renesys

Critical Infrastructure: Root Server Location Analysis
NANOG 37 – San Jose, CA.

Martin Hannigan

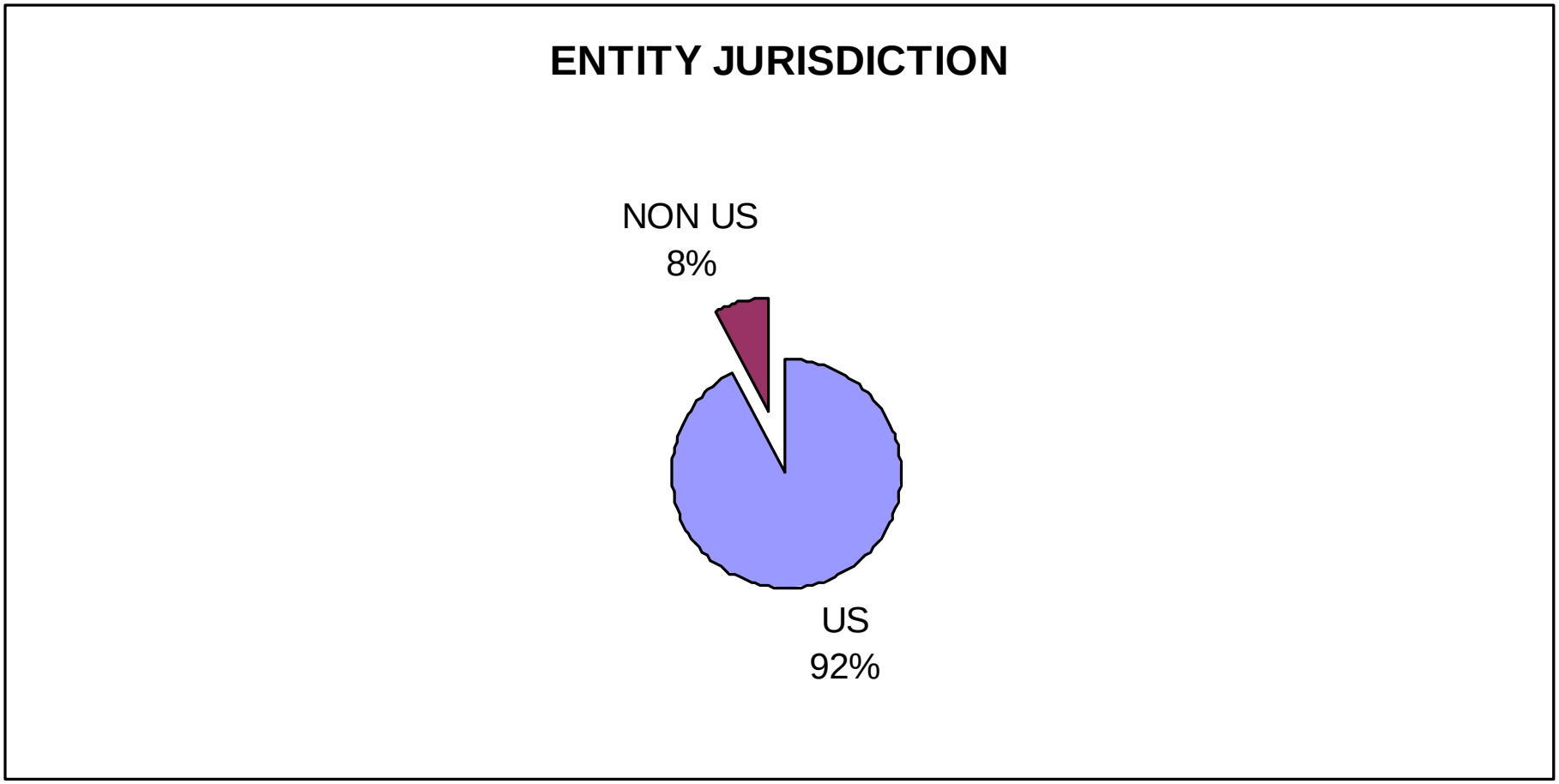
Member of Technical Staff

Operator Demographics: Where?

- 13 root server instances operated by entities in 3 countries
  - **United States of America**
    - 3 Corporate (a, c, & j)
    - 2 Educational (b & d)
    - 1 Military (g)
    - 2 Research (e & h)
    - 3 Non Profit (f, i, & l)
      - Autonomica is responsible for I, but hosts “some” instances on a CDN. The CDN operator is a US formed entity.
  - **European Union**
    - 1 Non Profit (k)
  - **Japan**
    - 1 Non Profit (m)

renesys

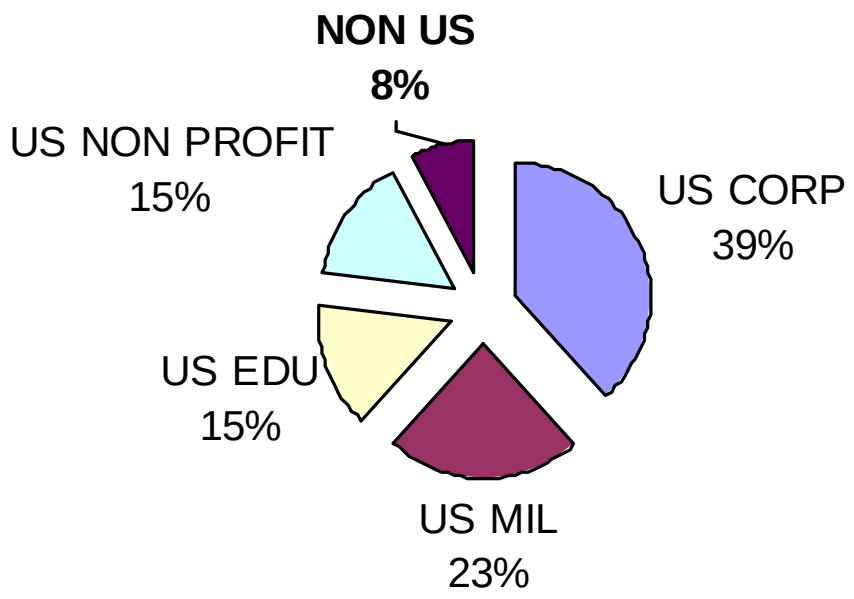
Operator Demographics (cont.)



renesys

Operator Demographics (cont.)

JURISDICTION BY US ENTITY TYPE VS. NON US



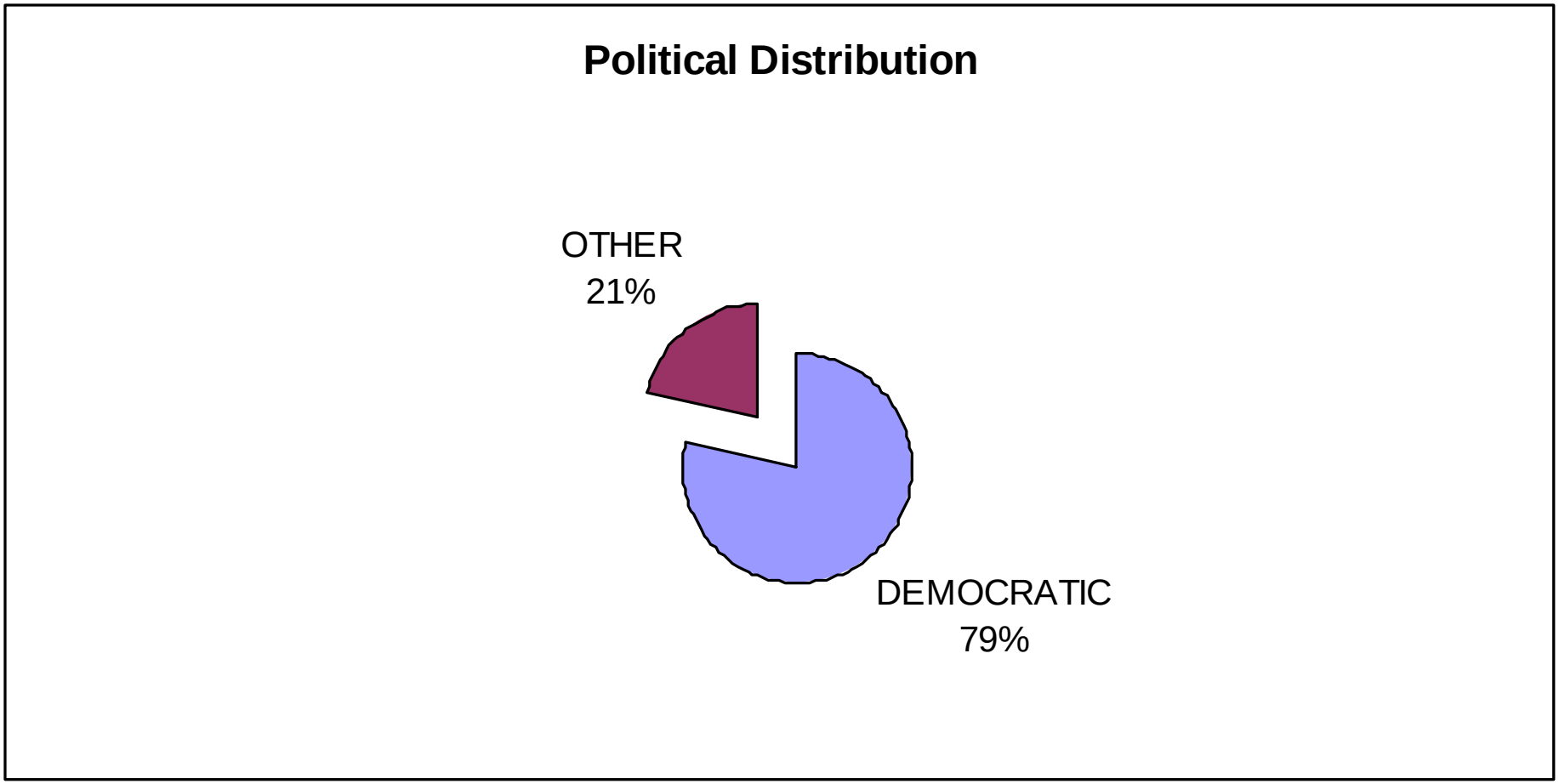
renesys

Operator Demographics (cont.)

- Where are the platforms?
  - In ~54 countries
  - All religions
  - All methods of Governance

renesys

Global Distribution (Political)

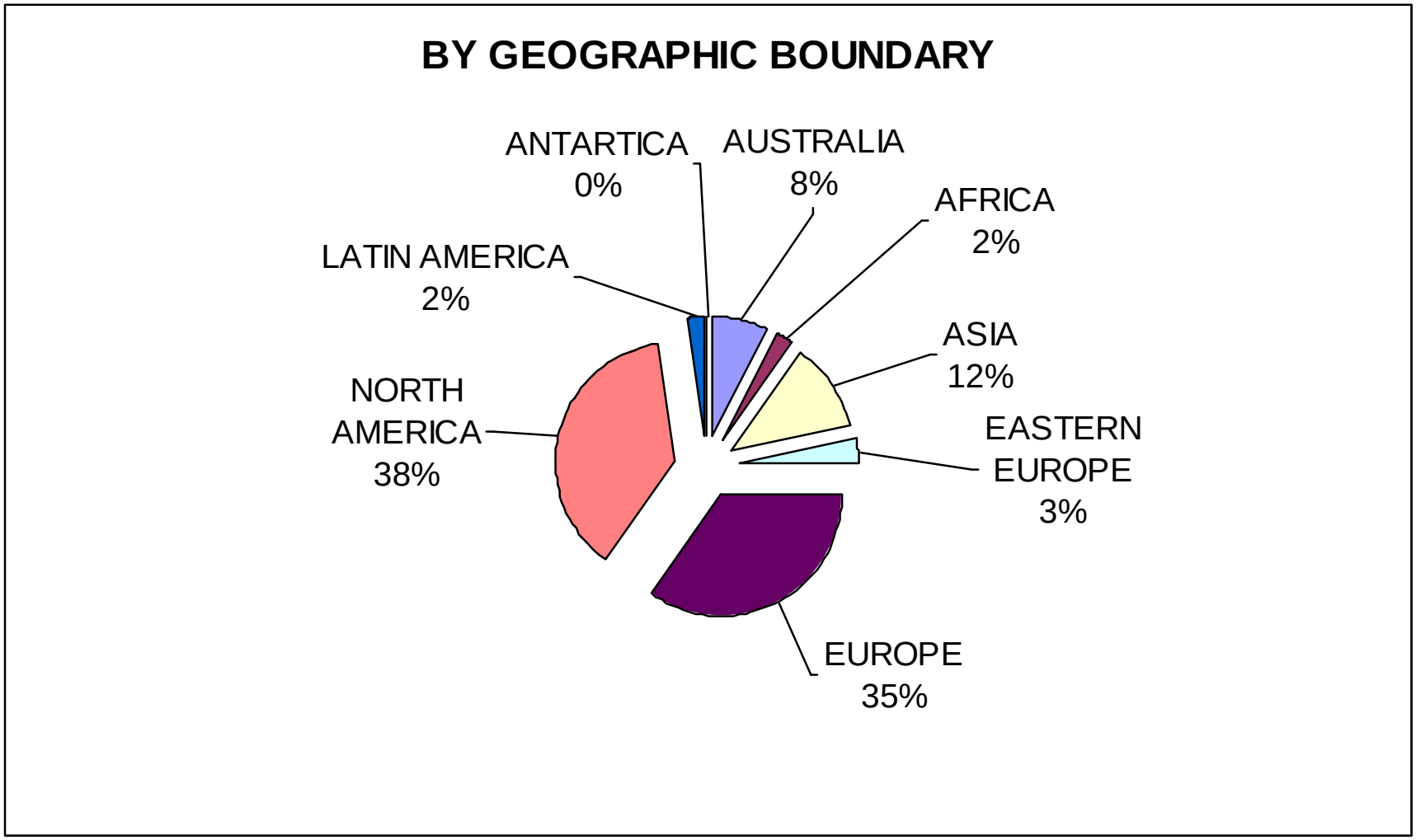


Operator Demographics (cont.)

- Global diversification for security and performance
  - Instances spread across continents
    - Different networks
    - Different procedures
    - Different software
    - Different hardware
    - Different weaknesses

renesys

Global Distribution (Geographical)



renesys

Situating a Root Server

- Relationships 101
  - Who you know
    - ICANN, Operator, IX, and RIR relationships
    - Regulators
  - How you spin it
    - National Pride
    - Performance and Security
    - Betterment of User Experience

renesys

Threats

- Not much different than anyone else
  - Direct attacks
  - Proxy Attacks
    - Botnets (collections of zombies w/c&c)
      - Easy money in indigent economies
      - Miscreants potentially masking other activities (what are they <u>really</u> doing?)

Hypothetically Speaking, let's attack

- Target: $-Root
  - Location: (EU Hosting Facility)
  - Multi-post cabinet configuration with cabling and power under-floor
  - Unlocked cabinet, single factor facility entry
- Physical Attack
  - Open cabinet Door
  - Turn it off
- Hijack attempt
  - Advertise a route
  - Return bad answers
- Network Attack
  - Spoof source
  - Random host querys
  - Send packet-love

renesys

Summary

- The root system is less likely subject to a single application exploit at the root DNS level, but it could be attacked at-large by at layer 3 (and is frequently – and more often)
- The system is accidentally robust as a result of layer “whatever” informal coordination vs. tight standard and operational procedure
- There is likely very good research other data coming across the interfaces of these systems
- (trend) A collapsed root system i.e. Where root servers and TLD's share the same hardware or networks should be more closely examined (Good? Bad? Ugly?)

renesys

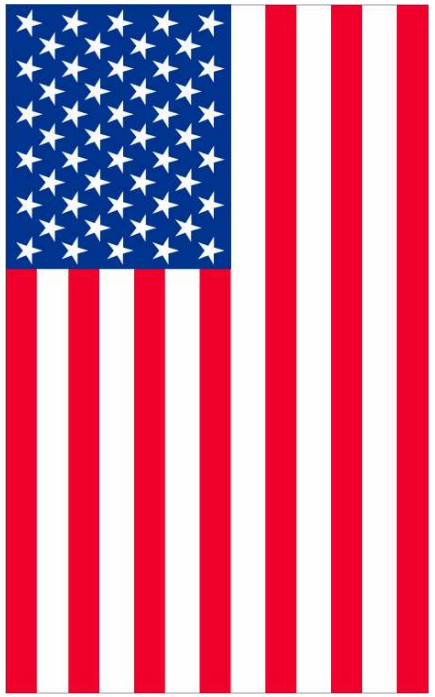
Credits

- Internet Assigned Numbers Authority
- Root Server Operators - www.root-servers.org
- World Atlas for Political and Geo Maps
- ICANN [GA] List
- Hallway conversations @ NANOG

renesys

About the Presenter

- Martin Hannigan
  - Boston, MA USA
  - ~20 Years Internet experience
  - CALEA, SS7, TCP/IP
  - Engineering and Ops Management
  - ARIN, RIPE, NANOG, & others
  - ICANN ASO AC Rep, ARIN Region



renesys

www.renesys.com