packet Loss
Fermilab (Batavia, United States)	Institute of High Energy Physics, CAS (Beijing, China)	87.2 MB	69.7 Mbps	58003	0.000 %
Lanzhou University (Lanzhou, China)	NASA Ames Research Center (Mountain View, United States)	49.1 MB	39.3 Mbps	34141	0.000 %
US NIH National Library of Medicine (Bethesda, United States)	Beijing Genomics Institute, CAS (Beijing, China)	11.5 MB	9.2 Mbps	7585	0.277 %
Institute of Atmospheric Physics, CAS (Beijing, China)	US NOAA (Silver Spring, United States)	10.9 MB	8.7 Mbps	7198	0.000 %
Institute of Atmospheric Physics, CAS (Beijing, China)	UCAR CISL Research Data Archive (Boulder, United States)	10.7 MB	8.6 Mbps	7047	0.000 %
Country of China (China)	NASA Ames Research Center (Mountain View, United States)	9.3 MB	7.4 Mbps	6472	0.000 %
Institute of Atmospheric Physics, CAS (Beijing, China)	Florida State University (Tallahassee, United States)	7.3 MB	5.9 Mbps	4827	0.000 %
Institute of Remote Sensing Applications, CAS (Beijing, China)	NASA Ames Research Center (Mountain View, United States)	7.2 MB	5.7 Mbps	4734	0.000 %
Institute of Atmospheric Physics, CAS (Beijing, China)	Lawrence Livermore National Laboratory (Livermore, United State	6.8 MB	5.4 Mbps	4724	0.000 %
Institute of High Energy Physics, CAS (Beijing, China)	CERN LHC (Geneva, Switzerland)	5.9 MB	9.5 Mbps	3892	0.000 %
Country of China (China)	University of Toronto (Toronto, Canada)	5.8 MB	4.7 Mbps	4198	0.000 %
Institute of Atmospheric Physics, CAS (Beijing, China)	NASA Marshall Space Flight Center Huntsville, Alabama (Huntsv	5.7 MB	4.6 Mbps	3761	0.000 %
Institute of Atmospheric Physics, CAS (Beijing, China)	NASA Ames Research Center (Mountain View, United States)	5.4 MB	4.3 Mbps	3554	0.000 %
Civil Aviation Institute of China (Tianjin, China)	NASA Ames Research Center (Mountain View, United States)	4.7 MB	3.7 Mbps	3259	0.000 %
Institute of High Energy Physics, CAS (Beijing, China)	TRIUMF (Tri University Meson Facility) (Vancouver, Canada)	4.0 MB	10.8 Mbps	2678	0.000 %
Brock University (Saint Catharines, Canada)	Changchun Institute of Optics and Fine Mechanics (Changchun, (	3.9 MB	3.1 Mbps	2672	0.000 %
Institute of Remote Sensing Applications, CAS (Beijing, China)	US Geological Survey (Menlo Park, United States)	3.7 MB	2.9 Mbps	2537	0.000 %
HUST Res. Districts-Cernet Broadband (Wuhan, China)	Camosun College (Victoria, Canada)	3.3 MB	5.0 Mbps	2262	0.000 %
PEKING (Beijing, China)	GEOS-Chem Model, Atmospheric Composition Analysis Group, I	2.7 MB	2.2 Mbps	1808	0.000 %
University of Alberta (Edmonton, Canada)	Sciences Division of Tongji Medical ... (Wuhan, China)	2.2 MB	1.8 Mbps	1938	0.000 %

GLORIAD's monitoring system builds on all open-source tools - MySQL, Perl and Argus

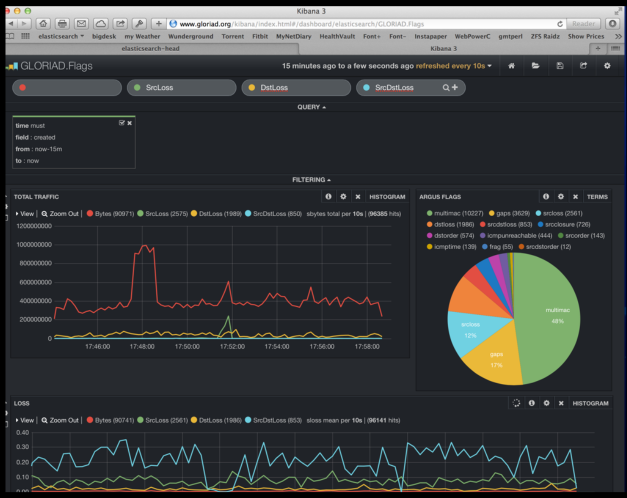


GLORIAD InSight

Time Period (US East Coast): 2013-01-15 00:38:52 - 2013-01-15 00:39:00

Funded by the US National Science Foundation

GLORIAD's monitoring system runs on Cisco UCS Servers and builds on all open-source tools - MySQL, Perl and Argus



Kibana 3

www.gloriad.org/kibana/index.html#/dashboard/elasticsearch/GLORIAD.Flags

GLORIAD.Flags — 15 minutes ago to a few seconds ago refreshed every 10s

time must
field : created
from : now-15m
to : now

for sustaining and operating global advanced research & education networks

August 1, 2015: New NSF Funding ($1M / 2.5 years)

Abstract: The GLORIAD/InSight program is a global, open-source software development effort to research and experimentally deploy advanced flow-level network measurement technologies at various levels of the research and education (R&E) network eco-system. The tools developed will enable far-reaching research towards better understanding network utilization, identifying network application performance issues while carefully attending to differing community concerns and requirements regarding data privacy and security. Experimental deployments will showcase actionable analytics and visualizations for network operations, new methods and models of data sharing across the global R&E fabric, and thus a better understood, more performant fabric.

Through a global, community-focused, open-source development effort, the project extends the current beta version of InSight - the flow-level passive measurement, analysis and visualization system in use on the GLORIAD network. The InSight tools are based on passive network measurement and monitoring by combining the rich detail of comprehensive, non-sampled, bi-directional, multi-model, multi-layer Argus flow-data with modern big-data analytic and visualization tools. A flexible stream-based method of enriching network flow metadata enables broader, customer-defined analytics. Working closely with interested large-network providers, the project works toward experimentally deploying InSight on links up to 100 Gbps.

August 1, 2015: New NSF Funding ($1M / 2.5 years)

Abstract: The GLORIAD/InSight program is a global, open-source software development effort to research and experimentally deploy advanced flow-level network measurement technologies at various levels of the research and education (R&E) network eco-system. The tools developed will enable far-reaching research towards better understanding network utilization, identifying network application performance issues while carefully attending to differing community concerns and requirements regarding data privacy and security. Experimental deployments will showcase actionable analytics and visualizations for network operations, new methods and models of data sharing across the global R&E fabric, and thus a better understood, more performant fabric.

Through a global, community-focused, open-source development effort, the project extends the current beta version of InSight - the flow-level passive measurement, analysis and visualization system in use on the GLORIAD network. The InSight tools are based on passive network measurement and monitoring by combining the rich detail of comprehensive, non-sampled, bi-directional, multi-model, multi-layer Argus flow-data with modern big-data analytic and visualization tools. A flexible stream-based method of enriching network flow metadata enables broader, customer-defined analytics. Working closely with interested large-network providers, the project works toward experimentally deploying InSight on links up to 100 Gbps.

Demo

Leadership Team

- Carter Bullard, Qotient
- Joe Gipson, Cisco
- Buseung Cho, KISTI
- Nan Kai, CSTnet

Summary

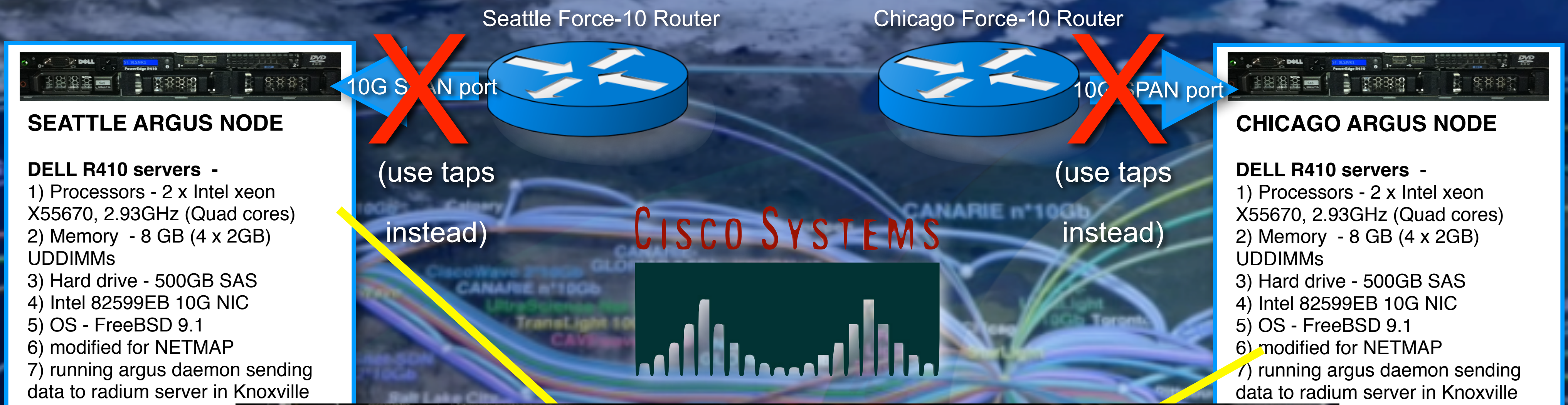
- Work builds on efforts since 1999
- Argus has offered us a huge number of advantages over our previous (netflow, sflow, packeteer, etc.) technologies (and we're still beginners with it) (btw, Argus also reads netflow data so we're working on new version to directly support netflow)
- Resulting information products provide near real-time update on live flows (for troubleshooting and shining light on good uses of R&E networks)
- Data management problem (500 million flow records/day) is difficult but solvable
- Everything builds on top of Global Science Registry
- We will encourage an open global, community effort to deploy common standards and tools addressing metrics for R&E network performance, operations and security
- Ultimate goal is distributed virtual network operations center (dvNOC)

Technical Weeds

Underlying Open-Source Technologies

- Argus (and other flow data sources)
- Elasticsearch (scalable, extremely fast indexing/search/discovery tool)
- ZeroMQ (for local and global messaging fabric)
- MySQL and SQLite for metadata
- Event-loopy Perl/POE, Python, Ruby, Go, C/++ for “farm animals”

Near-future GLORIAD-US Deployment of Argus



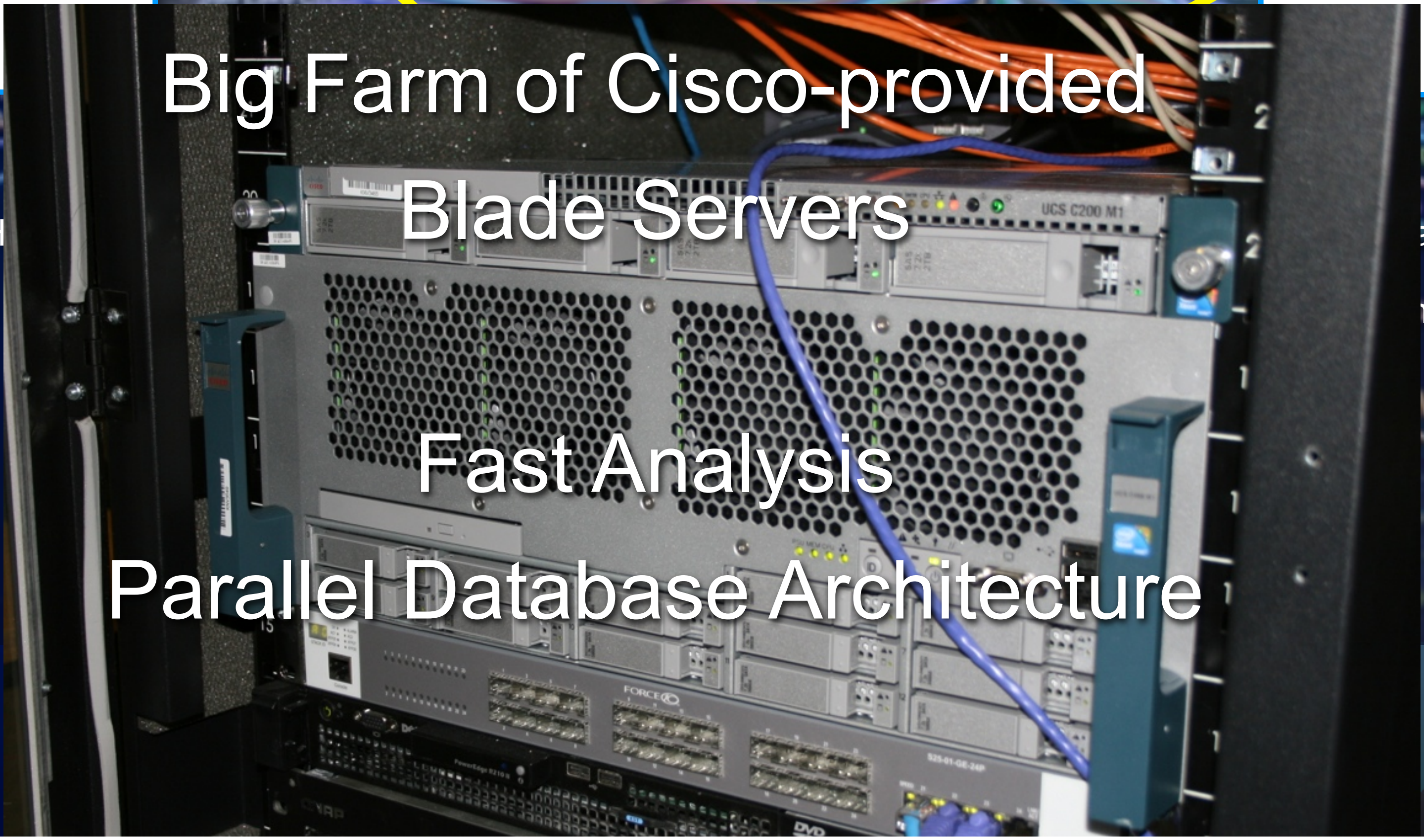
SEATTLE ARGUS NODE

DELL R410 servers -
1) Processors - 2 x Intel xeon X55670, 2.93GHz (Quad cores)
2) Memory - 8 GB (4 x 2GB) UDDIMMs
3) Hard drive - 500GB SAS
4) Intel 82599EB 10G NIC
5) OS - FreeBSD 9.1
6) modified for NETMAP
7) running argus daemon sending data to radium server in Knoxville

CHICAGO ARGUS NODE

DELL R410 servers -
1) Processors - 2 x Intel xeon X55670, 2.93GHz (Quad cores)
2) Memory - 8 GB (4 x 2GB) UDDIMMs
3) Hard drive - 500GB SAS
4) Intel 82599EB 10G NIC
5) OS - FreeBSD 9.1
6) modified for NETMAP
7) running argus daemon sending data to radium server in Knoxville

- Local Storage
- Local Analysis H ardware
- Ability to handle much more capacity



Big Farm of Cisco-provided Blade Servers

Fast Analysis

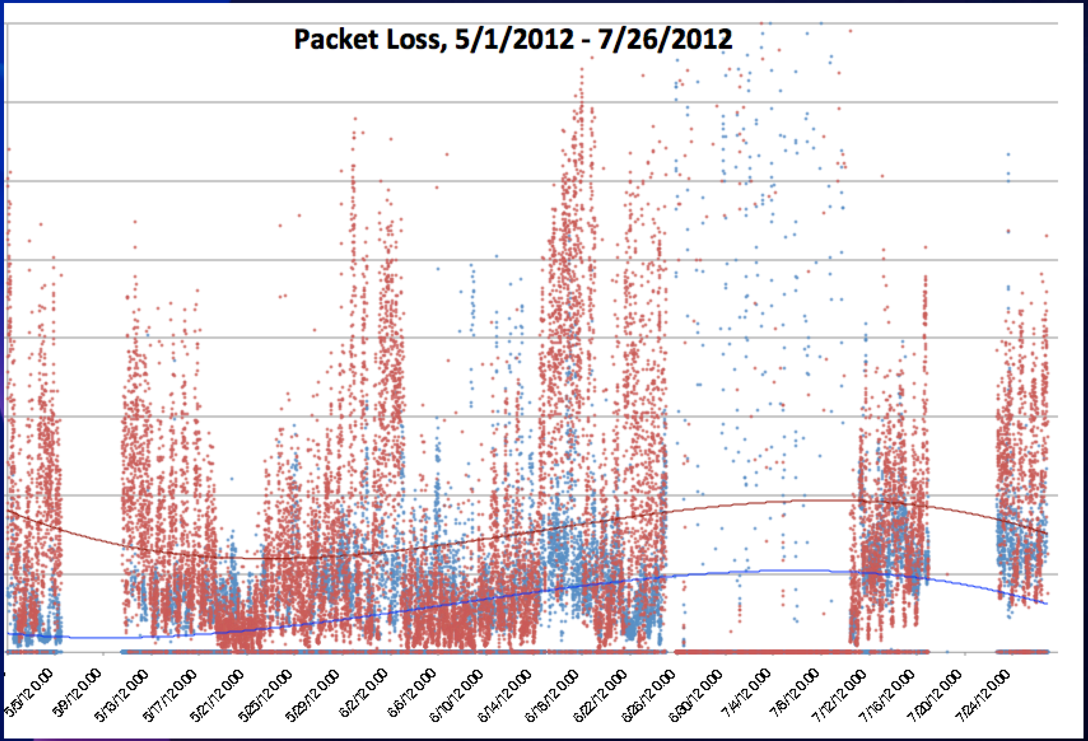
Parallel Database Architecture

Why all this power?

- Preparing the data for this graph from 250G argus archive (which helped a large international R&E network systemically address a huge performance problem) took me 3 days with our old setup

- We want any of our partners to be able do this in 3 minutes (or less)

- We want “room” to better research the area of performance, operations and security analytics with our international partners



But we're still designing for lesser needs as well (targeting single 1G and 10G networks)

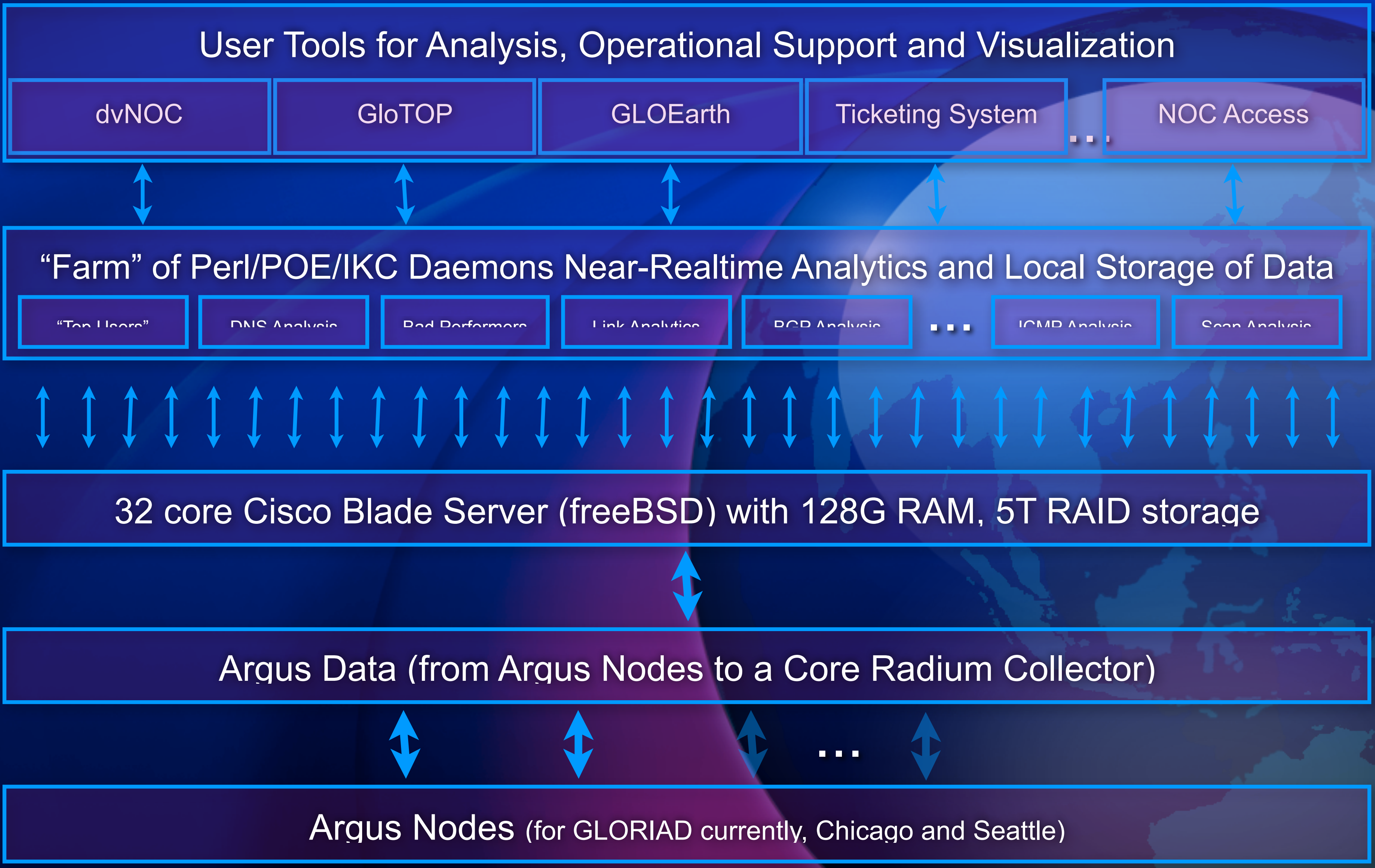
MacOSX

Linux

FreeBSD

New Process

(2015)



User Tools for Analysis, Operational Support and Visualization

"Farm" of Perl/POE/IKC Daemons Near-Realtime Analytics and Local Storage of Data

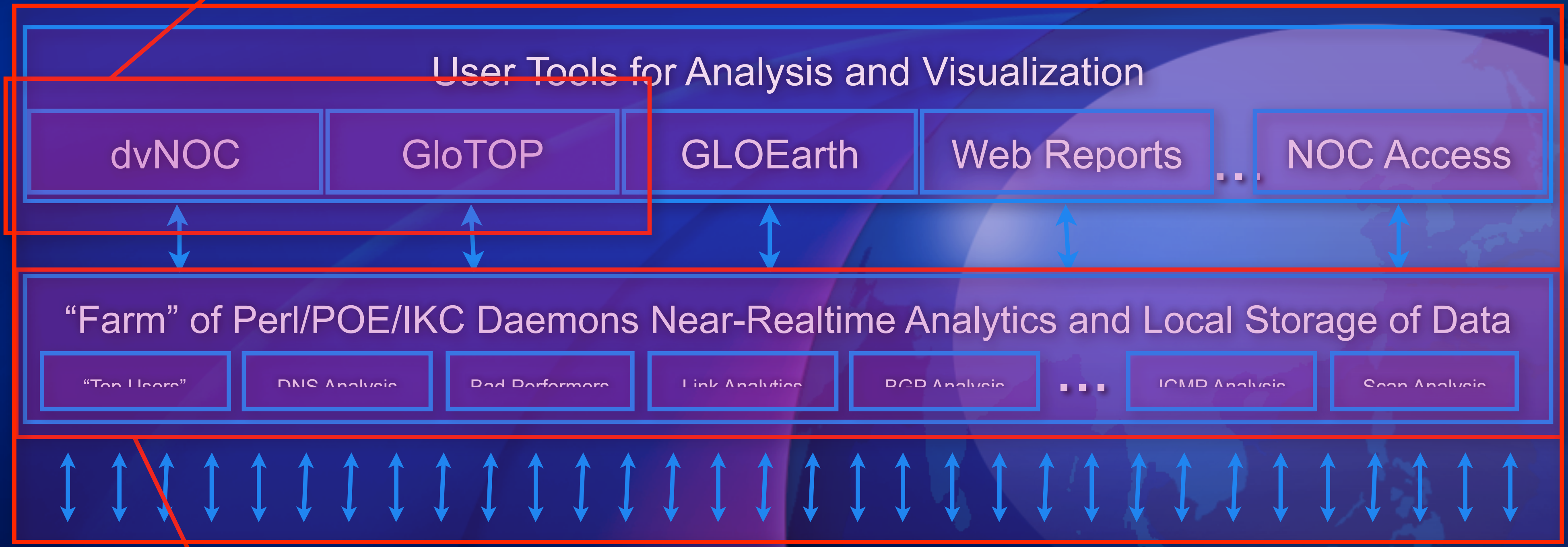
32 core Cisco Blade Server (freeBSD) with 128G RAM, 5T RAID storage

Argus Data (from Argus Nodes to a Core Radium Collector)

Argus Nodes (for GLORIAD currently, Chicago and Seattle)

More detail ..

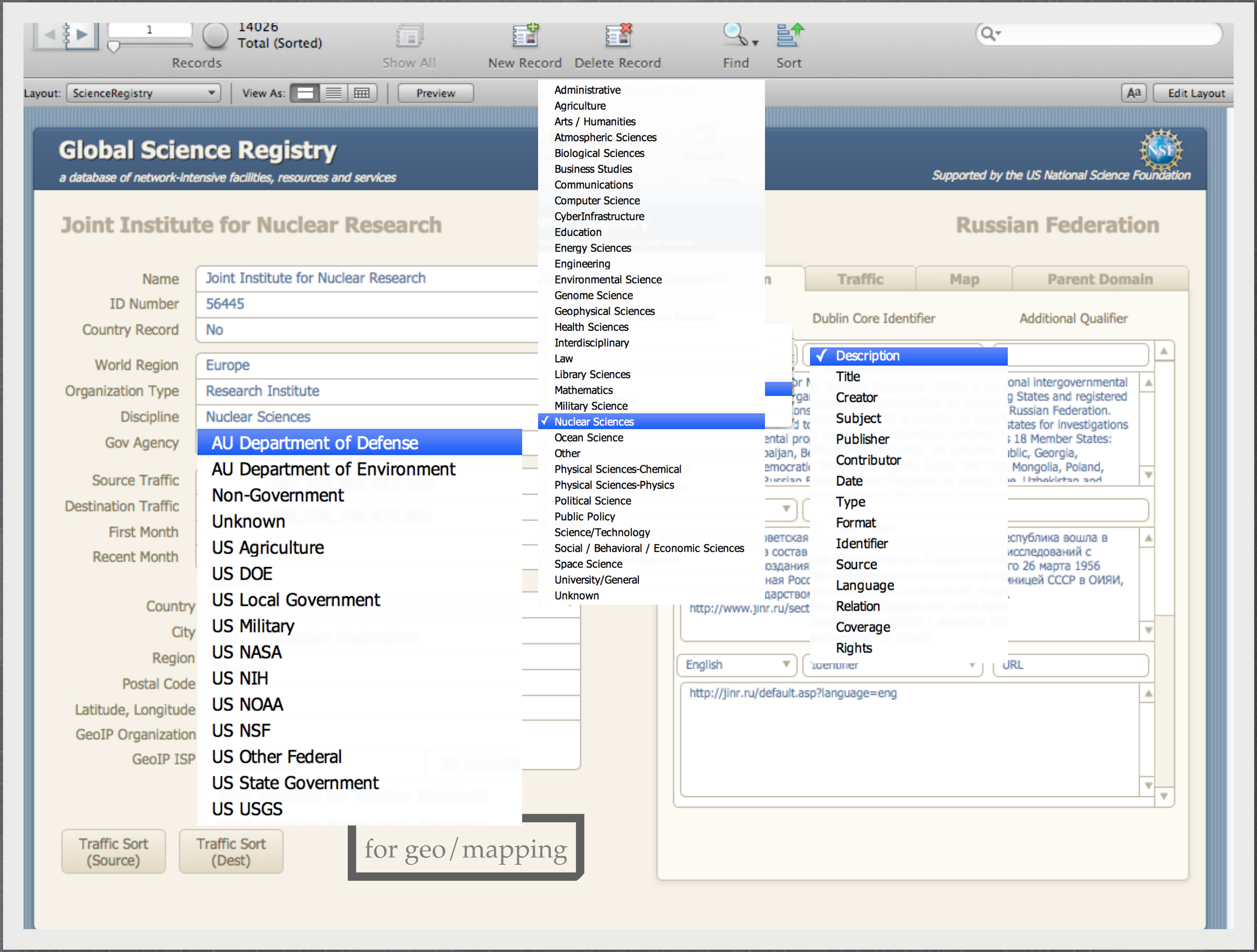
- Built with Runrev LiveCode
- Multi-platform (Mac, Windows, Linux, iOS, Android)
- Event-driven, graphic/media rich applications



- Perl POE event-loop, event-driven programming for “cooperative multi-tasking”
- ZeroMQ for inter-kernel communications between “animals”
- Elasticsearch for fast searching/browsing repository
- Daemonized (fast)
- Use MySQL (or any other) for long-term storage; SQLlite for local (fast) in-memory database
- Each “animal” on the “farm” is autonomous and very specialized
- Most read from a single argus RABINS stream (changing to ZeroMQ queues)

Global Science Registry

- Absolutely critical component
- Global database of Science institutions, resources, repositories
- Means of geo-locating and flexible assignment of metadata
- Flexible tagging/labeling scheme



Global Science Registry

a database of network-intensive facilities, resources and services

Joint Institute for Nuclear Research

Russian Federation

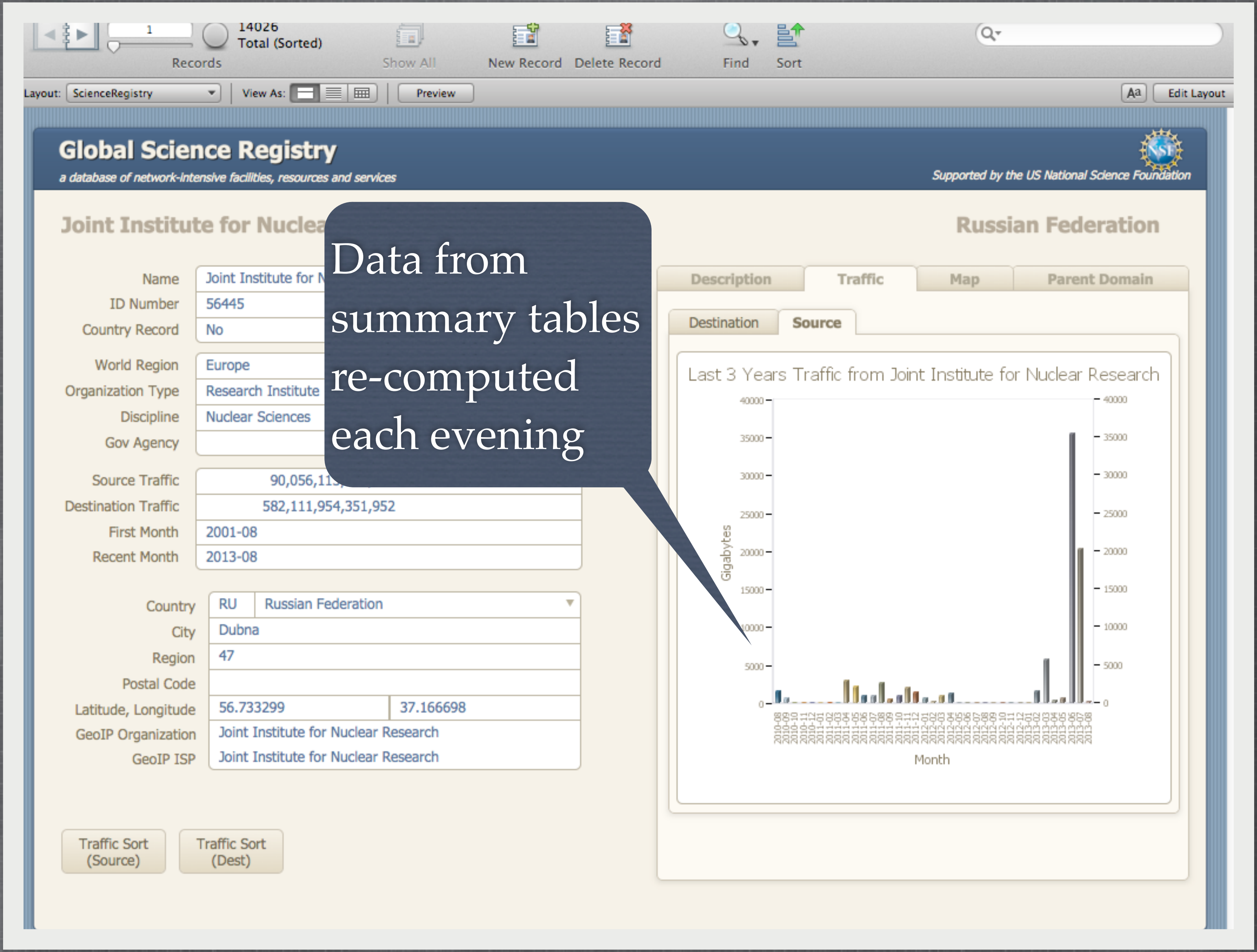
Name	Joint Institute for Nuclear Research
ID Number	56445
Country Record	No
World Region	Europe
Organization Type	Research Institute
Discipline	Nuclear Sciences
Gov Agency	
Source Traffic	
Destination Traffic	
First Month	
Recent Month	
Country	
City	
Region	
Postal Code	
Latitude, Longitude	
GeoIP Organization	
GeoIP ISP	

Dublin Core Identifier	Additional Qualifier
Description	
Identifier	URL

English

http://jinr.ru/default.asp?language=eng

for geo / mapping



Global Science Registry

a database of network-intensive facilities, resources and services

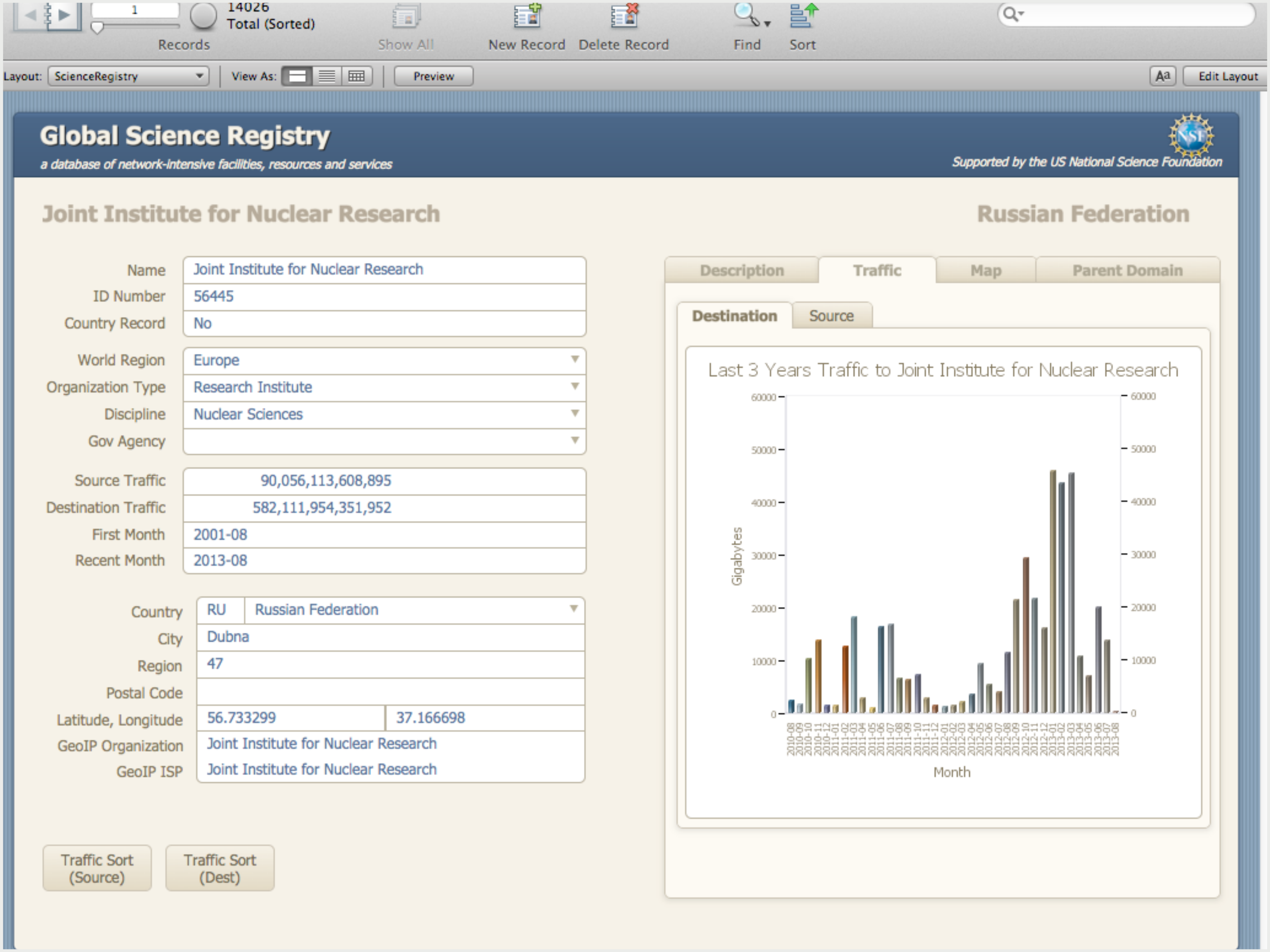
Supported by the US National Science Foundation

Joint Institute for Nuclea

Russian Federation

Name	Joint Institute for N
ID Number	56445
Country Record	No
World Region	Europe
Organization Type	Research Institute
Discipline	Nuclear Sciences
Gov Agency	
Source Traffic	90,056,11
Destination Traffic	582,111,954,351,952
First Month	2001-08
Recent Month	2013-08
Country	RU Russian Federation
City	Dubna
Region	47
Postal Code	
Latitude, Longitude	56.733299 37.166698
GeoIP Organization	Joint Institute for Nuclear Research
GeoIP ISP	Joint Institute for Nuclear Research

Data from summary tables re-computed each evening



Global Science Registry

a database of network-intensive facilities, resources and services

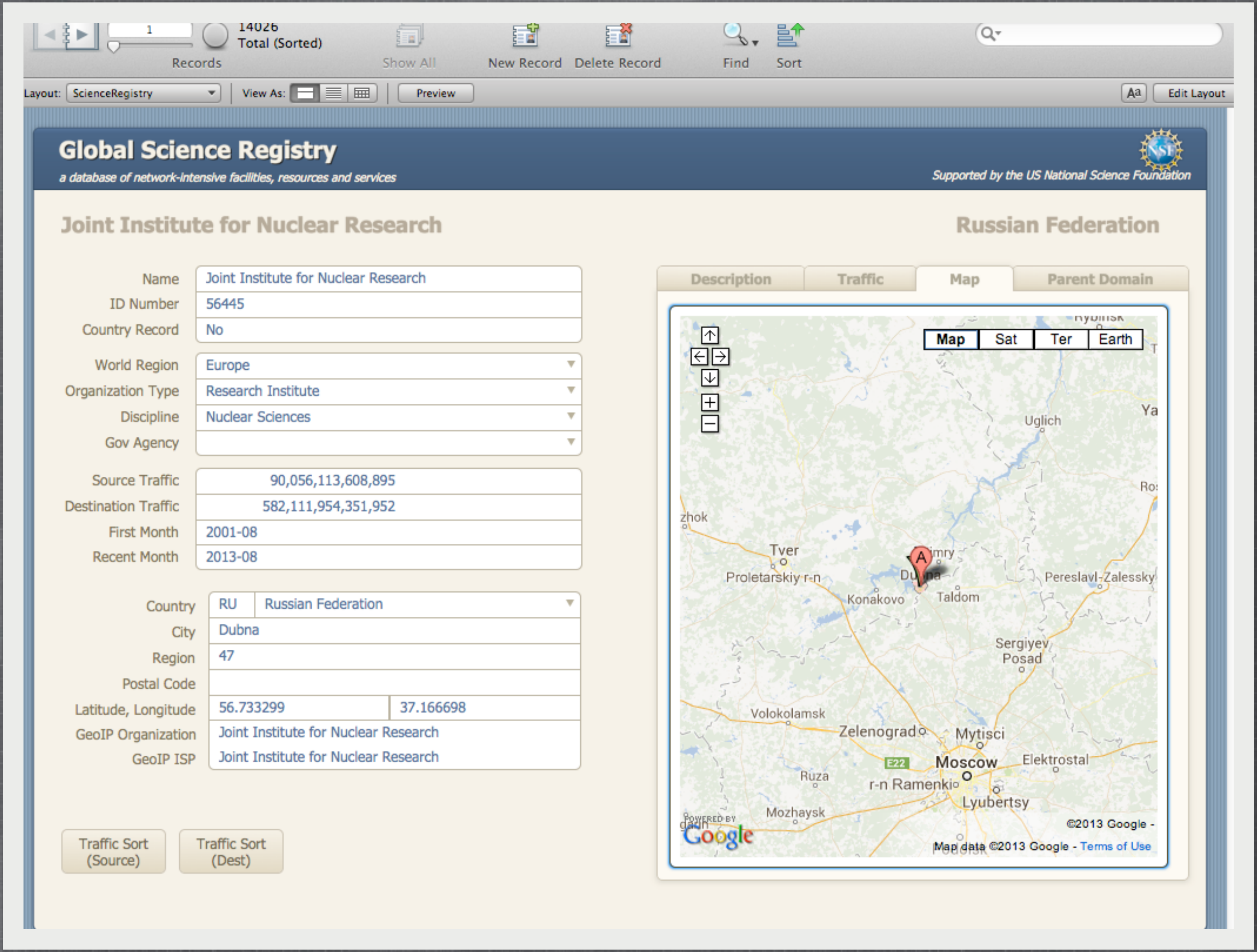
Supported by the US National Science Foundation

Joint Institute for Nuclear Research

Russian Federation

Name	Joint Institute for Nuclear Research
ID Number	56445
Country Record	No
World Region	Europe
Organization Type	Research Institute
Discipline	Nuclear Sciences
Gov Agency	
Source Traffic	90,056,113,608,895
Destination Traffic	582,111,954,351,952
First Month	2001-08
Recent Month	2013-08
Country	RU Russian Federation
City	Dubna
Region	47
Postal Code	
Latitude, Longitude	56.733299 37.166698
GeoIP Organization	Joint Institute for Nuclear Research
GeoIP ISP	Joint Institute for Nuclear Research

Last 3 Years Traffic to Joint Institute for Nuclear Research



Global Science Registry

a database of network-intensive facilities, resources and services

Supported by the US National Science Foundation

Joint Institute for Nuclear Research

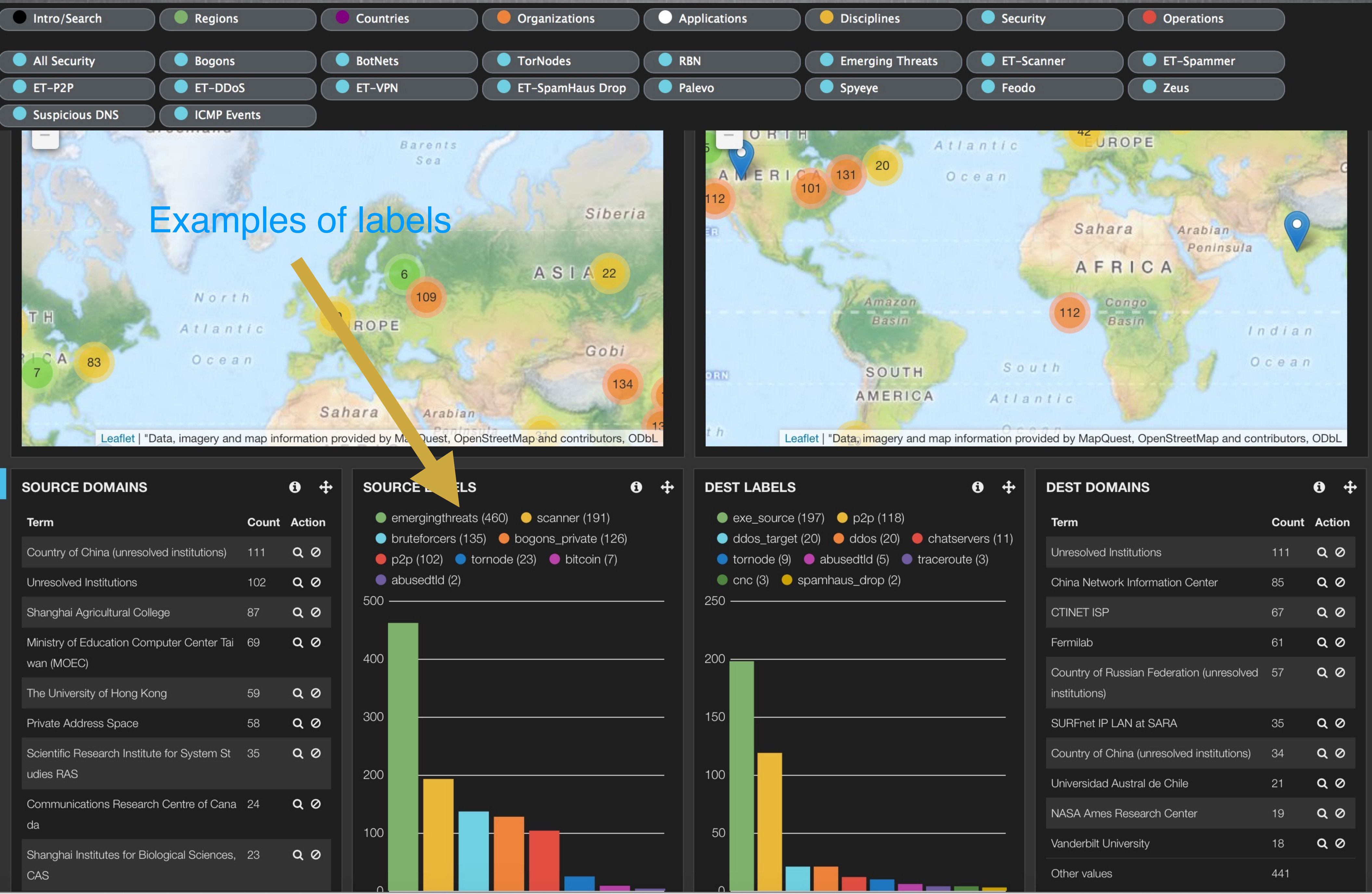
Russian Federation

Name	Joint Institute for Nuclear Research
ID Number	56445
Country Record	No
World Region	Europe
Organization Type	Research Institute
Discipline	Nuclear Sciences
Gov Agency	
Source Traffic	90,056,113,608,895
Destination Traffic	582,111,954,351,952
First Month	2001-08
Recent Month	2013-08
Country	RU Russian Federation
City	Dubna
Region	47
Postal Code	
Latitude, Longitude	56.733299 37.166698
GeoIP Organization	Joint Institute for Nuclear Research
GeoIP ISP	Joint Institute for Nuclear Research

Intend to work with others on ..

- AMIS Consortium on Data Privacy (and 100G deployment)
- Northwestern Univ on 100G deployment (via SDN/Cloud-based approach)
- Industry partners on 100G deployment
- R&E deployments (Indiana U)
- GLIF Performance Verification Task-force (Jerry Sobieski)
- "The World" on GSR Improvements and on open-source InSight itself

New: Labeling/Tagging facility



Examples of labels

SOURCE DOMAINS

Term	Count	Action
Country of China (unresolved institutions)	111	🔍 ⊘
Unresolved Institutions	102	🔍 ⊘
Shanghai Agricultural College	87	🔍 ⊘
Ministry of Education Computer Center Taiwan (MOEC)	69	🔍 ⊘
The University of Hong Kong	59	🔍 ⊘
Private Address Space	58	🔍 ⊘
Scientific Research Institute for System Studies RAS	35	🔍 ⊘
Communications Research Centre of Canada	24	🔍 ⊘
Shanghai Institutes for Biological Sciences, CAS	23	🔍 ⊘

SOURCE LABELS

● emergingthreats (460) ● scanner (191)
● bruteforcers (135) ● bogons_private (126)
● p2p (102) ● tornode (23) ● bitcoin (7)
● abusedtld (2)

DEST LABELS

● exe_source (197) ● p2p (118)
● ddos_target (20) ● ddos (20) ● chatservers (11)
● tornode (9) ● abusedtld (5) ● traceroute (3)
● cnc (3) ● spamhaus_drop (2)

DEST DOMAINS

Term	Count	Action
Unresolved Institutions	111	🔍 ⊘
China Network Information Center	85	🔍 ⊘
CTINET ISP	67	🔍 ⊘
Fermilab	61	🔍 ⊘
Country of Russian Federation (unresolved institutions)	57	🔍 ⊘
SURFnet IP LAN at SARA	35	🔍 ⊘
Country of China (unresolved institutions)	34	🔍 ⊘
Universidad Austral de Chile	21	🔍 ⊘
NASA Ames Research Center	19	🔍 ⊘
Vanderbilt University	18	🔍 ⊘
Other values	441	

Please Join Us!

(help ...)