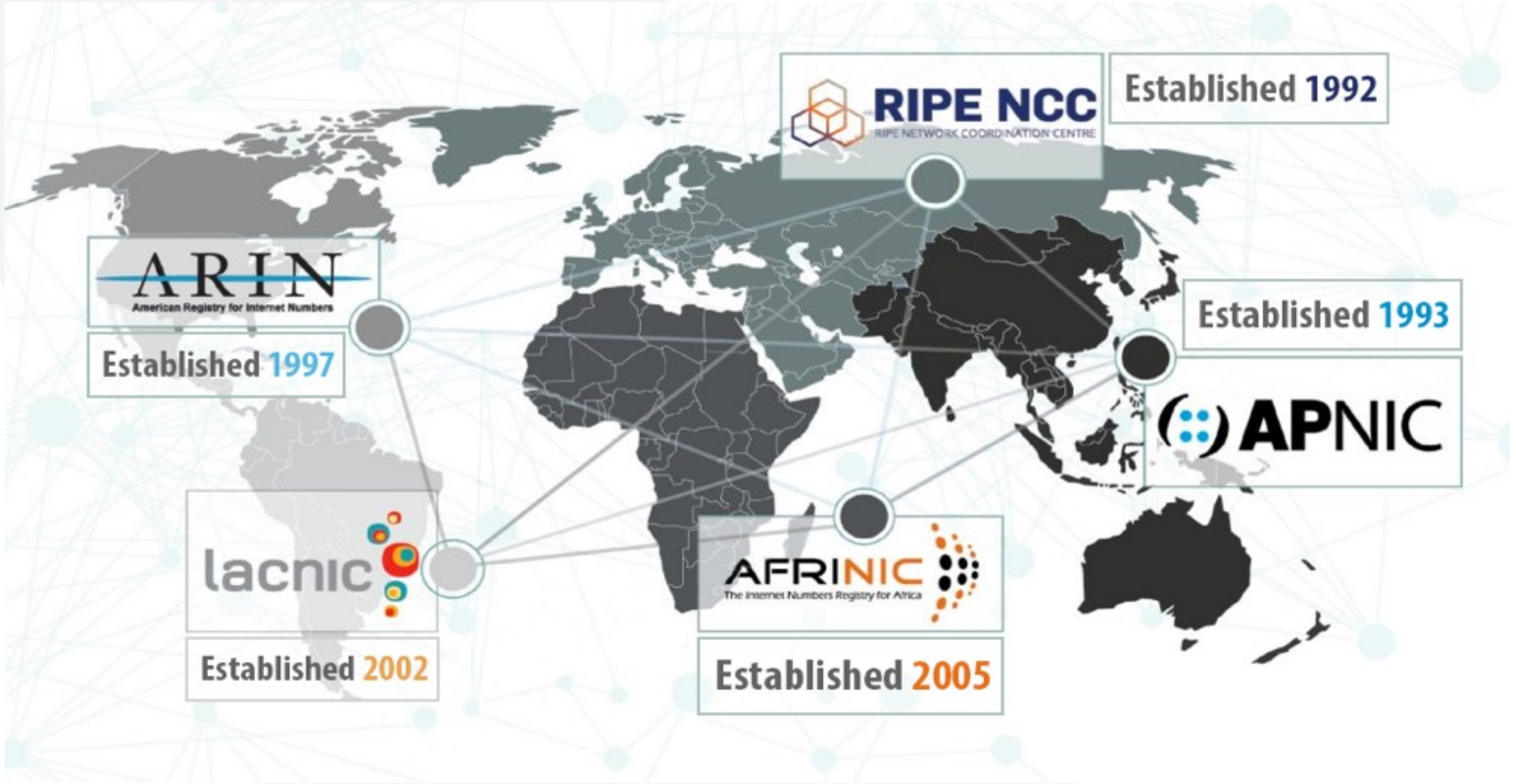
Protecting Infrastructure, Applications, Assets and Personnel

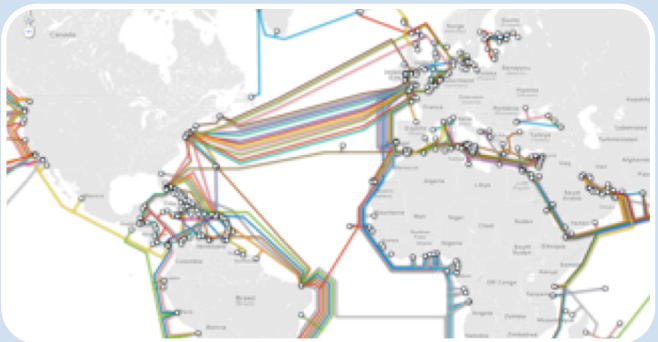
ARIN, RIRs, Cybersecurity and Public Trust

Leslie Nobile
Senior Director, Trust and Public Safety
leslie@arin.net

Who Are the RIRs?



Core Functions of an RIR



*Manage, distribute and register Internet Number Resources (IPv4 & IPv6 addresses and Autonomous System numbers (ASNs)

*Maintain Directory Services (Whois, Whowas, routing registries)

*Facilitate policy development process

*Provide reverse DNS delegation

*Support Internet infrastructure through technical coordination

*Provide technical capacity building

RIR Whois Directory

- **Publicly displayed** registration data including:
  - IP number resources issued by RIR (or predecessor registry)
  - Organizations responsible for number resources and their points of contact
  - Some customer reassignment information (ISP customers)
  - Original registration date and last updated date
- Referential information to authoritative RIR
- Routing information (AFRINIC, APNIC and RIPE)

*NON-PUBLIC DATA REQUIRES SUBPOENA OR LEGAL ORDER

**MOST ACCURATE DATA WILL COME FROM ISP

RIRs and Law Enforcement

WHOIS Directory	• LE uses Whois data to identify IP address registrants
Data Accuracy	• Work with LE and the community to improve the integrity and accuracy of the data (new policies, procedures, etc.)
Case Support	• Respond to subpoenas and court orders and assist in prep of these requests
Capacity Building	• Provide training and information sharing sessions • RIR Public Safety Coordination Group created to support LE
Tools and Resources	• Variety of resources & tools available that can help fight fraud and abuse (e.g. fraud and Whois inaccuracy reporting, APNIC Honeypots, Ripe Labs, RPKI…)

Current Trends

- **Adoption of IPv6 - slow but steady**
  - ISPs slowly rolling out IPv6
  - Steady increase in IPv6 traffic globally
- **Still high demand for IPv4**
  - RIRs have policies to enable market based transfers
  - Customers turning to IPv4 market for address space
- **Monetization of IPv4 addresses leading to increase in fraudulent activity across RIRs**
  - Current market prices ~ $20-$22 per IP address

Current Challenges

More fraudulent requests to transfer IPv4 addresses

Leasing/buying/selling of IPv4 address space (outside of registry system, often use falsified LOAs)

Hijacking of IPv4 addresses & ASNs

- *Make fraudulent Whois changes; Target dormant/out of date records*
- *Submit falsified documents; set up shell companies*

Route Hijacking

Unauthorized use of abandoned/un-routed IPv4 addresses

Improving Routing Security

- **Two technologies the RIRs directly involved in developing/deploying**
  - **Resource Public Key Infrastructure (RPKI)**
    - Security framework designed to secure the Internet's routing infrastructure by verifying association between resource holders and their number resources
      - Cryptographically certifies network resources
      - Certifies route announcements
  - **Validated Internet Routing Registry (IRR)**
    - Validation mechanisms added to IRR that guarantee routing announcements are published only by an authorized network

THANK YOU!

Protecting Infrastructure, Applications, Assets and Personnel

ARIN, RIRs, Cybersecurity and Public Trust

Leslie Nobile
Senior Director, Trust and Public Safety, ARIN
leslie@arin.net | www.arin.net

About the Presenter

LESLIE NOBILE

Leslie serves as ARIN's global law enforcement liaison and focuses much of her attention on global registry data integrity and accuracy.

Her work encompasses capacity building, training, and collaboration, with a focus on Regional Internet Registries and their role in the Internet eco-system, and more specifically, ARIN policy, operations and contractual requirements as they relate to data inaccuracy, fraud and abuse.

She has over 25 years of experience in the Internet industry, including supporting the development and expansion of the Defense Data Network (DDN), a high-speed military data network that evolved from the ARPANET

Links to Some Useful Tools

- **Number and Name Lookup Services**
  - **Root zone database for TLDs**
    https://www.iana.org/domains/root/db
  - **GeekTools**
    http://www.geektools.org/whois.php
- **Routing Information**
  - **Routing history (RIS)**
    http://www.ripe.net/projects/ris/index.html
  - **Route Views**
    http://www.routeviews.org
  - **Looking glass information**
    http://www.caida.org/analysis/routing/reversetrace/
  - **Blacklisting**
    http://www.mxtoolbox.com/blacklists.aspx
- **RIR Extended Delegated Stats**
  https://www.nro.net/wp-content/uploads/apnic-uploads/delegated-extended
- **Threat Intelligence**
  https://team-cymru.com/

Links to RIR LE Pages

- AFRINIC
  - https://afrinic.net/support/law-enforcement-authorities
- APNIC
  - https://www.apnic.net/community/security/security-cooperation/#LEAs
- ARIN
  - https://www.arin.net/about/relations/law_enforcement/
- LACNIC
  - https://www.lacnic.net/info-leas
- RIPE
  - https://www.ripe.net/about-us/legal/information-for-law-enforcement-agencies

Which Whois to Use?

- **APNIC**
  - http://wq.apnic.net/static/search.html
- **AFRINIC**
  - https://www.afrinic.net/whois-web/public
- **RIPE NCC**
  - https://apps.db.ripe.net
  -
- **ARIN**
  - http://whois.arin.net
- **LACNIC**
  - http://lacnic.net/cgi-bin/lacnic/whois