On the Past, Present and Future of "Big (Internet) Data"

Walter Willinger
NIKSUN, Inc., Princeton, NJ
wwillinger@niksun.com

December 7, 2017

My Encounter with "Big (Internet) Data"

- 1991 – 2002: Internet traffic
  - An early instance of "big (Internet) data"
- 2000 – 2015: Internet topology
  - A different kind of "big (Internet) data"
- 2013 – present: Cyber security
  - A new kind of "big (Internet) data"

My Work with “Big (Internet) Data” …

- Aiding in scientific discovery (Internet traffic)
- Enforcing scientific rigor (Internet topology)
- For the good of the Internet (cyber security)

Aiding Scientific Discovery – Internet Traffic

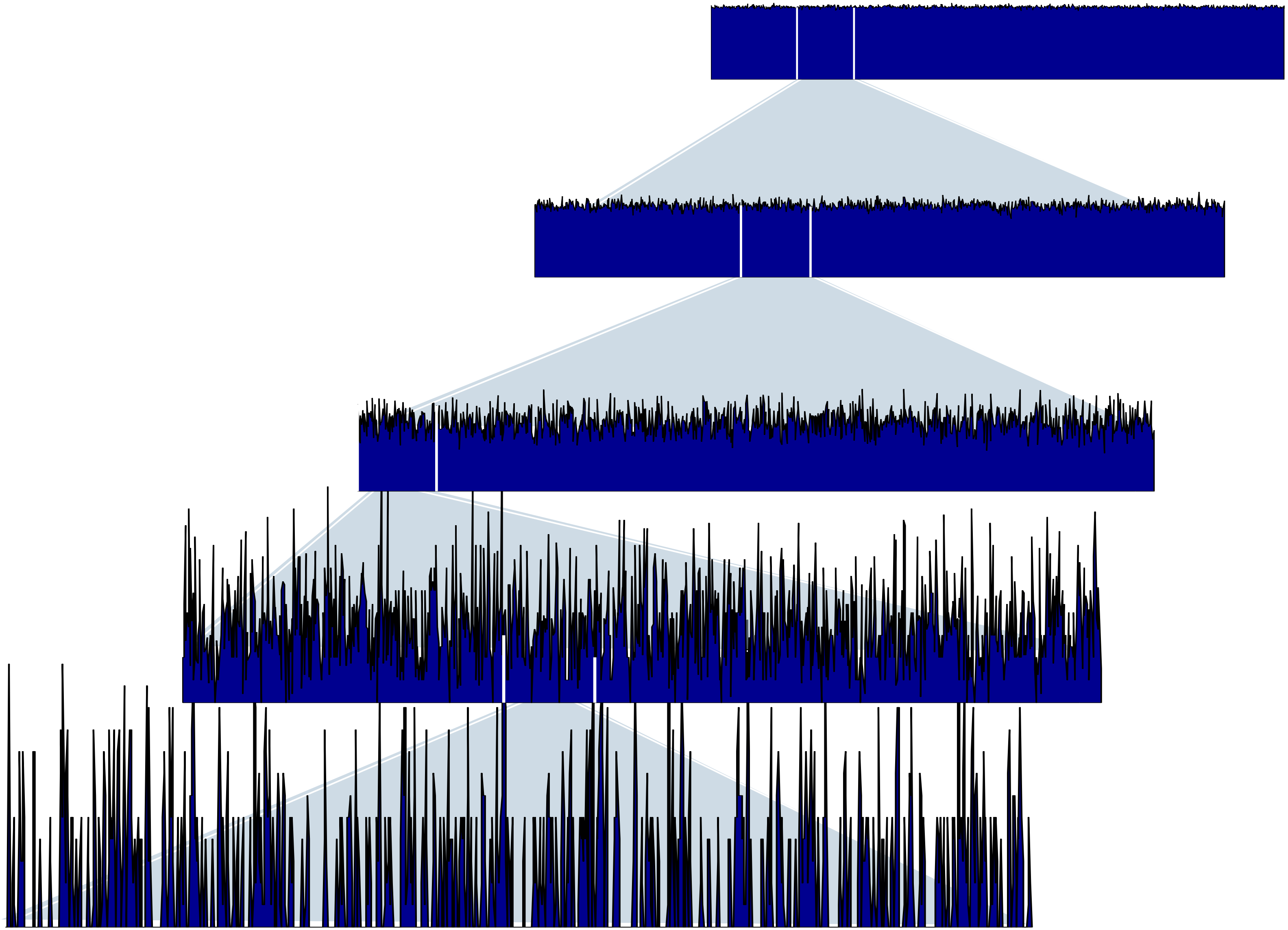
Internet Traffic: ~1990

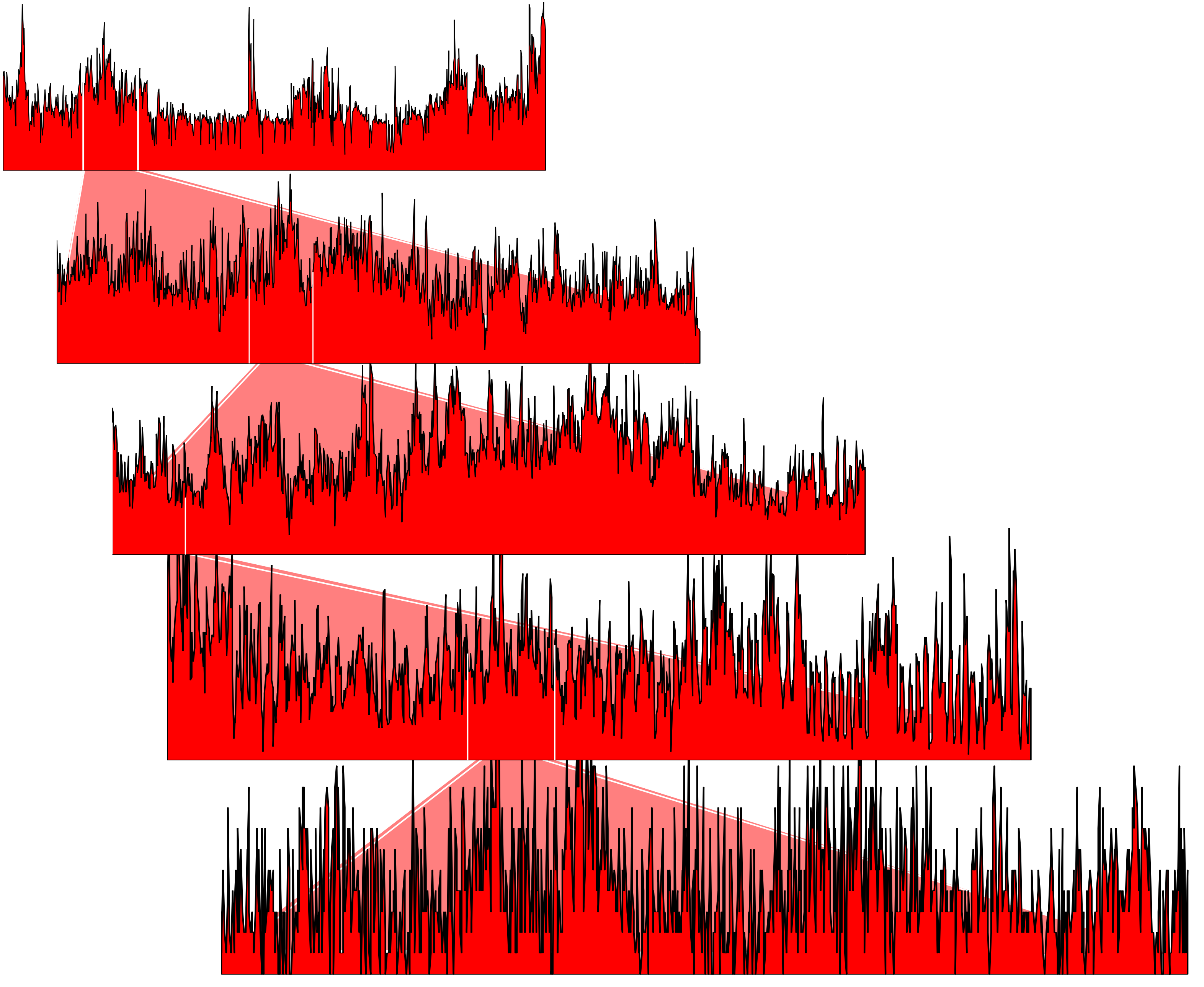
- Conventional wisdom
  - Shaped by decades of work on telephone traffic
  - No measurements of actual packet traffic over early Internet

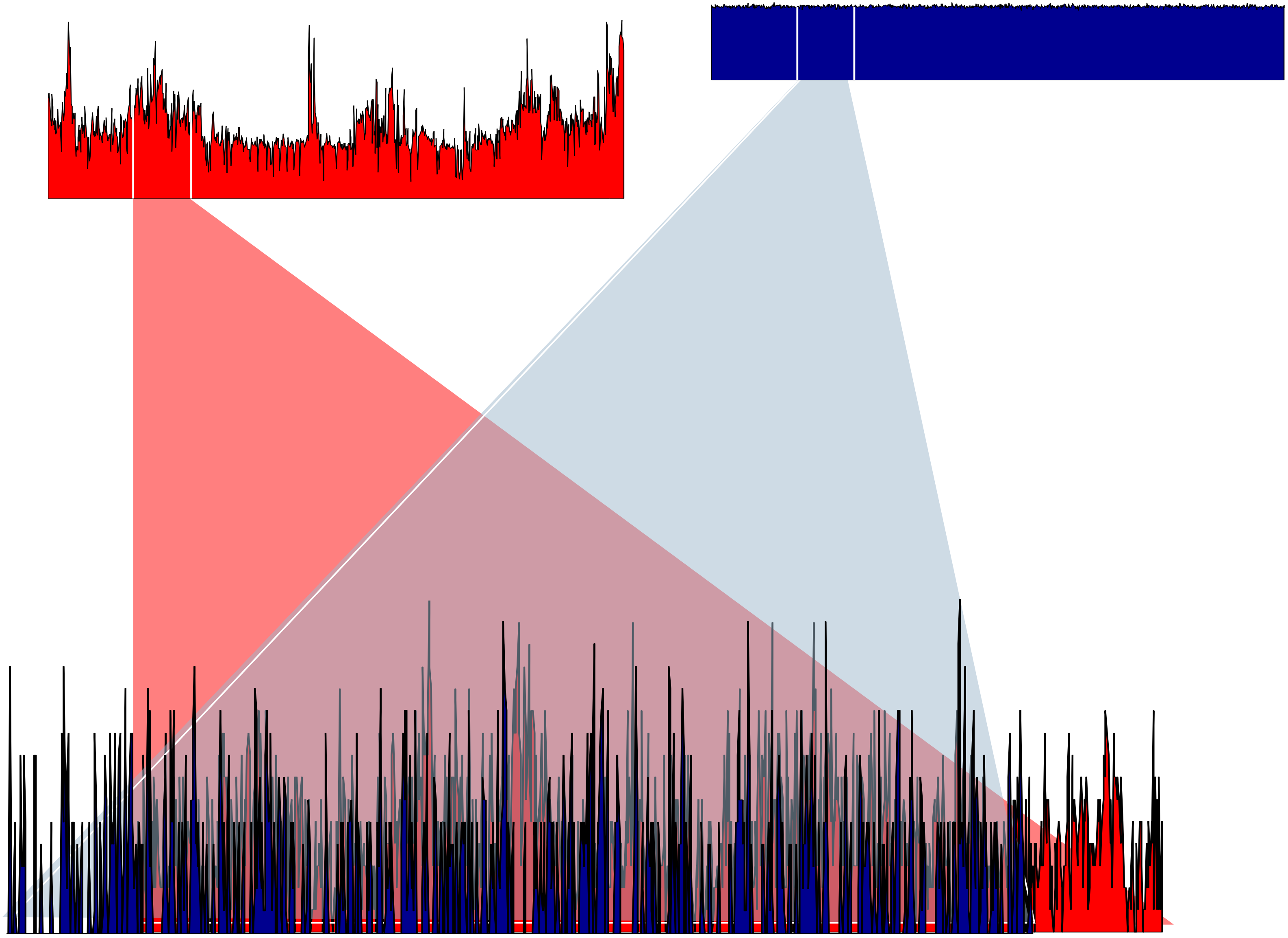
- Typical assumptions made about packet-level Internet traffic
  - Network traffic is Poisson
  - Network traffic exhibits no (weak) temporal dependencies
  - Call durations, packet inter-arrival times, etc. are well-modeled by light-tailed distributions (e.g., exponential distribution)

Internet Traffic: ~1993

- First measurements of actual packet-level traffic
  - High time-resolution packet traces (Leland and Wilson, Bellcore)
  - Week-long Ethernet LAN (1-10 Mbps) traffic traces
  - Early instance of "big (Internet) data" (millions of packets)
- Year-long analysis effort
  - Findings are described in our SIGCOMM'93 paper







Internet Traffic: ~1993

- Empirical findings that dispense with conventional wisdom
  - Real-world network traffic is self-similar ("fractal")
  - Measured traffic exhibits strong (long-range) temporal dependencies
- Mathematical results that explain the discovery
  - Simple generative mathematical models point towards heavy-tailed distributions as main root cause for observed self-similarity
  - Empirical analysis of the measured traffic at the level of sessions, TCP connections, IP flows, etc. shows that measured sessions, TCP connections, IP flows, etc. are well-modeled by heavy-tailed distributions (e.g., Pareto-type distributions)

Internet Traffic: post-1993

- Many subsequent traffic studies
  - Essentially all studies confirmed observed self-similarity
  - Many demonstrated a refined version of self-similarity

- The "new" type of conventional wisdom re Internet traffic
  - Heavy-tailed distributions are the norm, not the exception
  - Heavy-tailed distributions have become an "invariant" of Internet traffic
  - Root cause(s) of heavy tails
  - **Reference**: *Heavy tails, generalized coding, and optimal Web layout*; X. Zhu, J. Yu, and J. Doyle; appeared in: IEEE Infocom 2001

  - 2006 SIGCOMM Test-of-Time Award for our SIGCOMM'93 paper

Internet Traffic: An early "big data" angle

- Real-time estimation of self-similarity parameter H
  - Treat packet traces as streaming data ("data in motion")
  - Basic requirement: No multiple passes over data are allowed

- Early instance of a streaming data algorithm
  - **Reference**: *Real-time estimation of the parameters of long-range dependence*; M. Roughan, D. Veitch, and P. Abry; appeared in: IEEE/ACM Transactions on Networking, 2000

Enforcing Scientific Rigor – Internet Topology

Internet Topology: ~1969 (ARPANET)

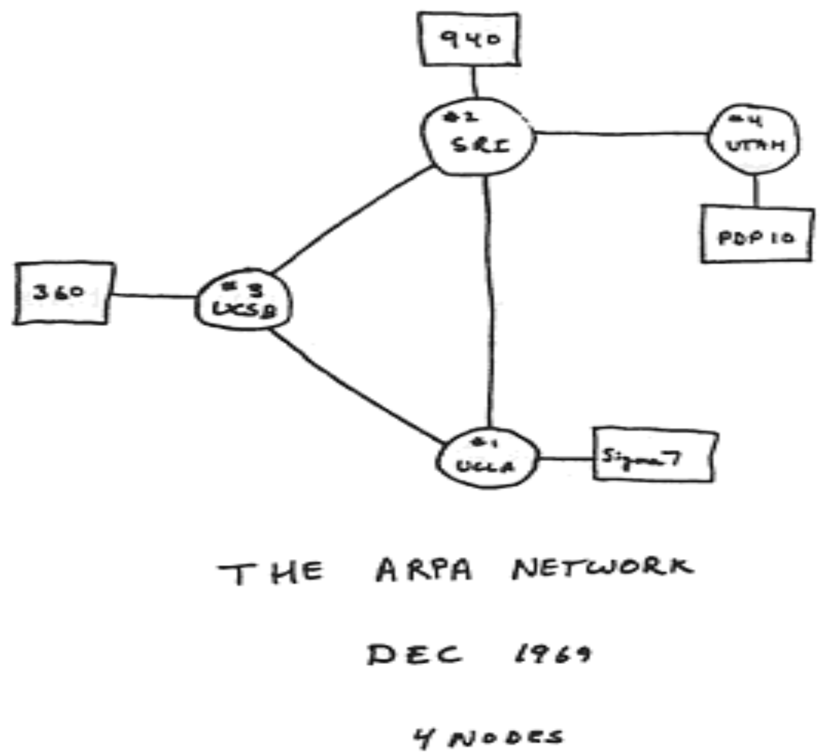
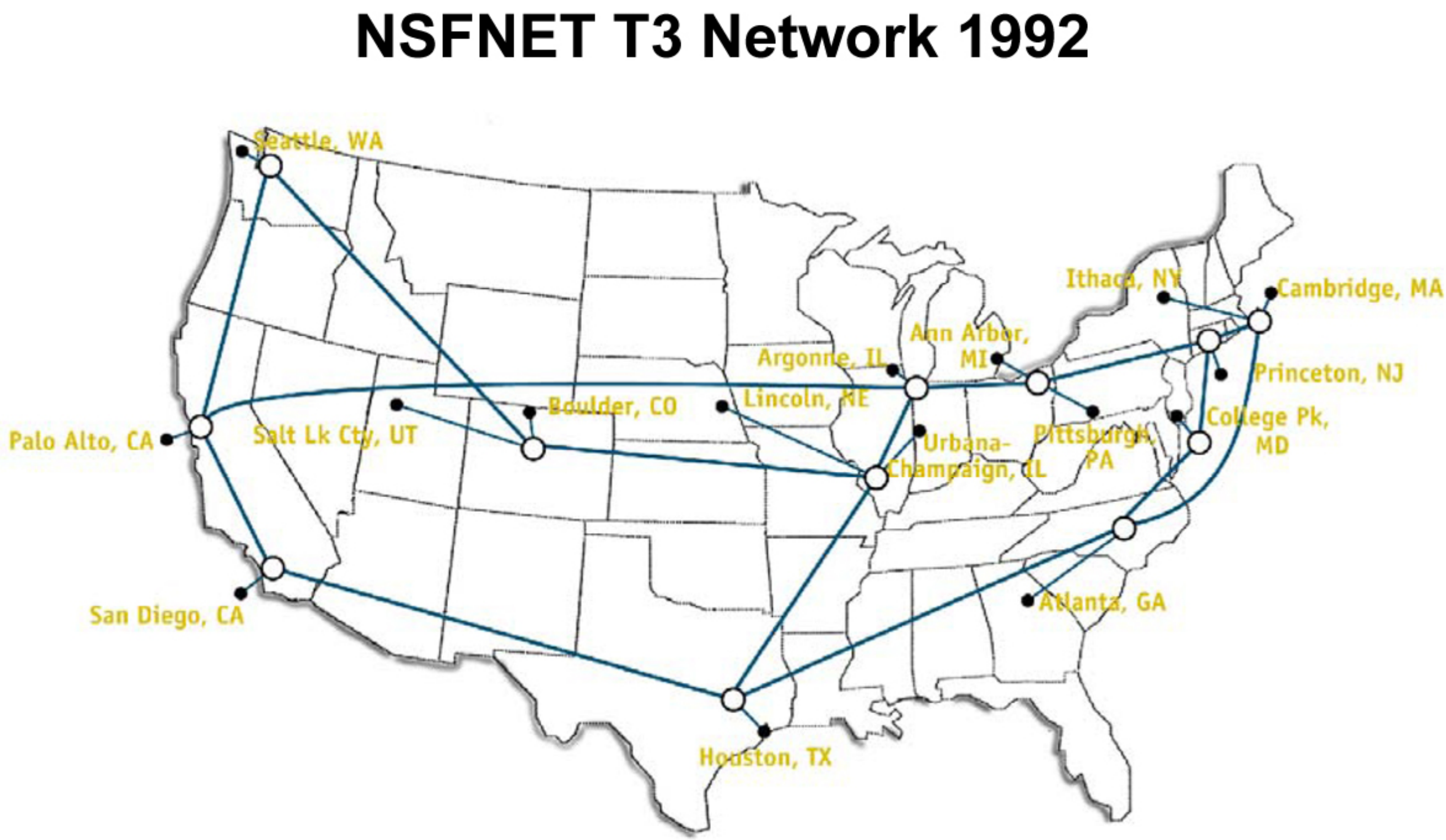


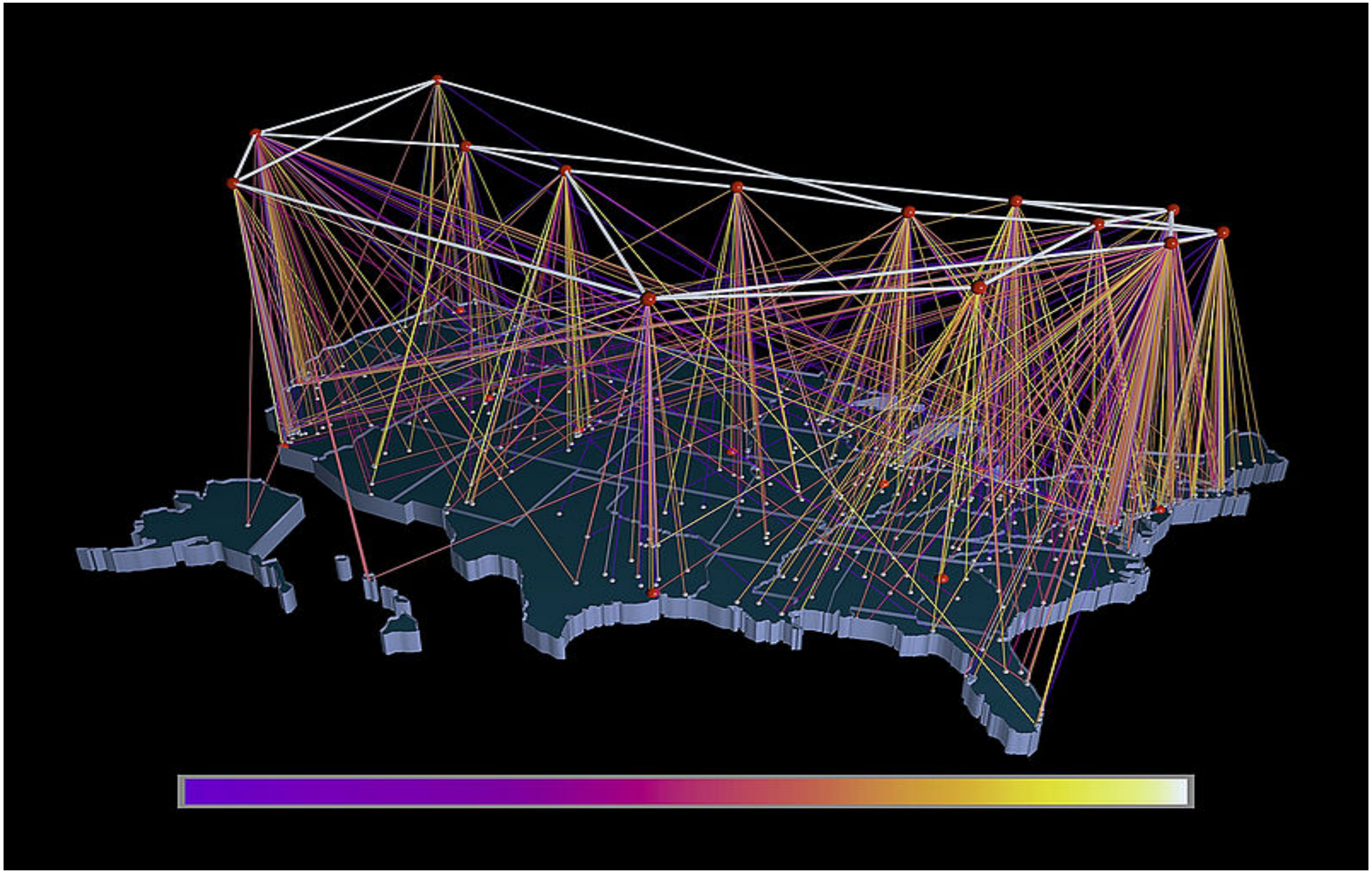
FIGURE 6.2 Drawing of 4 Node Network
(Courtesy of Alex McKenzie)

Internet Topology: ~1991 (NSFNET)



Merit Network, Inc. - Merit Network, Inc.(1992)

Internet Topology: ~1994 (NSFNET)



Source: https://en.wikipedia.org/wiki/National_Science_Foundation_Network

Internet Topology: Pre-1995

- One person/group/organization had all the information to draw a detailed map of the network's physical topology
  - Geographic locations of routers/end devices
  - Connectivity
  - Traffic
- 1995 – Decommissioning of the NSFNET

Internet Topology: Post-1995

- 1995 – Birth of the "public Internet"
  - An increasing number of different networks, companies, organizations
  - Some 50,000 Autonomous Systems (AS) as of 2015
- No one person/group/organization has all the information to draw a detailed map of the network's physical topology
  - Geographic locations of routers/end devices?
  - Connectivity??
  - Traffic???

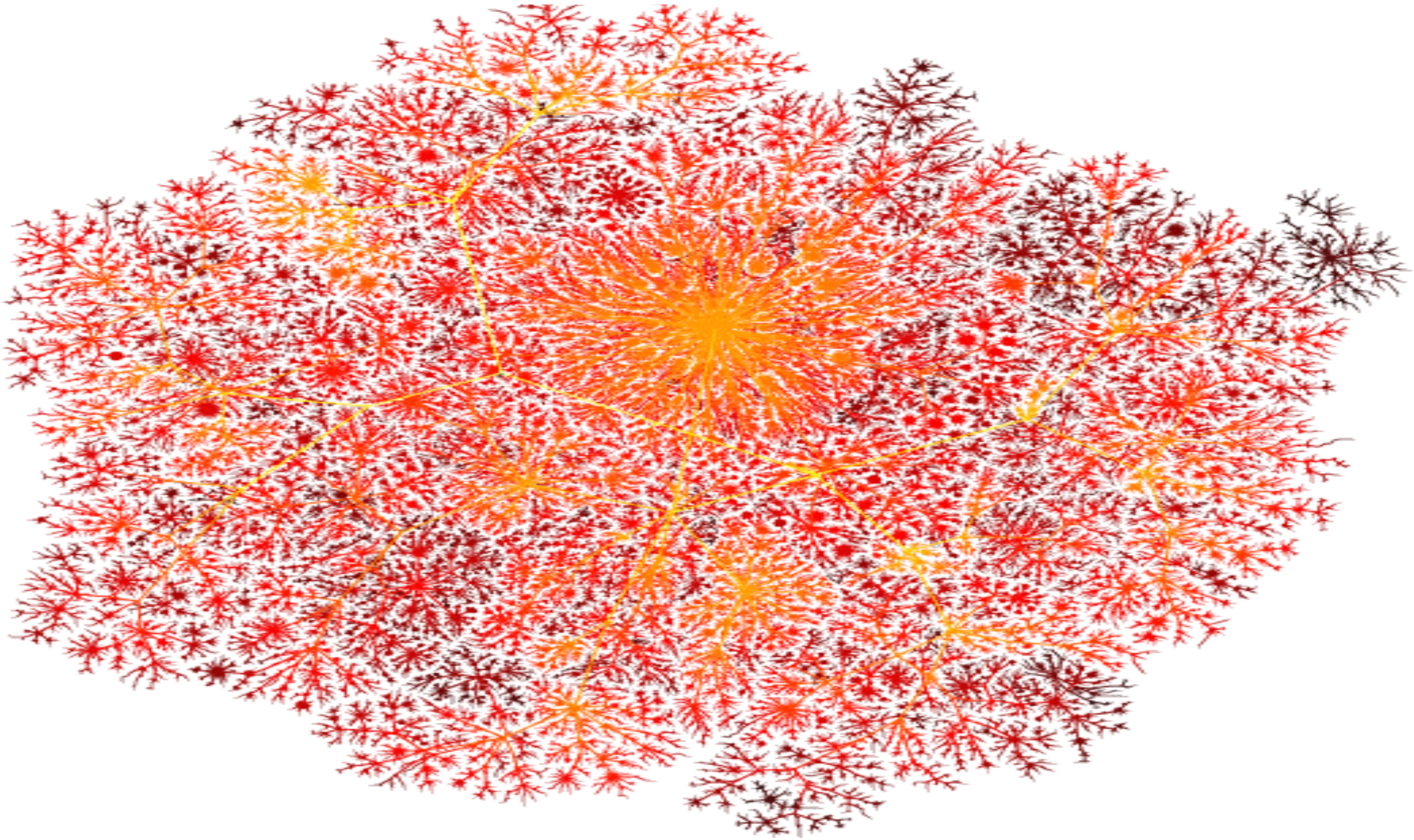
Internet Topology: Post-1995

- Measurement studies for (physical) topology discovery
  - Basic tool: traceroute (Van Jacobson, 1988)
  - Large-scale traceroute campaigns by many different research groups
- New types of "big (Internet) data"
  - Example: Archipelago Measurement Infrastructure (Caida, 2007)
  - 3 teams (~20 monitors each) independently probe some 20M /24's (full routed IPv4 address space) at 100pps in 2-3days
  - As of early 2011, the campaign has resulted in some 10 billion traceroute measurements (about 4TB of data) collected from about 60 different vantage points across the Internet

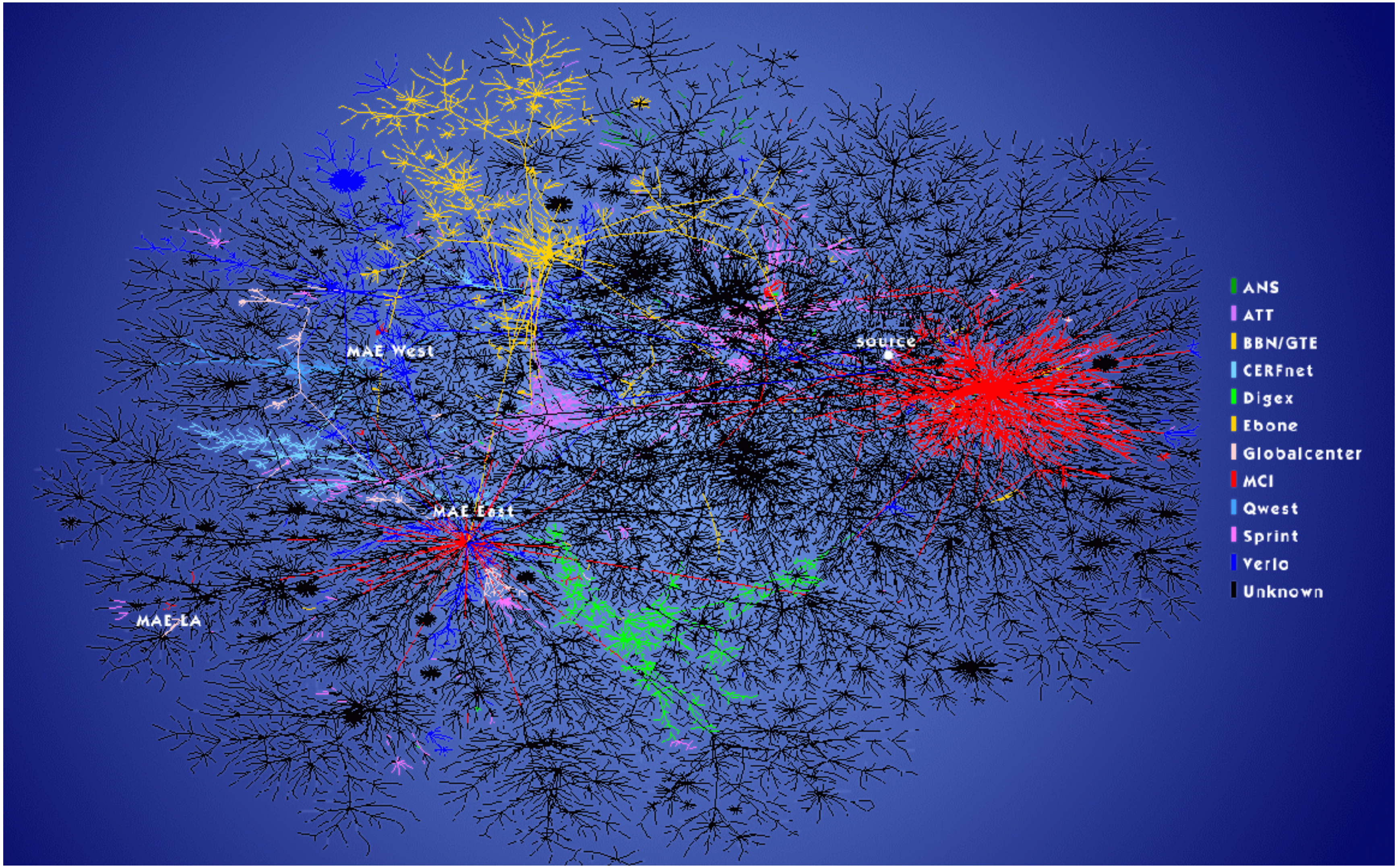
traceroute from NJ to 130.126.0.201

- 1 wireless_broadband_router (192.168.1.1)
- 2 173.63.208.1 (173.63.208.1)
- 3 g0-3-3-1.nwrknj-lcr-22.verizon-gni.net (130.81.179.194)
- 4 130.81.162.84 (130.81.162.84)
- 5 0.xe-3-2-0.br2.nyc4.alter.net (152.63.20.213)
- 6 204.255.168.114 (204.255.168.114)
- 7 be2063.mpd22.jfk02.atlas.cogentco.com (154.54.47.57)
- 8 be2117.mpd22.ord01.atlas.cogentco.com (154.54.7.58)
- 9 te0-0-2-0.rcr12.ord09.atlas.cogentco.com (154.54.31.230)
- 10 university-of-illinios-urbana.demarc.cogentco.com (38.104.99.42)
- 11 t-ch2rtr.ix.ui-iccn.org (72.36.126.77)
- 12 t-710rtr.ix.ui-iccn.org (72.36.126.81)
- 13 72.36.127.86 (72.36.127.86)
- 14 iccn-ur1rtr-uiuc1.gw.uiuc.edu (72.36.127.2)
- 15 t-exite1.gw.uiuc.edu (130.126.0.201)

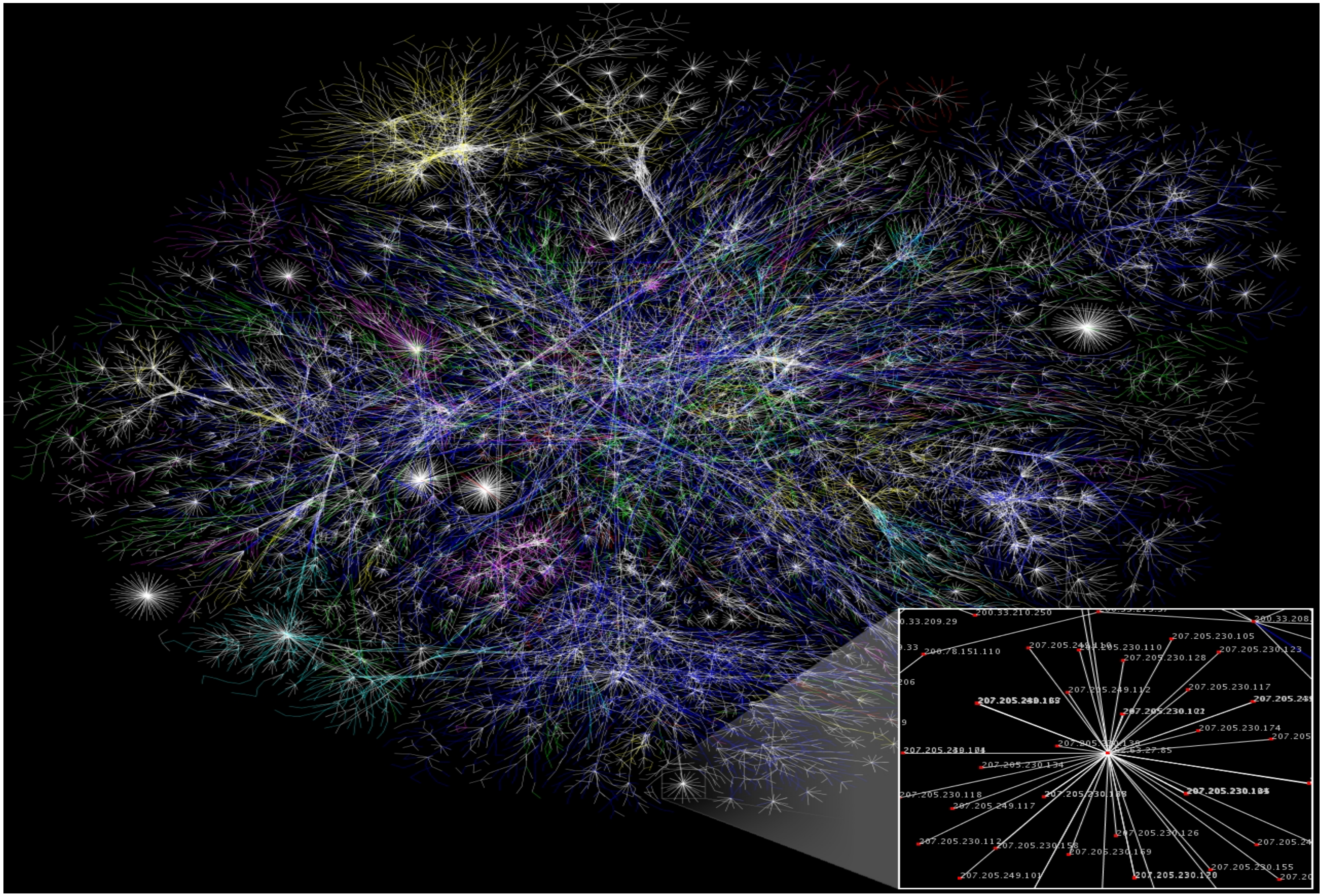
Internet Topology: ~1998



Internet Topology: ~2000



Internet Topology: ~2010



Source: https://en.wikipedia.org/wiki/File:Internet_map_1024.jpg

Internet Topology: Post-1995 (Part I)

- Surprising first "discovery" …
  - The physical (i.e., router-level) Internet topology has power-law node degree distribution (Faloutsos et al, SIGCOMM 1999)
  - 2013 SIGCOMM Test-of-Time Award for SIGCOMM'99 paper
- Surprising second "discovery" …
  - The physical Internet is well-modeled by scale-free random graph models of the preferential attachment type
  - Such graph models are highly vulnerable to knocking out "hubs"
  - Discovery of the Internet's "Achilles' heel"
  - Article/Cover story in Nature (Barabasi et al, 2000)


nature
Achilles' heel of the Internet
Obesity Mice that eat more but weigh less
Ocean anoxic events Not all at sea
Cell signalling Fringe sweetens Notch

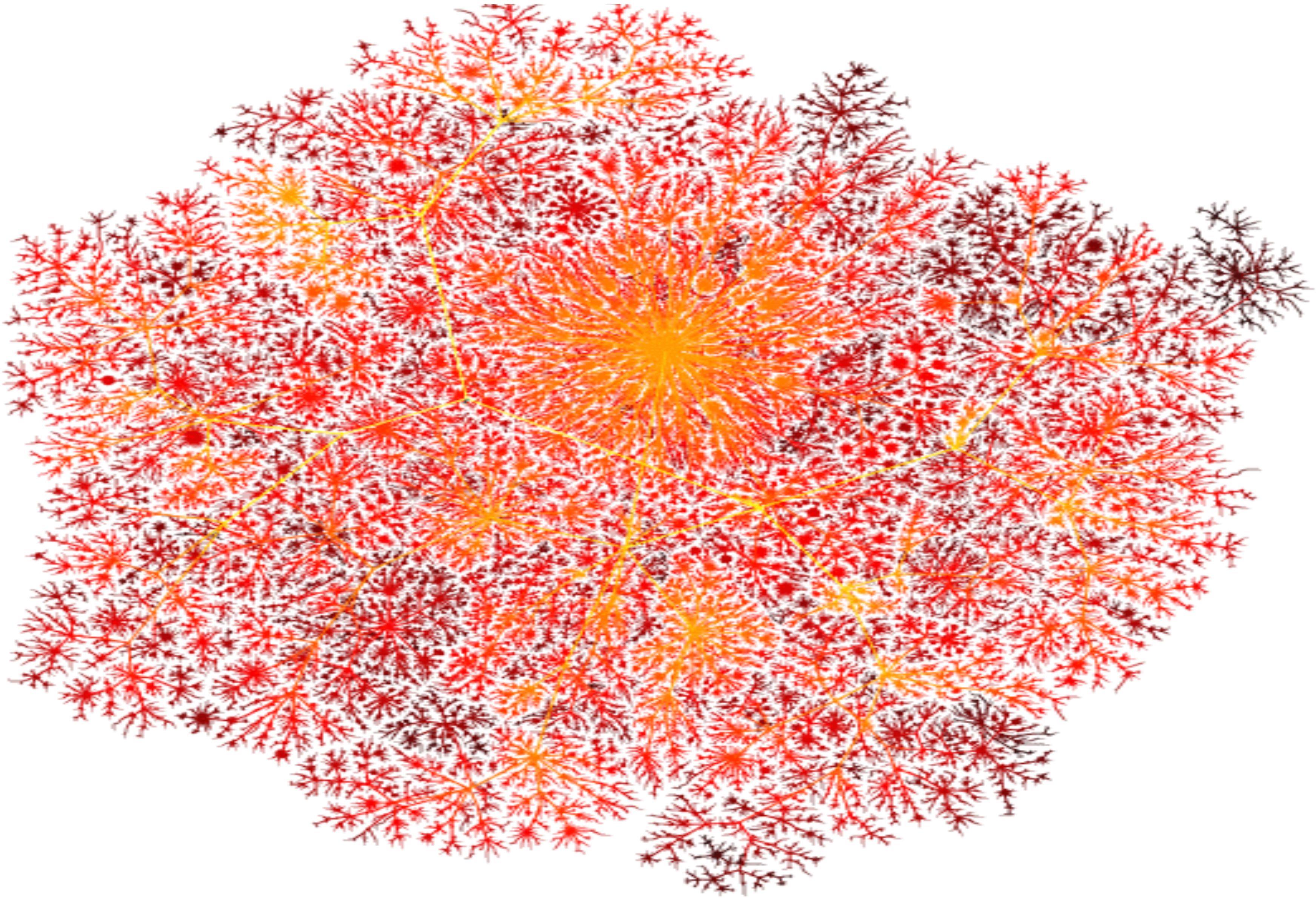
Internet Topology: Post-1995 (Part II)

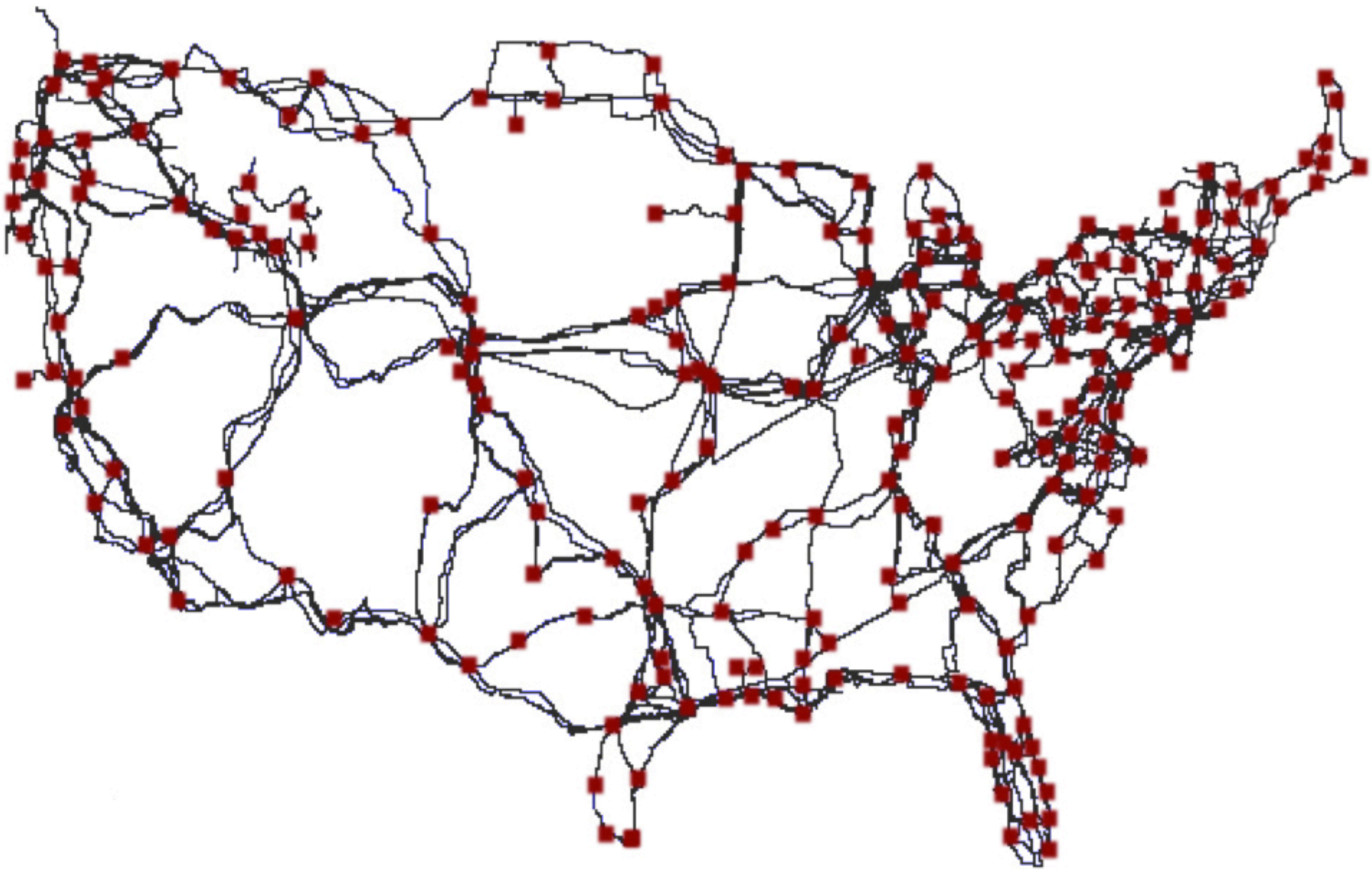
- Debunking the "discoveries" as "myths" …
  - "Big (Internet) data" consisting of billions of traceroute measurements is too dirty to infer node degree distribution, be it power-law or some other type of distribution
  - SIGCOMM'04 paper on "A first-principles approach to understanding the Internet's router-level topology", L. Li, D. Alderson, W. Willinger, J. Doyle, provides technological and economic arguments that rule out claimed Achilles' heel on first-principles
  - 2005 PNAS paper on "The 'robust yet fragile' nature of the Internet", J. Doyle, D. Alderson, L. Li, S. Low, M. Roughan, S. Shalunov, R. Tanaka, and W. Willinger

- 2016 SIGCOMM Test-of-Time Award for our SIGCOMM'04 paper

Internet Topology: Post-1995 (Part III)

- A recent "big data" angle
  - An initial step, but not yet for "distributed streaming data"
  - **Reference**: *BGPStream: A software framework for live and historical BGP data analysis*, C. Orsini, A. King, D. Giordano, V. Giotsas, and A. Dainotti; appeared in: Proc. IMC'16, 2016.
- What is the Internet's physical topology?
  - The physical topology of the Internet is actually very simple!
  - Our SIGCOMM'15 paper





How to Map the (Physical) US Internet?

- Joint with R. Durairajan, P. Barford (Univ. Wisconsin) and J. Sommers (Colgate Univ.), SIGCOMM 2015

- For portal access: http://internetatlas.org
- For account access: https://www.impactcybertrust.org

Objectives of our Work

- Create and maintain a comprehensive catalog of the *physical Internet*
  - Geographic locations of nodes (buildings that house PoPs, IXPs etc.) and links (fiber conduits)
- Extend with relevant related data
  - Traffic, active probes, BGP updates, weather, etc.
- Maintain portal for visualization and analysis
- Apply maps to problems of interest
  - Robustness, performance, security, etc.

Objectives of our Work

- Create and maintain a comprehensive catalog of the *physical Internet*
  - Geographic locations of nodes (buildings that house PoPs, IXPs etc.) and links (fiber conduits)
- Extend with relevant related data
  - Traffic, active probes, BGP updates, weather, etc.
- Maintain portal for visualization and analysis
- Apply maps to questions of interest
  - Robustness, performance, security, etc.

Related Work

- Many prior Internet mapping efforts
  - Lots of traceroute-based studies
    - Data plane measurements to infer/map router topology
  - Many BGP update-based studies
    - Control plane measurements to infer/map AS topology
  - Some studies to infer/map the physical Internet
    - S. Gorman (2004) – FortiusOne (GeoCommons)
    - J.M. Kraushaar (FCC reports until 1998)
- Commercial activities
  - KMI Corp. (~early 2000)
  - TeleGeography, FiberLocator (NEF, Inc.)

The Physical Internet: Nodes

From Routers/Switches …

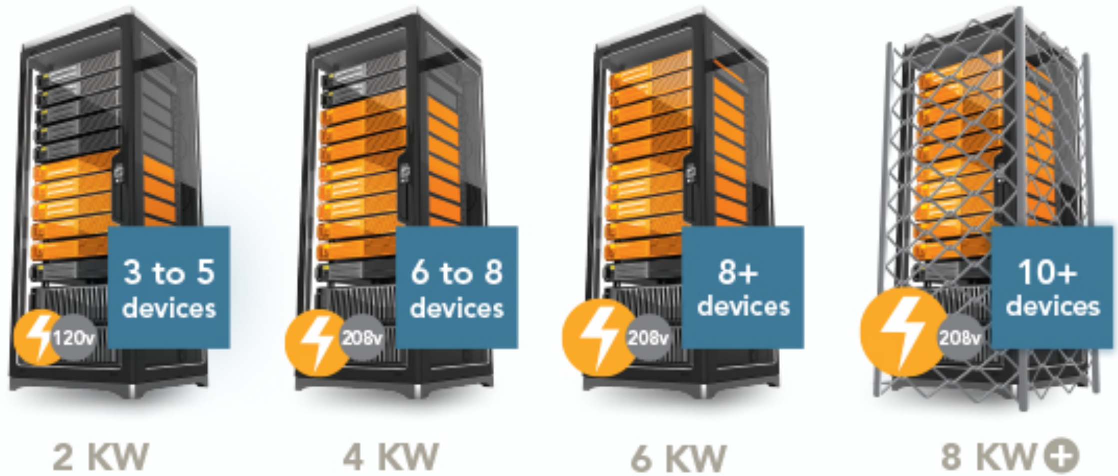
$$$$$

$$$$$$$

$

$$ to $$$$$

… to Racks/Cabinets/Cages …



… to Colocations (Colos) …

interxion

terremark

DIGITAL REALTY
Data Center Solutions

EQUINIX

DuPont Fabros Technology

TELEHOUSE
HOME TO YOUR GLOBAL ICT SOLUTIONS

cologix

CORESITE

telx
THE INTERCONNECTION COMPANY

… to Carrier Hotels/Data Centers

The Physical Internet: Nodes

- Major cities or metropolitan areas
  - Contain a majority of colocation facilities/data centers
  - Much is known about commercial colocation facilities/data centers
  - Places where long-haul fiber-optic cables originate/terminate

- Our map
  - Some 2000 colocation facilities/data centers
  - In 273 cities (nodes of our map)

The Physical Internet: Links

The Physical Internet: Links

- Long-haul links definition
  - Spans at least 30 miles or
  - Connects cities of population >= 100k people or
  - Shared by at least 2 providers

- Use maps of US infrastructure from 12 tier-1 and 4 major cable and 4 regional providers
  - Includes both geocoded and non-geocoded links

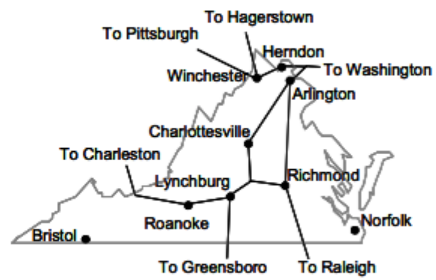
Examples of Maps Used

The Physical Internet: Links

- Step #1: Identification
  - Utilize *search* to find maps of physical locations
- Step #2: Transcription
  - Begin with maps of ISPs that are geocoded
  - Add links of maps that are not geocoded
- Step #3: Verification
  - Check consistency with <u>public</u> records of rights of way (ROW), etc.
- Step #4: Infer conduit sharing

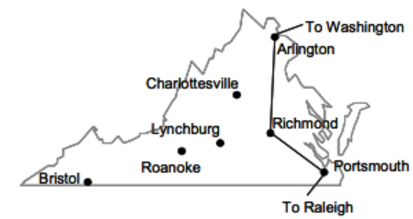
Consistency Checks 1

AT&T	
Address:	13630 Solstice Street Midlothian VA 23113
Telephone:	804-897-1734
Contact Person:	Chester Porter
Title:	Client Business Manager for VA
e-mail:	cdporter@att.com
Internet URL:	www.att.com
Offering:	"Full range of voice and data services, IT and professional services"



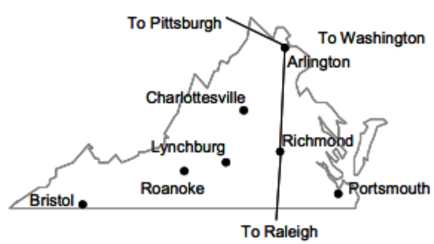
Source: KMI Corporation, Sept '01, www.kmicorp.com

Qwest	
Address:	1306 Concourse Drive Suite 400 Linthicum MD 21090
Telephone:	410-694-4848
Contact Person:	Joel Prescott
Title:	National Account Manager
e-mail:	Joel.prescott@qwest.com
Internet URL:	www.qwest.com
Offering:	"Private line services, Internet, collocation, fiber leasing, engineering, construction, hosting, VPNs"



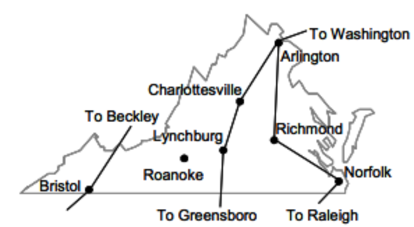
Source: KMI Corporation, Sept '01, www.kmicorp.com

Level 3	
Address:	8270 Greensboro Drive Suite 900 McLean VA 22102
Telephone:	571-382-7427
Contact Person:	Laura Spining
Title:	Account Director
e-mail:	Laura.spining@level3.com
Internet URL:	www.level3.com
Offering:	"Private line transport services, optical waves, managed services for construction, engineering, fiber leasing, collocation, MPLS transport product"



Source: KMI Corporation, Sept '01, www.kmicorp.com

Worldcom	
Address:	4951 Lake Brooke Drive Glen Allen VA 23060
Telephone:	804-527-6338
Contact Person:	Jim Nystrom
Title:	Director
e-mail:	Jim.nystrom@wcom.com
Internet URL:	www.wcom.com
Offering:	"Full array of voice and data services including private line, frame relay, ATM, Internet, Network Engineering and Managed Services, Worldcom is currently the enterprise service provider for the Commonwealth of Virginia including agencies, local and county government"



Source: KMI Corporation, Sept '01, www.kmicorp.com

Consistency Checks 2

AGREEMENT FOR THE LEASE OF CITY CONDUIT

and

LEASE OF THE PUBLIC RIGHT-OF-WAY FOR INSTALLATION OF CONDUIT AND FIBER OPTIC CABLE

between

THE CITY OF BOULDER AND ZAYO GROUP, LLC

This AGREEMENT FOR THE LEASE OF CITY CONDUIT AND LEASE ON THE PUBLIC RIGHT-OF-WAY FOR INSTALLATION OF CONDUIT AND FIBER OPTIC CABLE (this "Agreement") is made and entered into by and between the City of Boulder, Colorado (the "City") and Zayo Group, LLC, a Delaware limited liability corporation ("Zayo"). The City and Zayo may hereinafter be referred to individually as a "Party" or collectively as the "Parties."

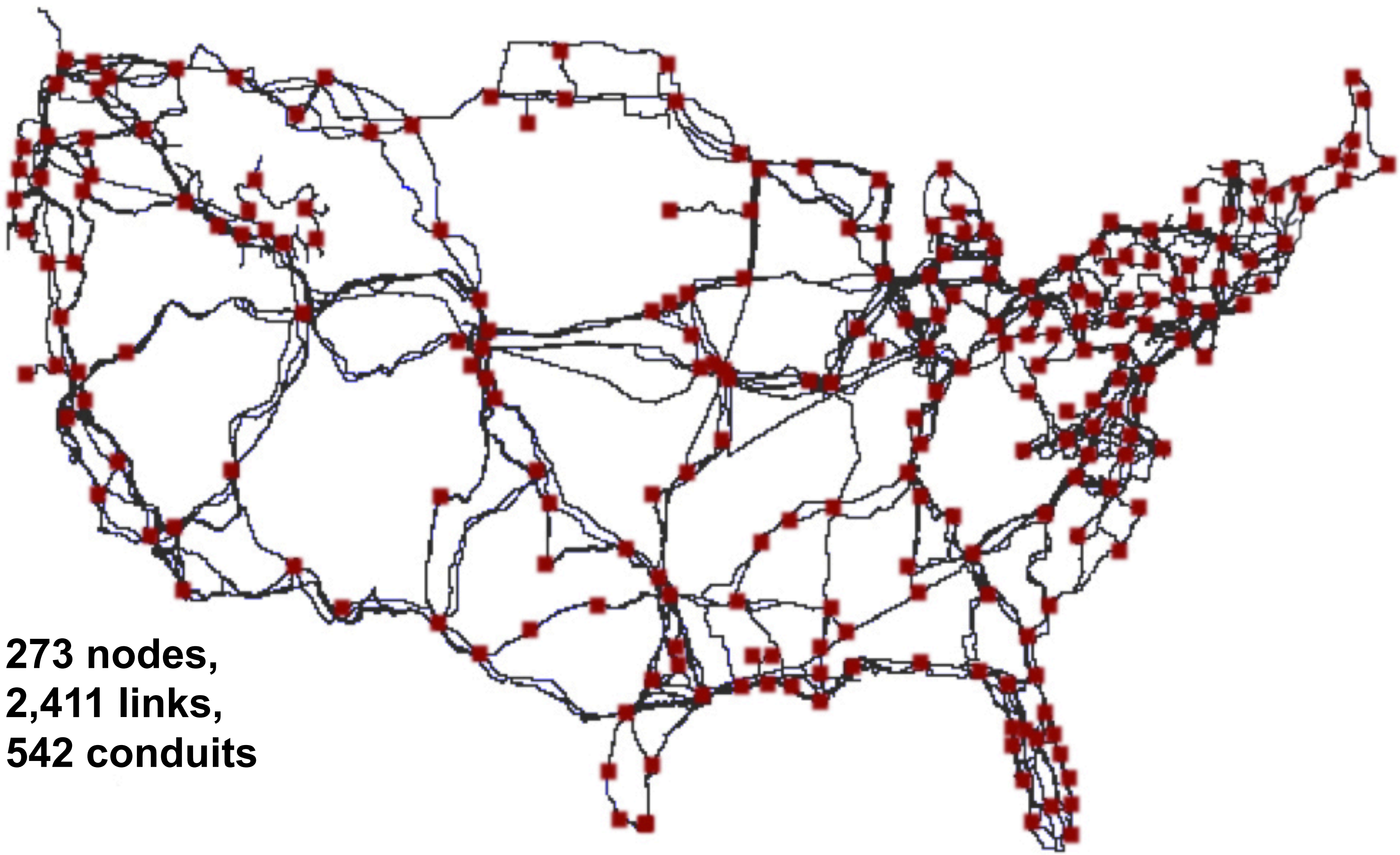
RECITALS

A. Zayo is a provider of telecommunications service, as defined in C.R.S. § 40-15-102, and, as such, holds a statewide franchise for the use of public rights-of-way pursuant to C.R.S. § 38-5.5-103 *et seq.*.

B. Zayo owns, operates and maintains metro fiber networks in multiple Colorado cities and desires to build a fiber optic network within Boulder to (i) serve large industrial, commercial and governmental clients within Boulder and (ii) connect to other municipalities along the Colorado Front Range and beyond. In order to accomplish this, Zayo wishes to lease unused conduit from the City.

C. The City owns certain underground conduit facilities, along with necessary handholes and manholes for access, located within the boundaries of the city of Boulder and depicted in red on **Exhibit A**, attached hereto and incorporated herein by this reference (the "City Duct System"). The City Duct System, which is 131,322 feet long, consists of as few as one and as many as four separate, but co-located, conduits that are typically used for routing wiring or fiber optic cable ("City Conduit").

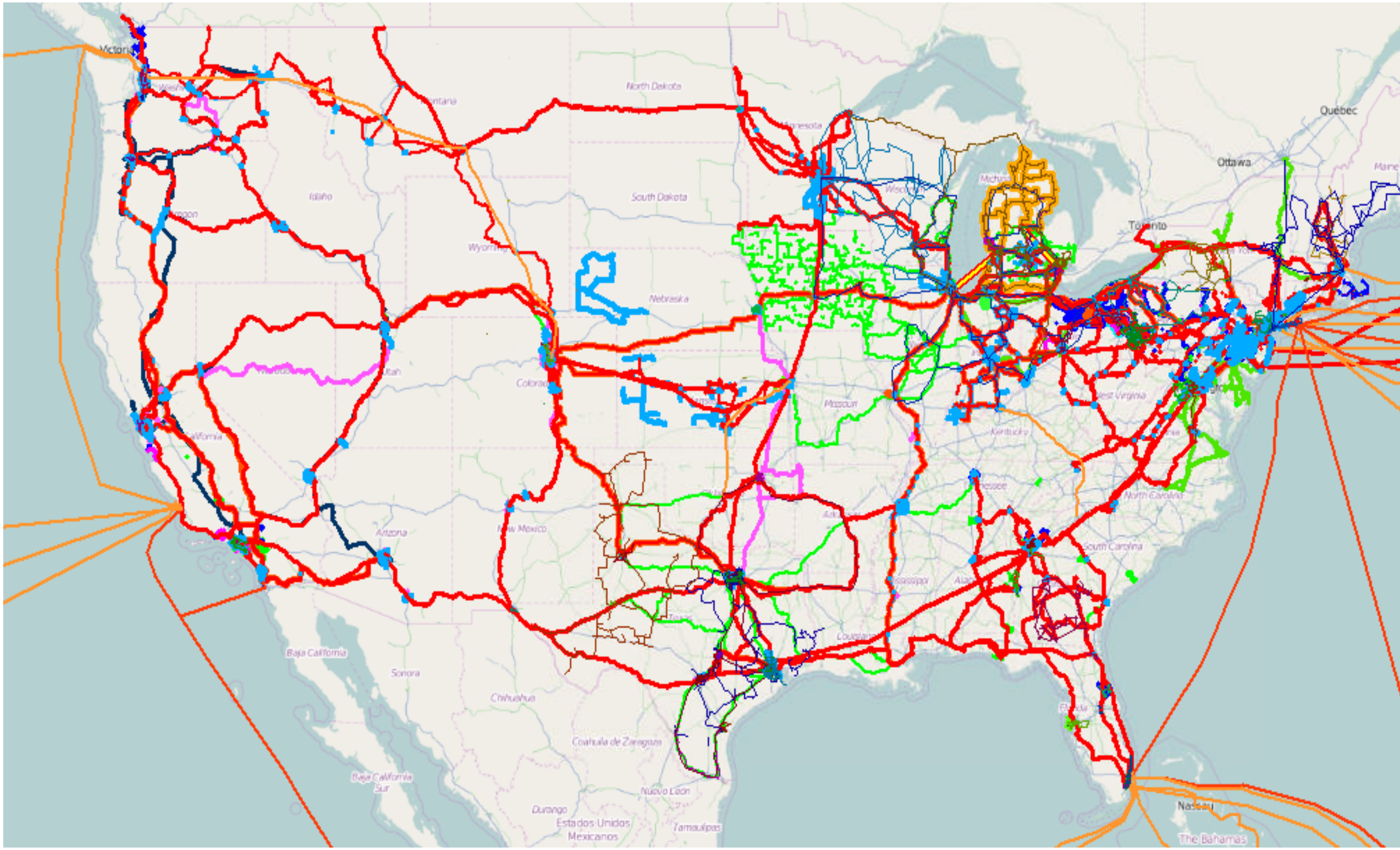
US Long-haul Infrastructure



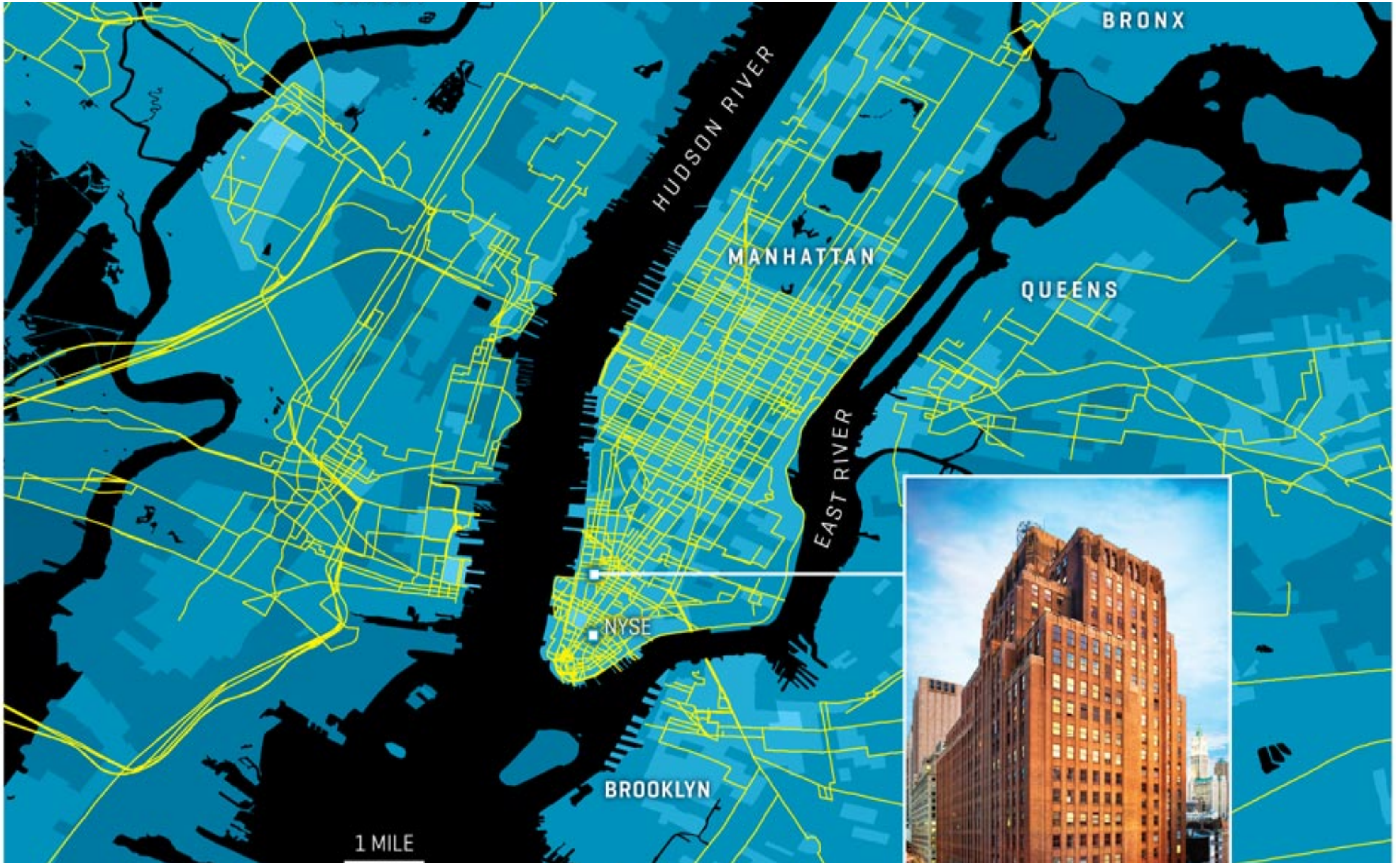
273 nodes,
2,411 links,
542 conduits

Some Missing Pieces …

Missing 1: Metro Fiber Maps

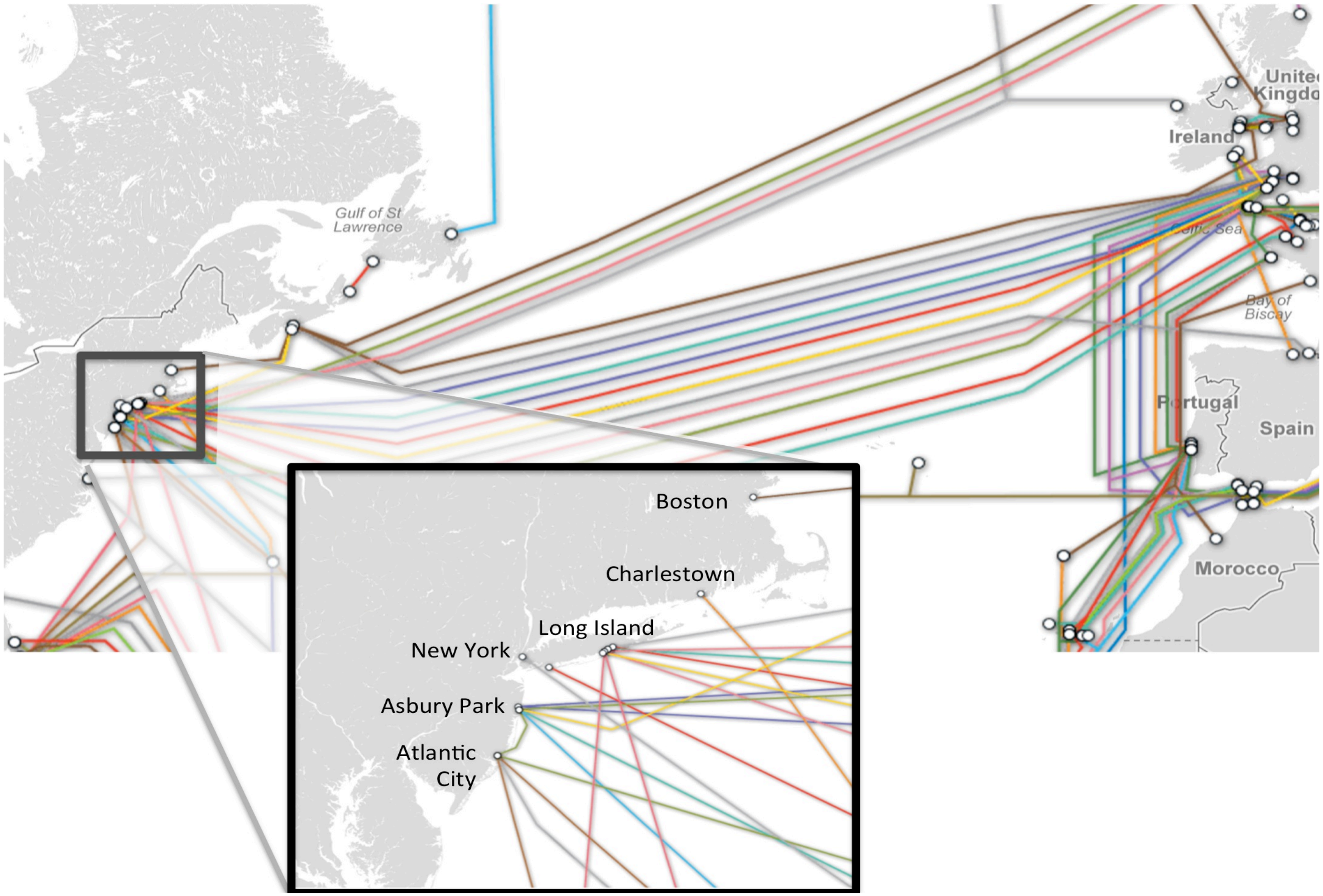


Example: NYC Metro Fiber



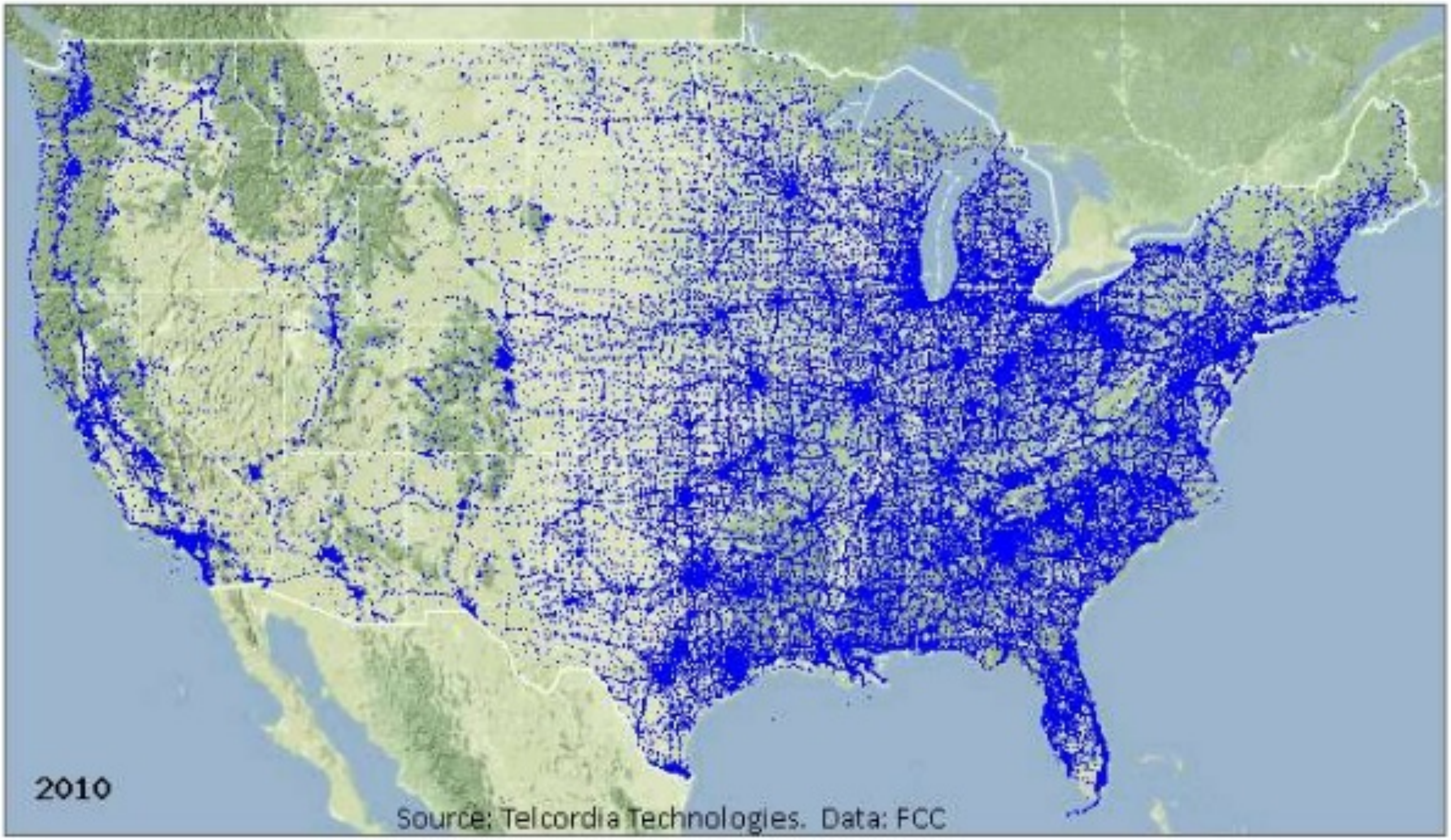
Source: http://ny.curbed.com/2012/7/17/10351100/mapping-manhattans-internet-with-underground-fiber-optics

Missing 2: Undersea Cables



Source: https://www.telegeography.com/telecom-resources/submarine-cable-map/

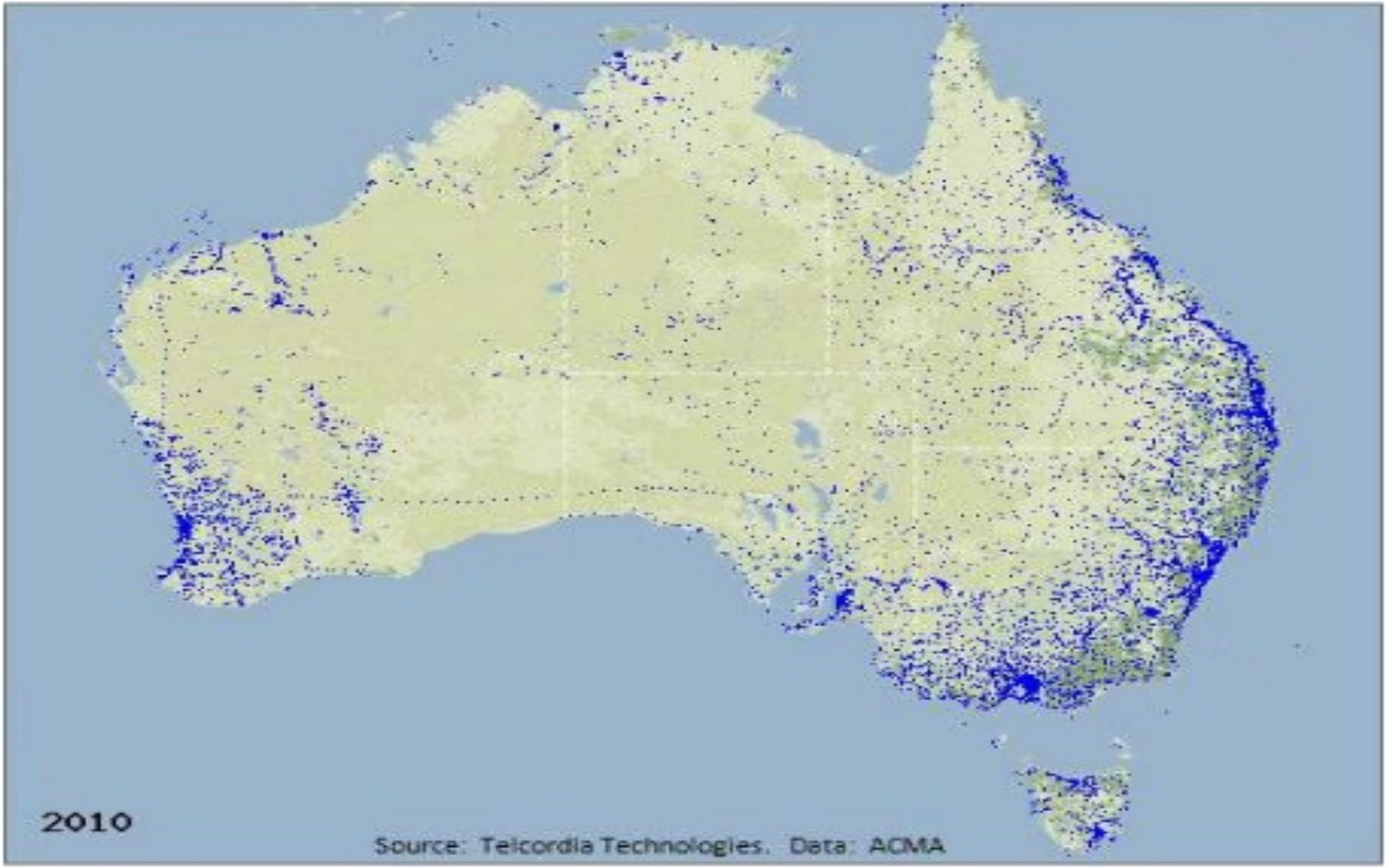
Missing 3: Cell Towers (US)



2010

Source: Telcordia Technologies, 2010

Missing 3: Cell Towers (Australia)



2010

Some Questions of Interest

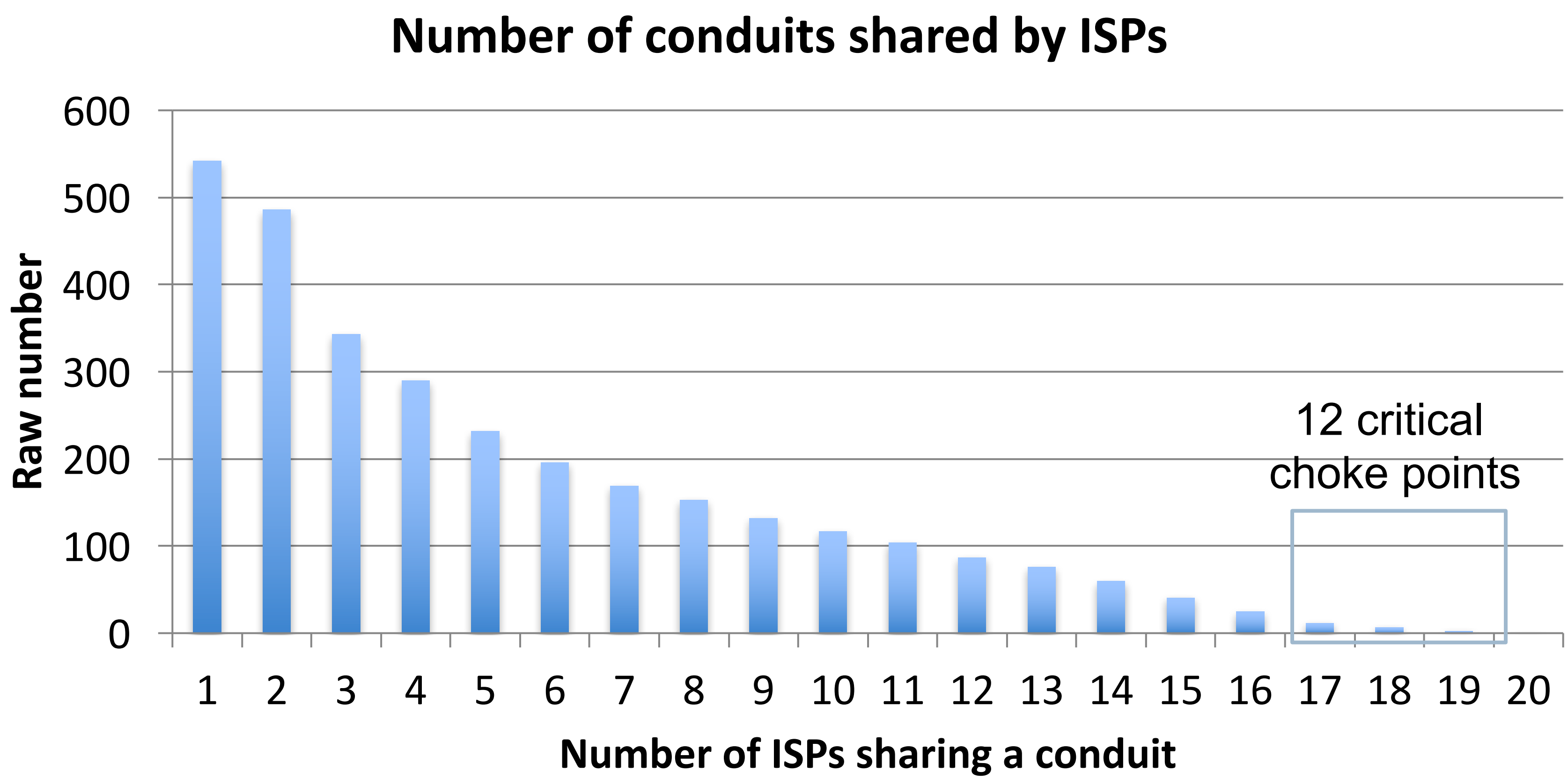
Q1: Assessing Shared Risk

- Striking characteristic of the constructed map is the amount of *conduit sharing*
- Analyze shared risk using risk matrix

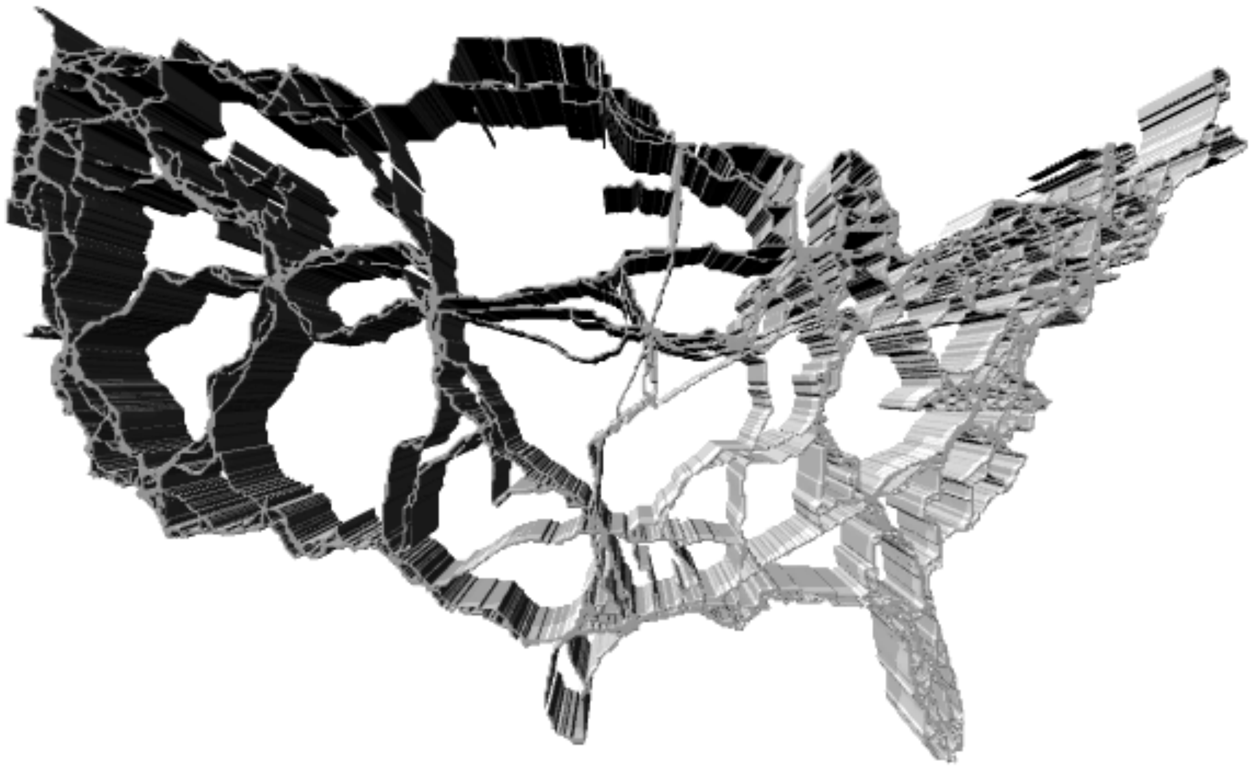
	c1	c2	c3
Level 3	2	2	1
Sprint	2	2	0

- Notions of shared risk
  - Connectivity only
  - Connectivity plus inferred traffic

Connectivity-only Risk

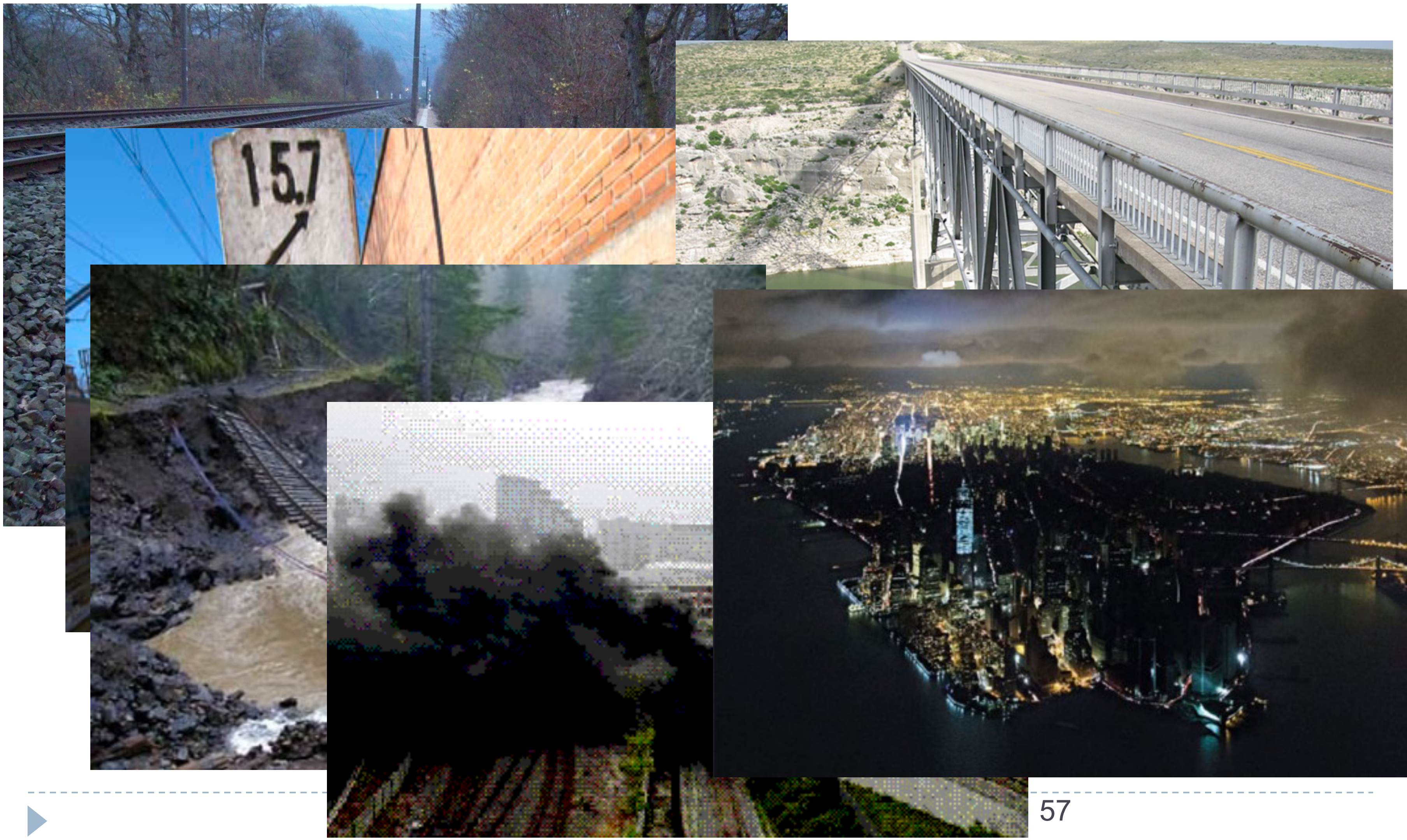


Connectivity plus Inferred Traffic

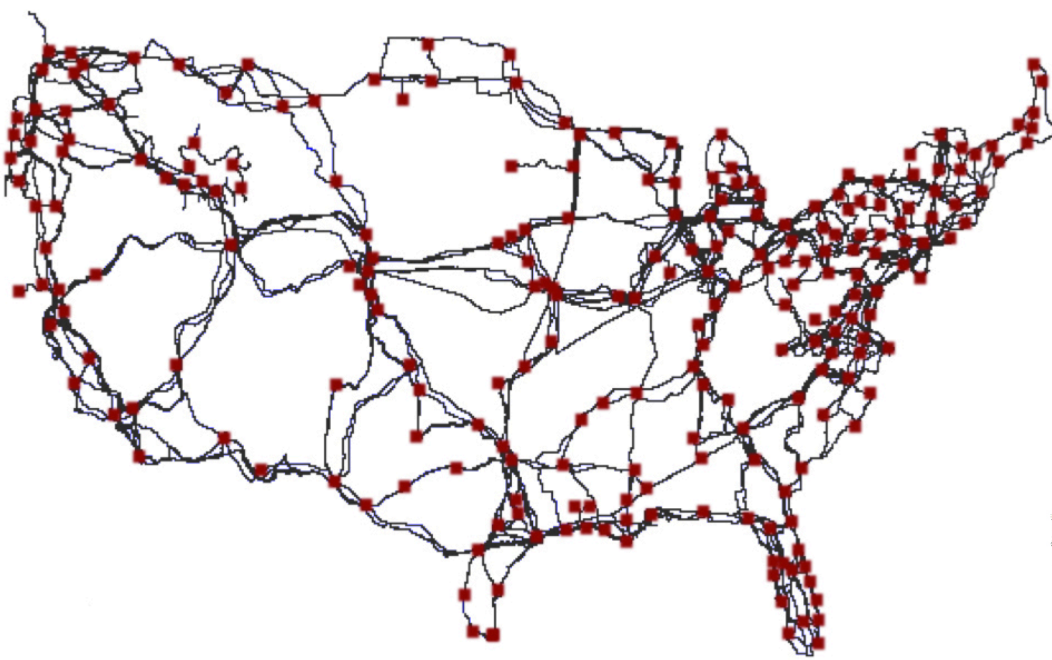


Dataset: Ono (BitTorrent clients) from Jan. 01, 2014 to Mar. 31, 2014;
Thickness number of probes traversing a conduit
Color number of ISPs sharing the conduits

Q2: Colocation With Other Infrastructure



Q2: Colocation With Other Infrastructure



Railway infrastructure

Roadway infrastructure

Improving Infrastructure

- We show that robustness and performance can be improved by adding just a few links in strategic places
  - Gain robustness to outages by reducing sharing
  - Better performance by minimizing propagation delay
  - Add new conduits or add new peers

- How to get there?
  - Regulation (e.g., Title II) may achieve the opposite?
  - Market forces (e.g., robustness as a competitive advantage)

An Observation …

- The physical Internet is resilient …
  - TCP/IP was designed so that the Internet can "live with" failures and "work/route around" them
  - TCP/IP allows for graceful degradation under failure while maintaining/providing basic services
- ... but it helps to understand its "weak spots"
  - Where would more redundancy be beneficial?
  - Where would more (physical) security pay off?
  - Redundancy in view of prevailing market forces vs regulations

… and Reminder …

A bad actor whose objective is to do maximum damage to an industry/country/society relies critically on a <u>fully functioning physical Internet infrastructure</u> to reach the intended victims and harm them

… and the $100M(?) Question:

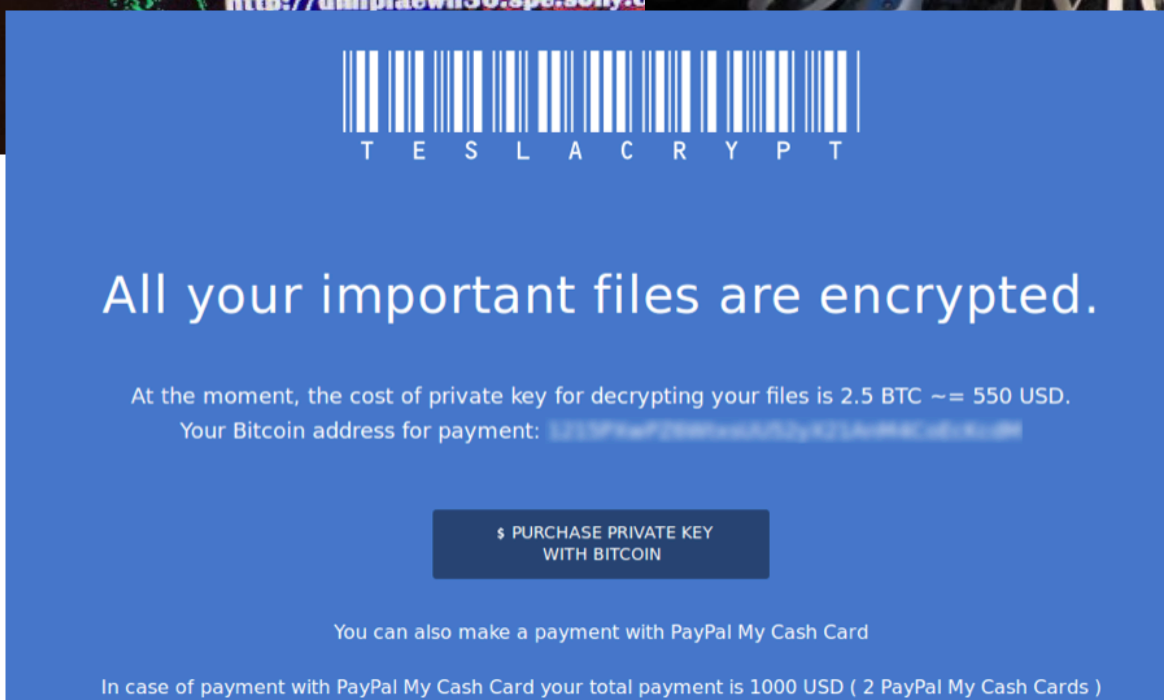
- Secure the physical Internet infrastructure?
  - Submarine cable, landing stations
  - Colocation facilities, data centers
  - Long-haul fiber optic cables, cell towers, …
- Secure the logical Internet infrastructure?
  - IP (BGP hijacking)
  - TCP (low-volume DDoS)
  - SCADA protocols (corrupting power grid, gas supply, …)

For the Good of the Internet – Cyber Security

Cyber Security: Today's Approach

- All security solutions filter incoming/outgoing traffic and only see/keep a small portion of the total traffic
- Without the complete traffic, (after-the-fact) intrusion reconstruction, network forensics, and/or (real-time) attack detection/mitigation are in general impossible to perform
- As a result, the mean dwell time (i.e., amount of time an attacker can roam around in the compromised network without being detected/discovered) is about 200 days!
- This is a main reason for why we keep seeing more and more severe types of attacks by more types of different bad actors


Hacked
Warning :
We've already warned you, and this is ju
We continue till our request be met.
We've obtained all your internal data inc
If you don't obey us, we'll release data s
Determine what will you do till November
Data Link :
https://www.sonypicturesstock
http://dmiplaewh36.spe.sony.c

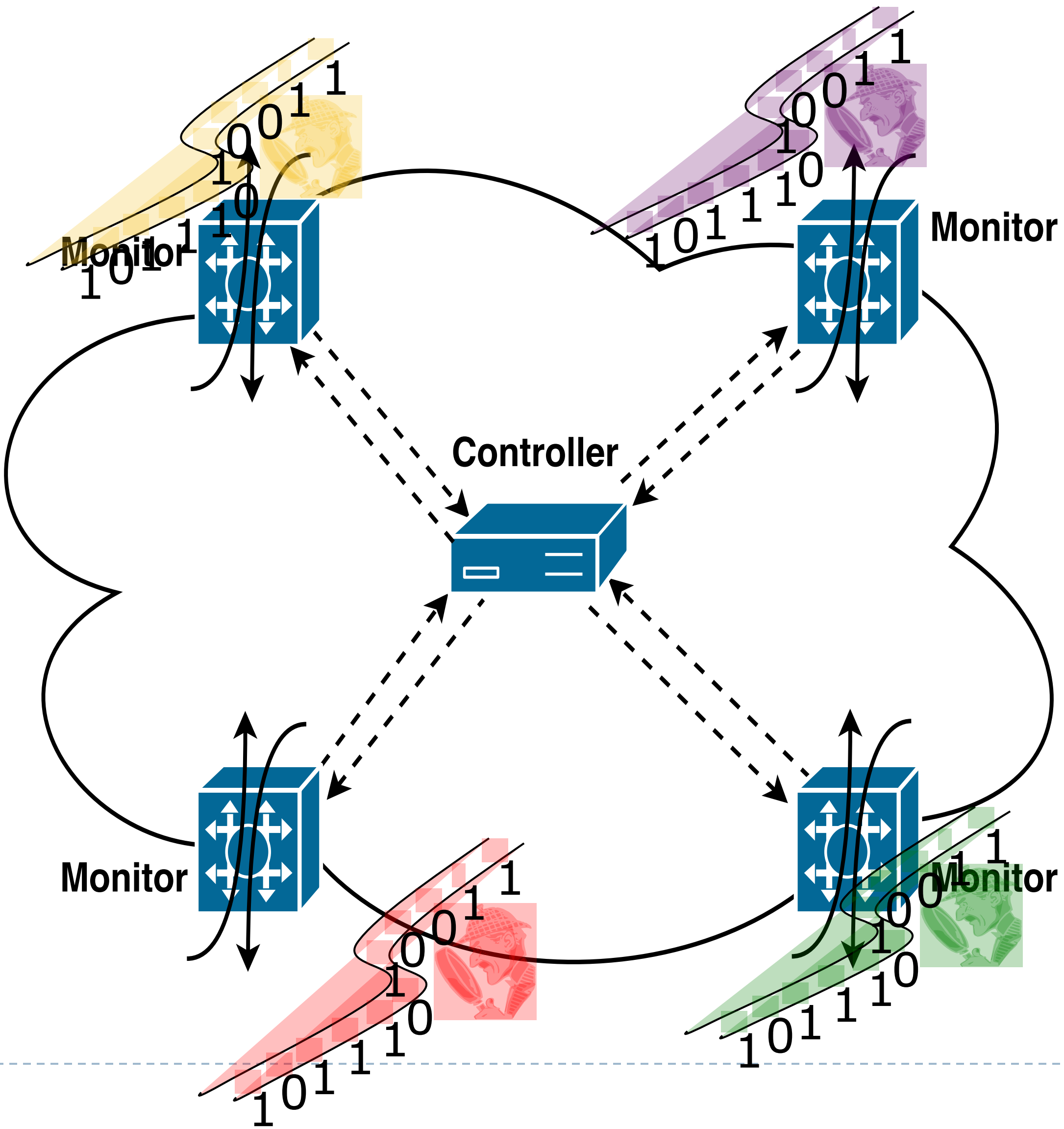
JPMORGAN CHASE & CO.

T E S L A C R Y P T
All your important files are encrypted.
At the moment, the cost of private key for decrypting your files is 2.5 BTC ~= 550 USD.
Your Bitcoin address for payment:
$ PURCHASE PRIVATE KEY WITH BITCOIN
You can also make a payment with PayPal My Cash Card
In case of payment with PayPal My Cash Card your total payment is 1000 USD (2 PayPal My Cash Cards)

nk cyber-
etected by

Cyber Security: Tomorrow’s Data

- A (the?) solution to today’s problem:
  - “All packets, all the time!”
  - Capture every packet that enters or leaves your network
  - NIKSUN’s industry-leading technology enables this solution at scale (up to 100 Gbps and beyond)
- A new type of “big (Internet) data”
  - “All packets, all the time” results in genuine instances of “big data”
  - The resulting “big data” is of the streaming type (i.e., dynamic)!
  - The resulting “big data” is in addition distributed!

Cyber Security: Tomorrow's Setup



Cyber Security: Tomorrow's Approach

- Basic requirements
  - No moving of "big streaming data" from remote to central node
  - No multiple passes over "big streaming data" at remote nodes
  - "Beefy" (i.e., resource-rich) remote nodes
  - "Command & Control"-like communication structure

- Basic approach
  - Develop effective and efficient techniques for mining "big data" of the distributed streaming type for the purpose of providing cyber security experts with powerful new tools for securing tomorrow's cyberspace

Cyber Security: Tomorrow's Research Needs

- Algorithms research
  - Development of new distributed streaming data algorithms
- Database research
  - Design of query processing engine in conjunction with appropriate streaming data processing platform
- Networking research
  - Systems support (using SDN) for (close-to) real-time detection and mitigation of known types of attacks and continuous acquisition of intelligence about new types of attacks

Some Initial Results

- Joint work with A. Gupta, N. Feamster, J. Rexford, R. Harrison (Princeton University), R. Birkner (ETH Zürich), M. Canini (UC Louvain), C. Mac-Stoker (NIKSUN, Inc.)
- *Network monitoring is a streaming analytics problem* appeared in: ACM HotNets 2016
- *Sonata: Query-Driven Streaming Network Telemetry* sonata.cs.princeton.edu

Thank you!

Questions?