renesys

The Internet Intelligence Authority

Using Security Metrics to Motivate a Response to a Critical Vulnerability

aka: The Importance of Context

James Cowie, CTO

Metricon 4.0

11 April 2009

Why Do We Pursue Security Metrics?

- Because metrics simplify and make concrete things that are complex and abstract.
- Because metrics allow us to **rank** different groups or approaches and **identify outliers** (the very bad)
- Because metrics make people take action, in ways that more complex arguments or threats do not
- **Because we want people to change their behavior**

How do we make people change their behavior?

- **Easy.**
- When there's a critical **operational** issue with **security** implications, we're justified in deploying metrics that cut straight to base emotions: **Fear and Shame.**

Smell something burning?
...Yeah, that's the context.

- Every organization owes its Internet connectivity to one protocol: BGP4. **There are no alternatives**.
- BGP4 has longstanding problems that **cannot be fixed,** and can only be monitored carefully.

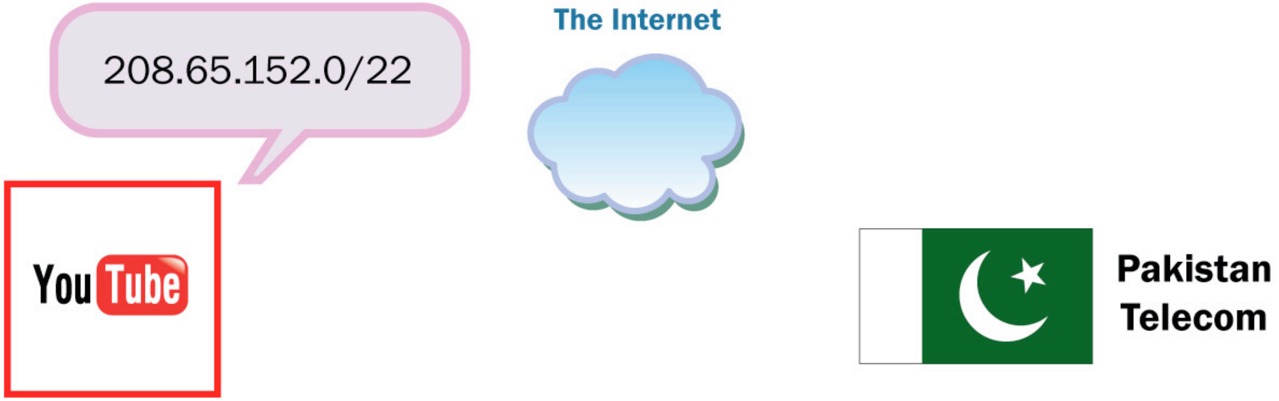
1) Everyone is exposed to various Internet routing vulnerabilities:
   - **downtime & instability, hijacking,wholesale traffic interception**.
   - **Risks: how much does leaving the Internet cost your enterprise per hour? Having your customers' traffic silently intercepted?**
2) Very few people understand these risks, so they are not being **measured** or **managed** appropriately. No one is covering your back!

Key to routing vulnerabilities

- No single authoritative source of who should be doing what.
- All routing is based on *trust* and *cooperation*.
  - Neighboring routers typically trust each other.
  - Traffic is assumed to flow unimpeded. Global connectivity!
- No requirements around physical redundancy.
- No mechanism in place to handle those who go ***rogue***. There are no Internet police!

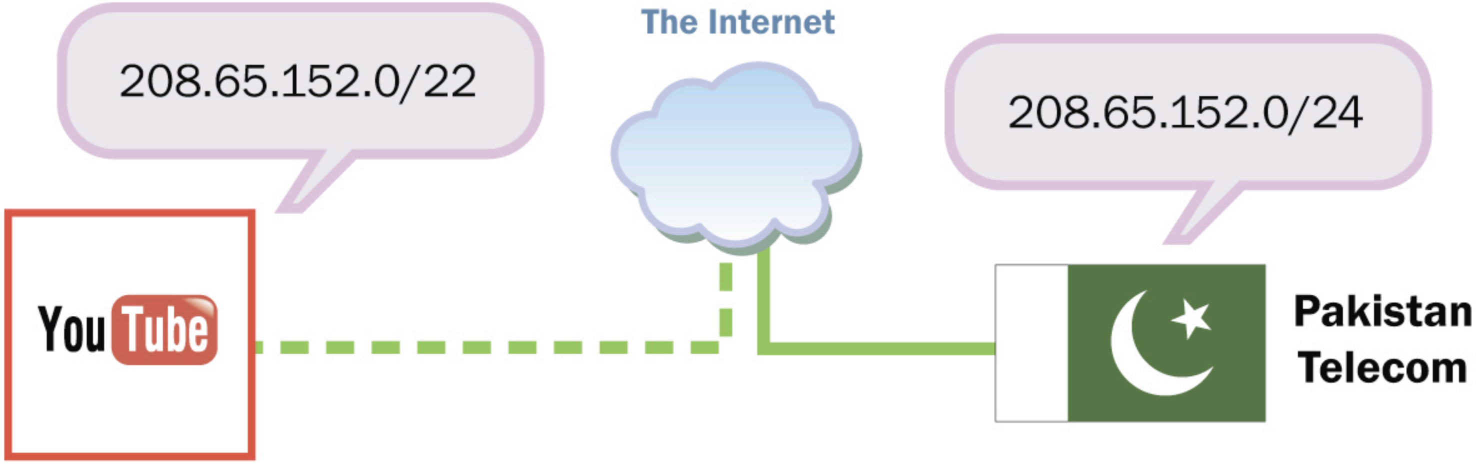
Hijacking Used Space – YouTube: Feb ’08

- YouTube owns 208.65.152.0/22
  - This contains the more-specific 208.65.153.0/24
  - The above /24 *used* to contain all of YouTube’s
    - DNS Servers (have since moved)
    - Web Servers (have since added additional IP space)
  - YouTube announced only the /22



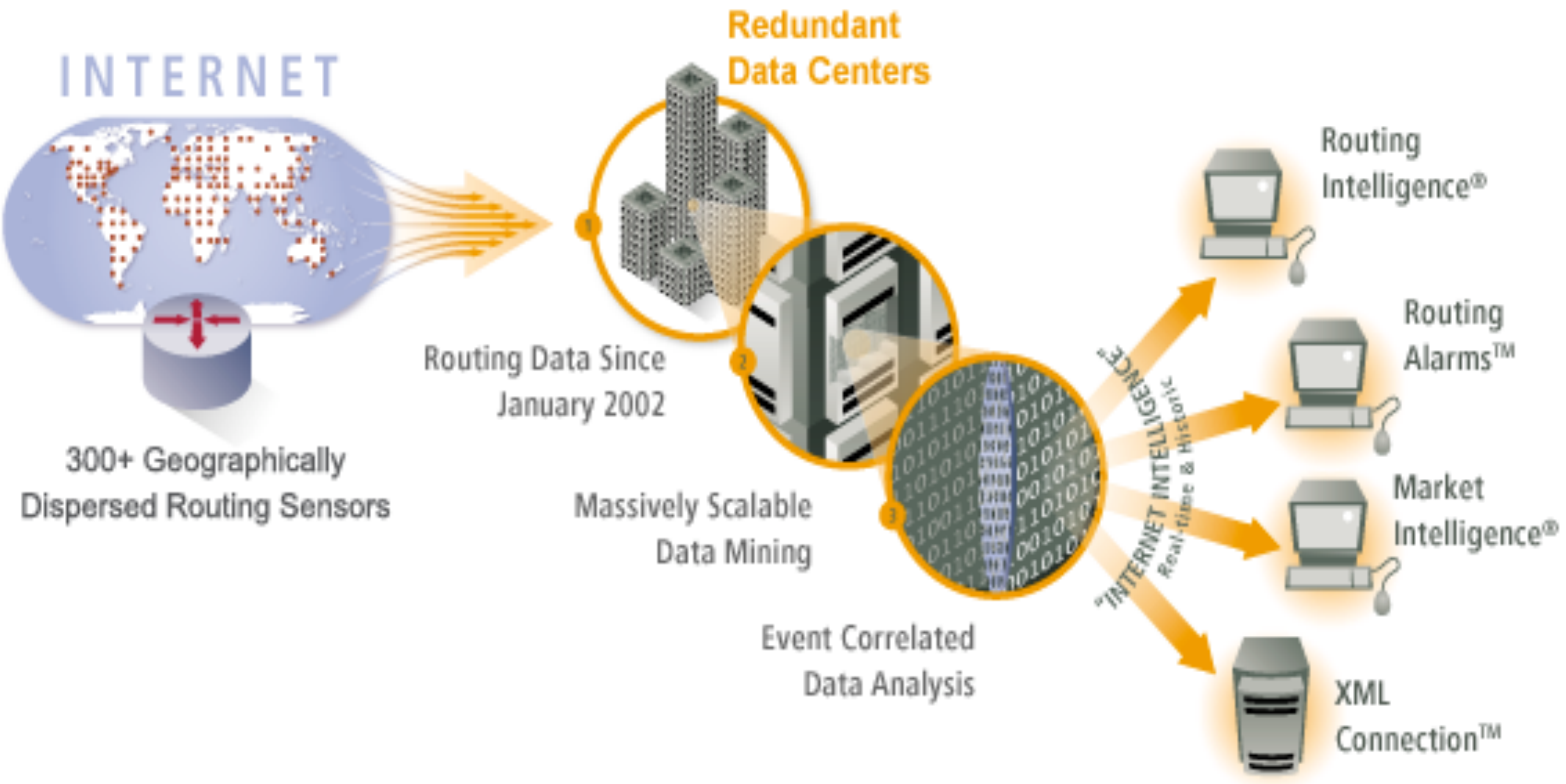
Hijacking Used Space – YouTube: Feb '08

– Pakistan Telecom announces the /24
  - In BGP, most specific route to an IP address wins!
  - Pakistan Telecom gets all traffic intended for YouTube
  - YouTube is globally unreachable for 2 hours



renesys

Renesys Studies Routing Relationships



Three Security Metrics for Routing

- **Compliance, Availability, Diversity**

- Organizations that measure these and change their behavior in response to them are dramatically less likely to be the target of successful routing attacks.
- You can't secure what you don't understand.
- “Living clean” and being consistent is the key to detecting and mitigating routing attacks

renesys

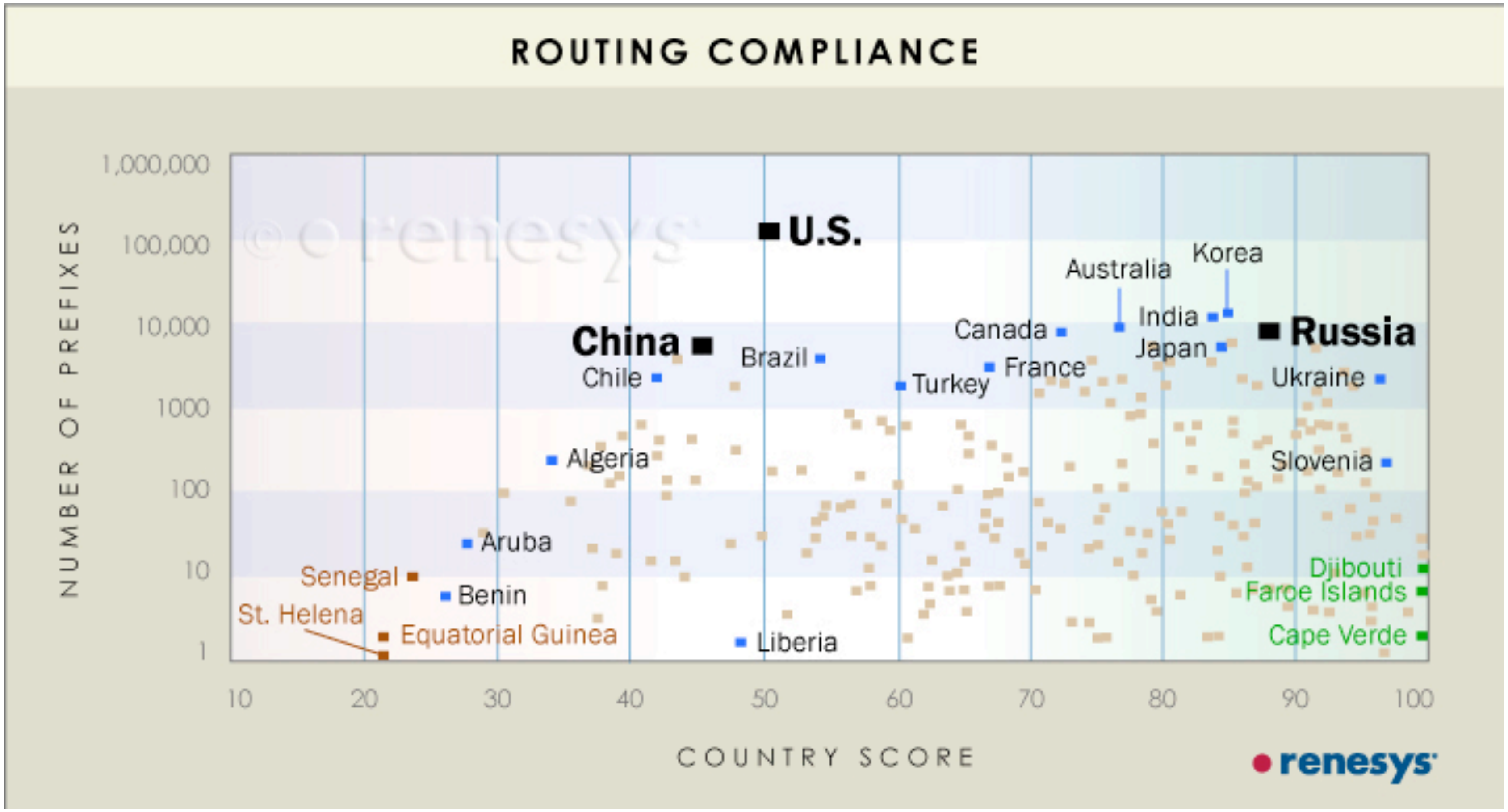
Compliance – Required for accountability

- Third-party routing registries give an organization a centralized place to declare their routing policies.

- We compare *routing registries* to *observed routing*
    - Do registered origins match observed origins? (majority of score)
    - Do registered providers match observed providers?
    - Possible scores range from 0 – 100.
        - Completely correct origins and providers yields a score of 100.
        - Registering *nothing* yields score of ~ 25.
        - Numerous mismatches, score approaches zero.

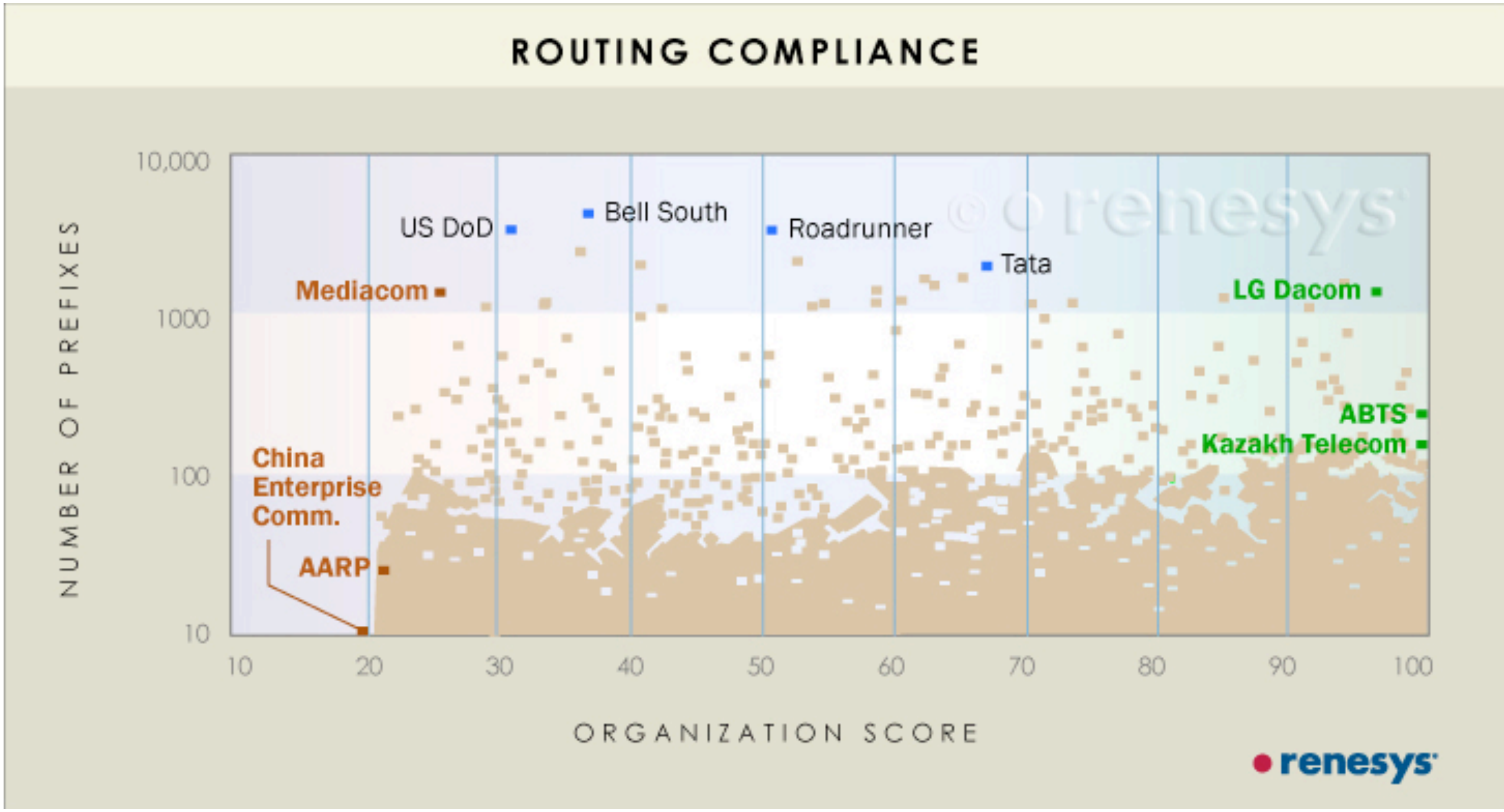
- Without knowing the correct origin for your prefixes, you have *no hope of detecting hijacks or ensuring the integrity of your Internet communications.*

Compliance Scoring by Country

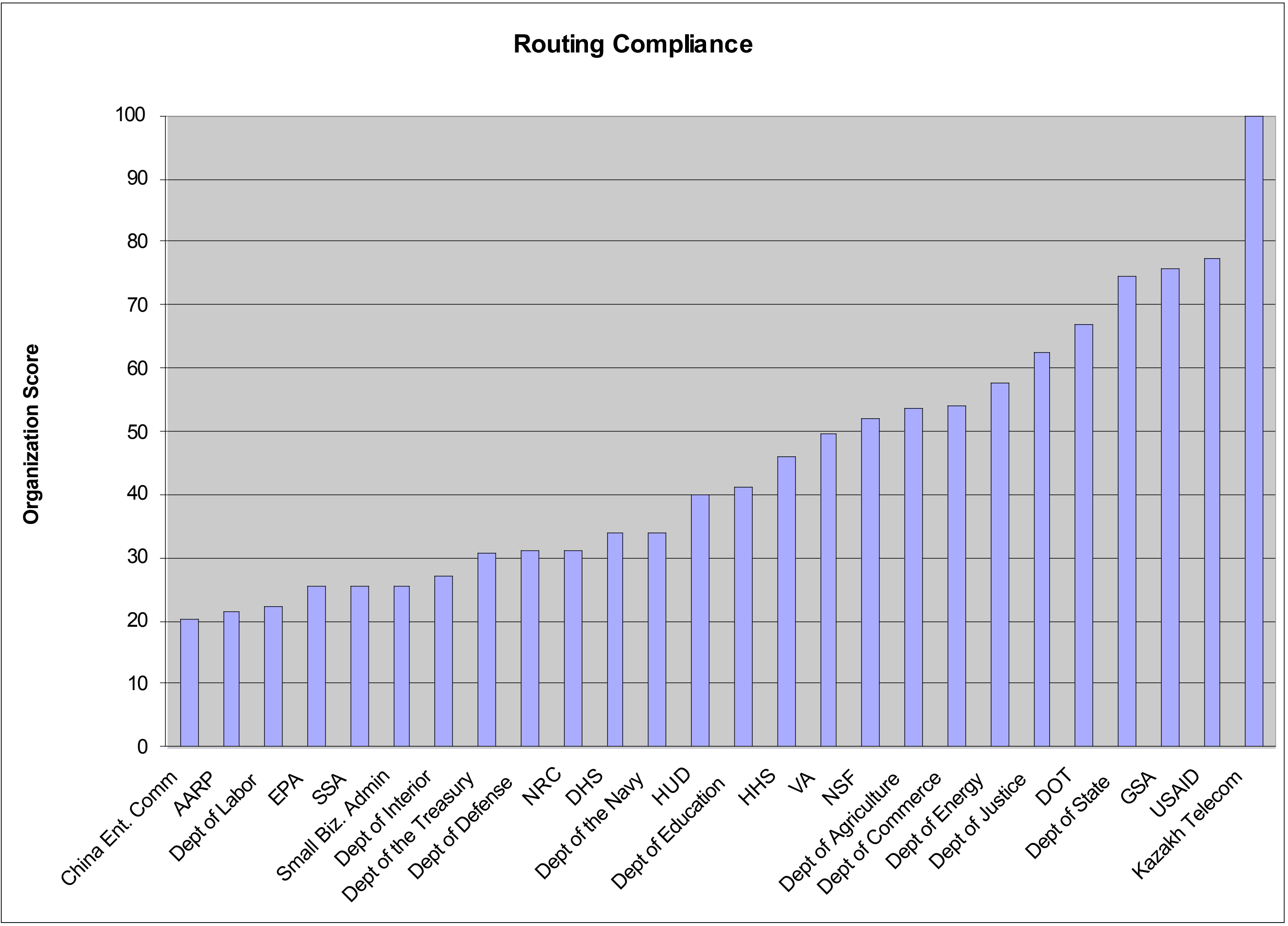


renesys

Compliance Scoring by Organization



Compliance Scoring by Agency

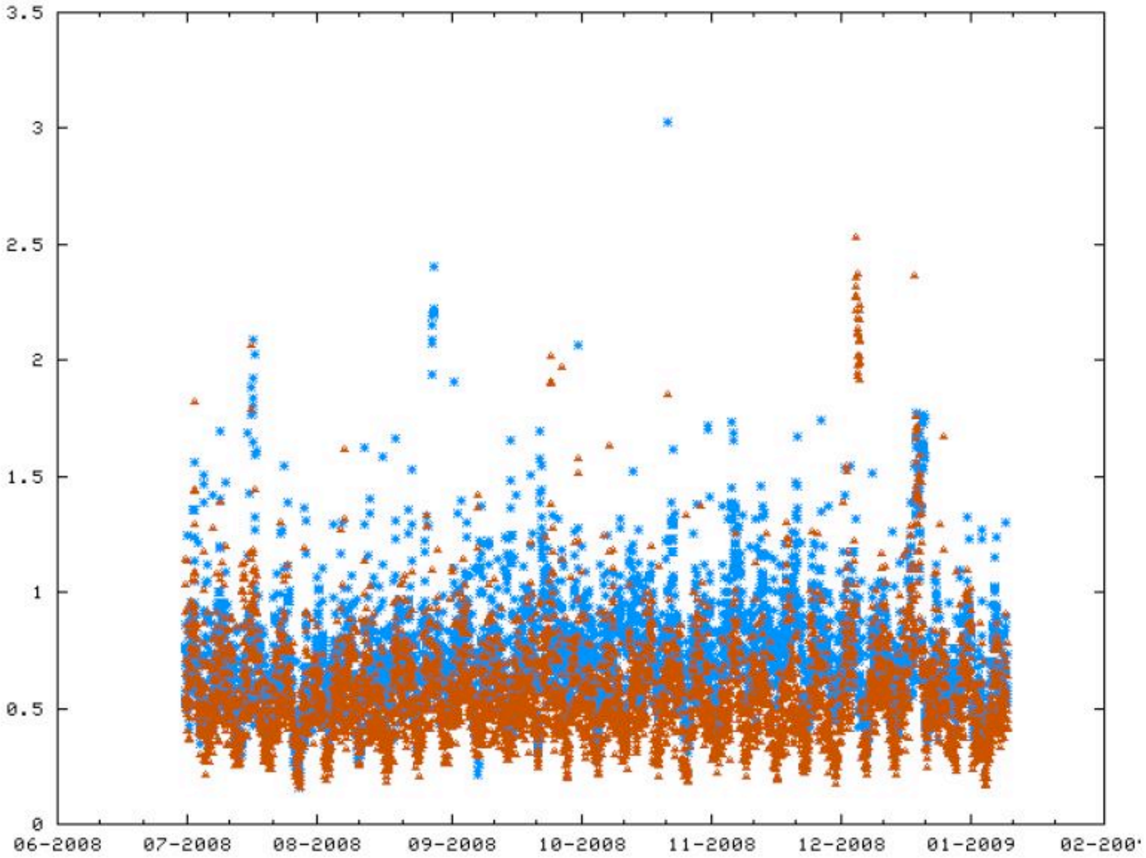


Availability – Required for Internet Access

- *Outaged* prefixes cannot be reached.
- *Unstable* prefixes show frequent routing changes.
  - Implies very poor connectivity, considerable packet loss
- We score organizations based on prefix availability, i.e., the absence of outages and instabilities.
  - Score range: 0 (never available) – 100 (always available)

Availability – Comparisons?

- How do customers of different providers compare?



% Unstable Prefixes:

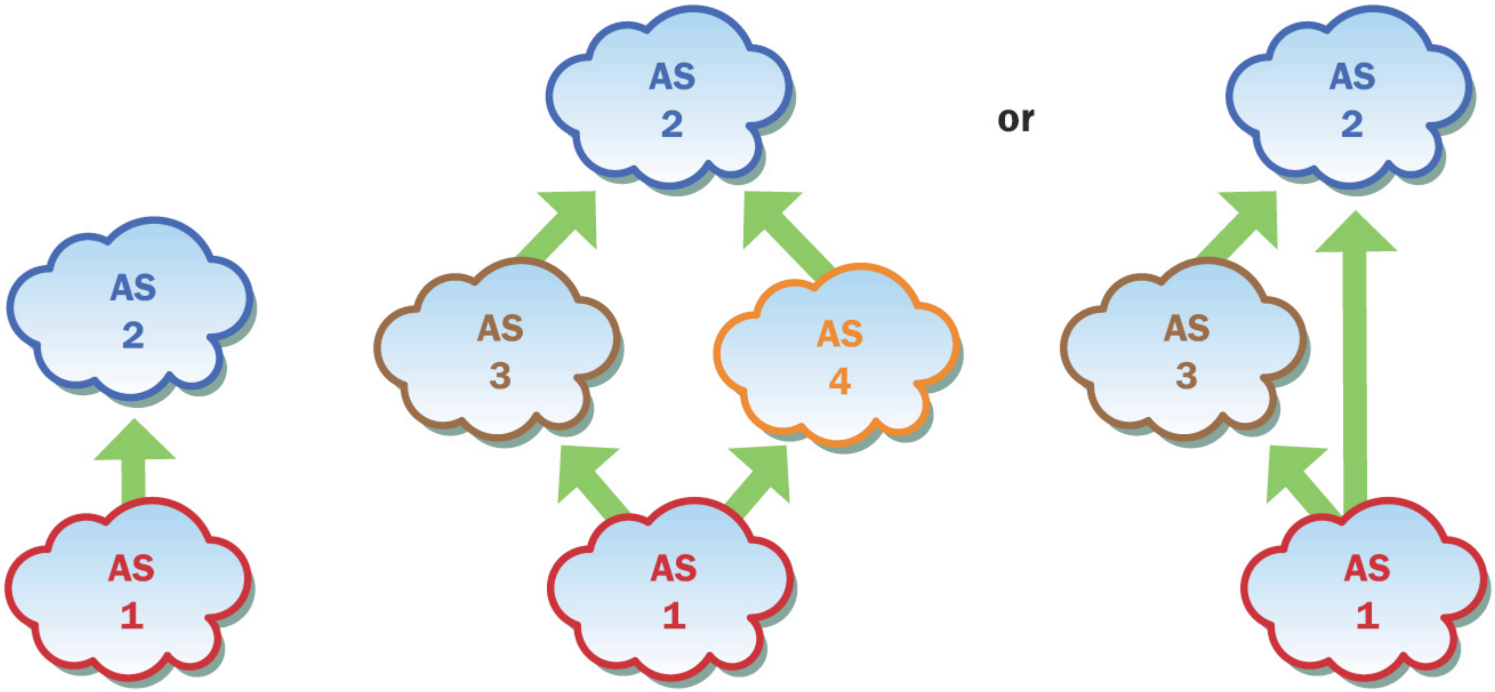
Verizon customers

Level(3) customers

Level(3) customers' prefixes are more stable and less bursty overall.

renesys

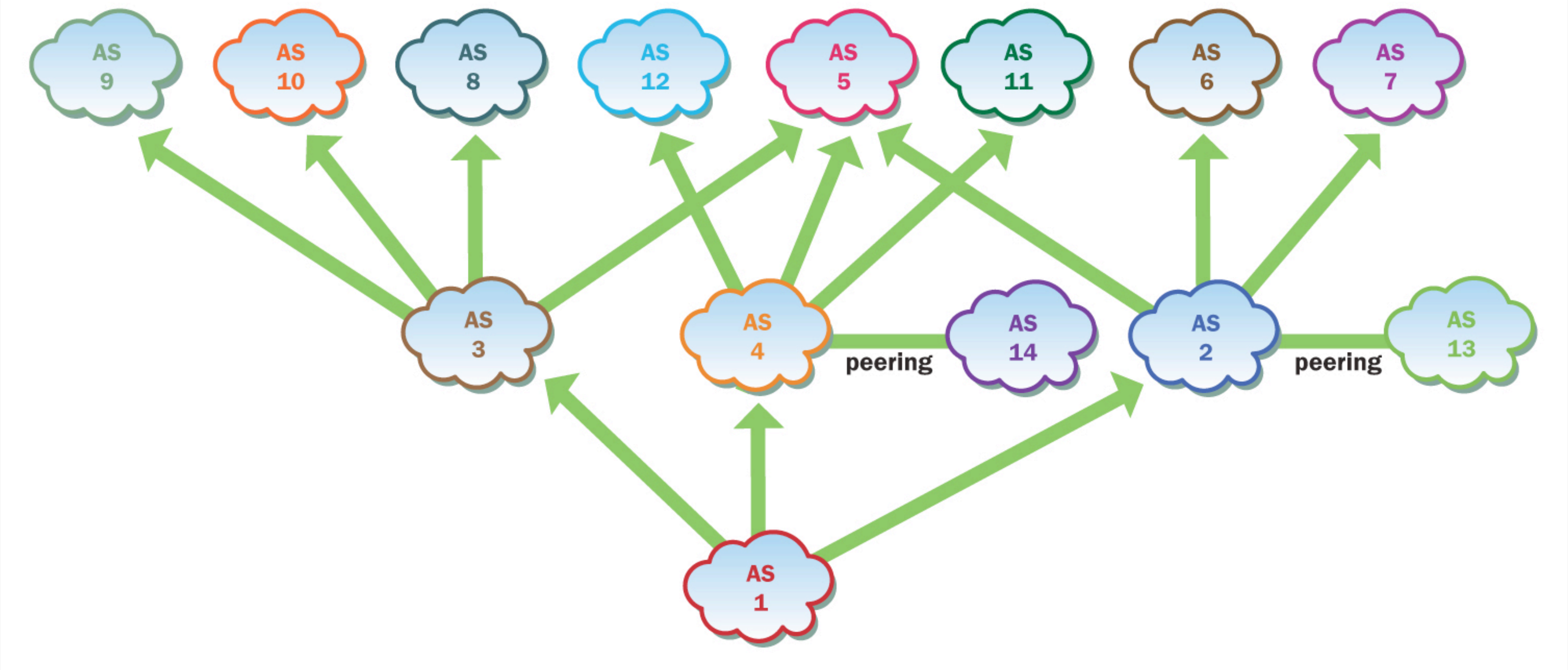
Diversity – Finding single points of failure



AS1 has only one provider **(very bad diversity)**

AS1 has two providers, but is ultimately solely dependent on **AS2 (less bad)**

Diversity – Eliminating single points of failure



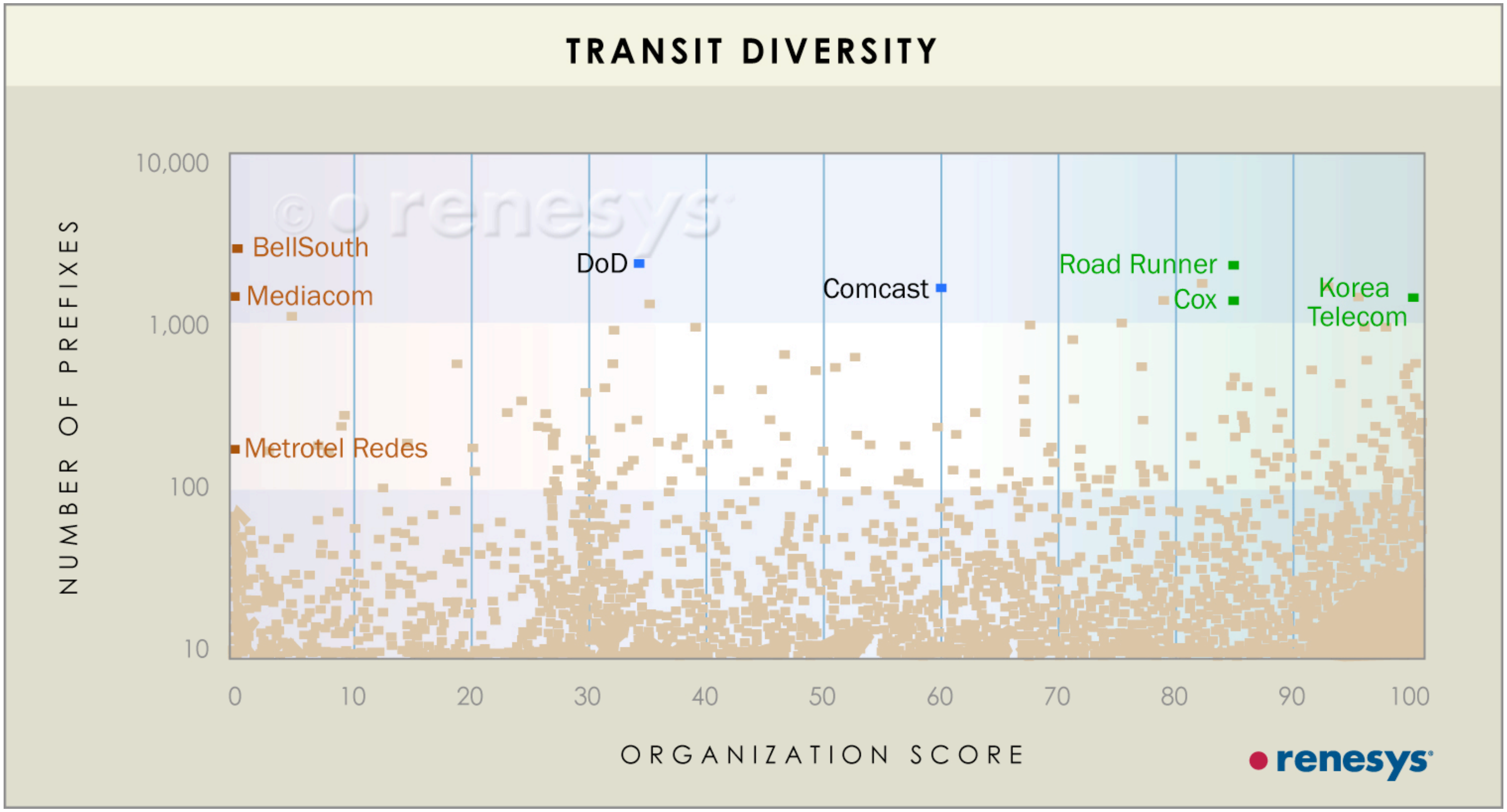
AS1 has three providers, each of which is richly interconnected to the rest of the Internet.

renesys

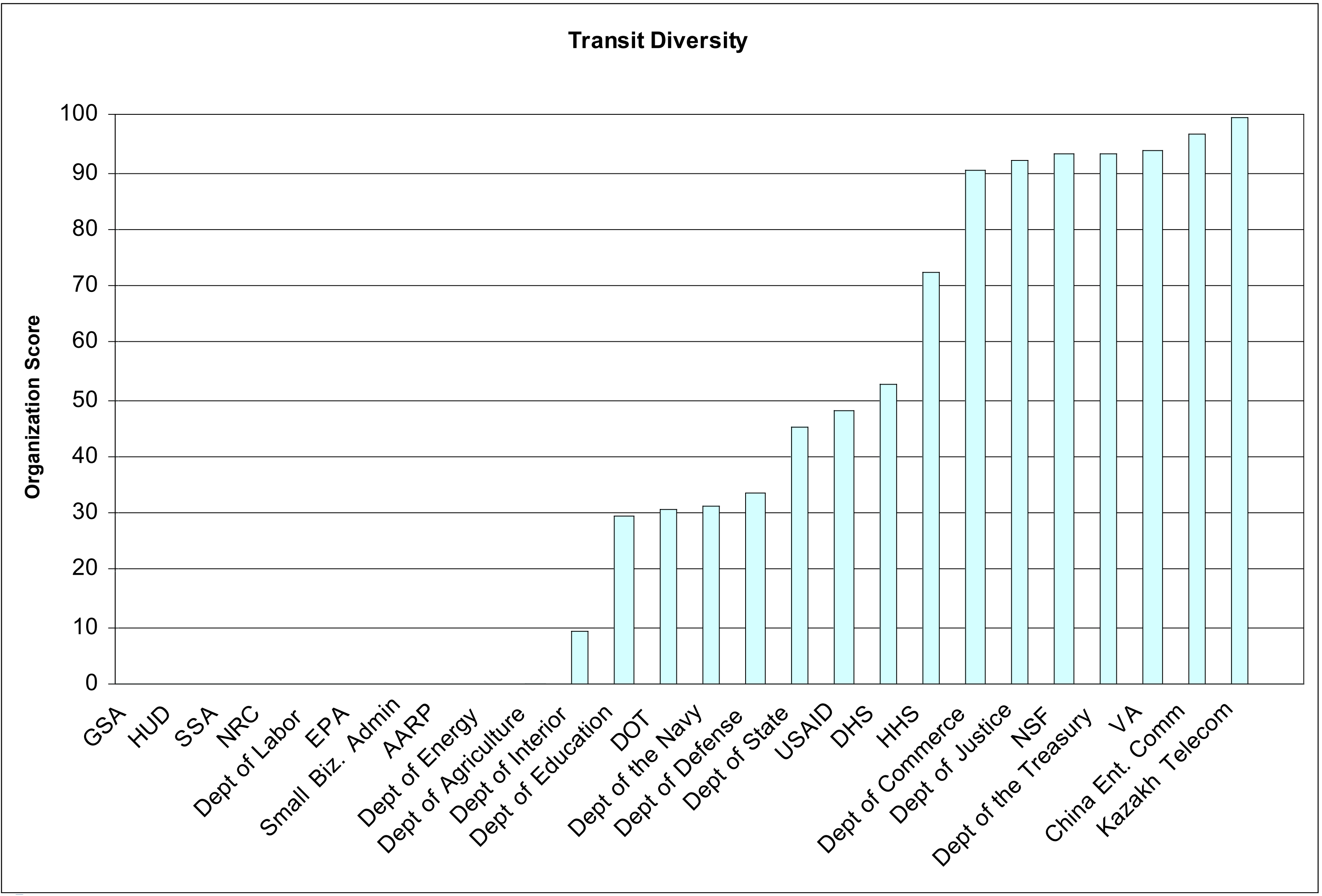
Measuring Diversity

- For each prefix …
  - How many direct providers are seen? (majority of score)
  - How many different Tier-1's ultimately provide transit?
- For each organization …
  - Average their prefix diversity scores in some way
    - Here we weight each prefix by its size
  - Composite score measures total *Internet transit diversity*
    - Score range: 0 (no diversity) – 100 (3 or more providers & Tier-1s)
  - Higher score → More diversity → Less risk

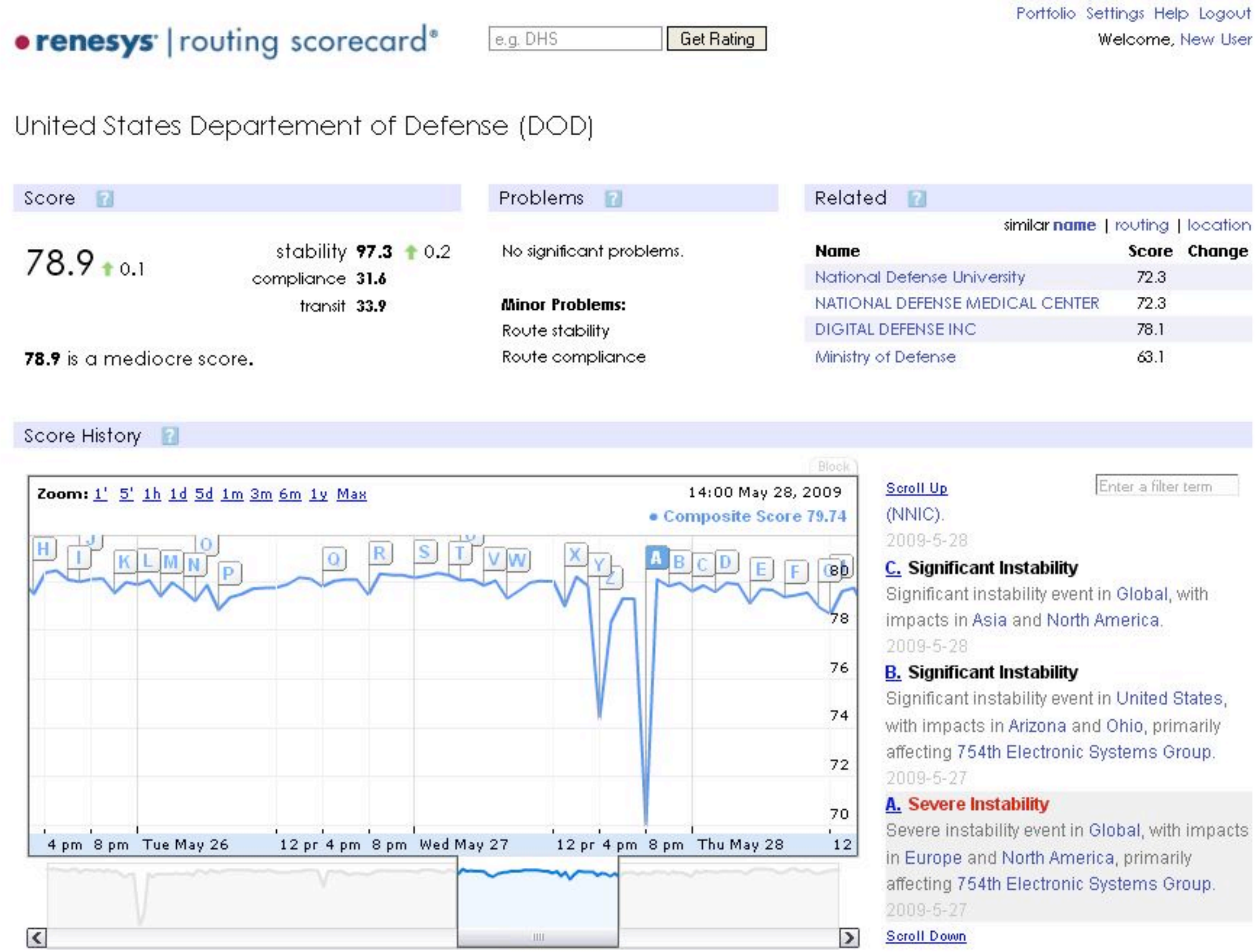
Diversity Scoring by Organization



Diversity Scoring by Agency



A Sample Scoring Application



renesys | routing scorecard®

e.g. DHS   Get Rating

Portfolio Settings Help Logout

Welcome, New User

United States Departement of Defense (DOD)

Score

78.9 ↑ 0.1

stability **97.3** ↑ 0.2
compliance **31.6**
transit **33.9**

78.9 is a mediocre score.

Problems

No significant problems.

Minor Problems:
Route stability
Route compliance

Related

similar **name** | routing | location

Name	Score	Change
National Defense University	72.3	
NATIONAL DEFENSE MEDICAL CENTER	72.3	
DIGITAL DEFENSE INC	78.1	
Ministry of Defense	63.1	

Score History

Scroll Up   Enter a filter term

(NNIC).
2009-5-28

C. Significant Instability
Significant instability event in Global, with impacts in Asia and North America.
2009-5-28

B. Significant Instability
Significant instability event in United States, with impacts in Arizona and Ohio, primarily affecting 754th Electronic Systems Group.
2009-5-27

A. Severe Instability
Severe instability event in Global, with impacts in Europe and North America, primarily affecting 754th Electronic Systems Group.
2009-5-27

Scroll Down

renesys

So *that's* why we should care.

- Routing is based on trust. BGP in the real world lacks a secure infrastructure for establishing trust.
- It falls to the participants in the routing system to watch their backs and think critically when constructing filters and policies.
- Having just **a few key metrics** that expose organizational clue levels, gives you leverage that can make key people change their behavior in ways that radically improve an organization's routing security posture.

Thanks for listening.

Jim Cowie

cowie@renesys.com

http://www.renesys.com