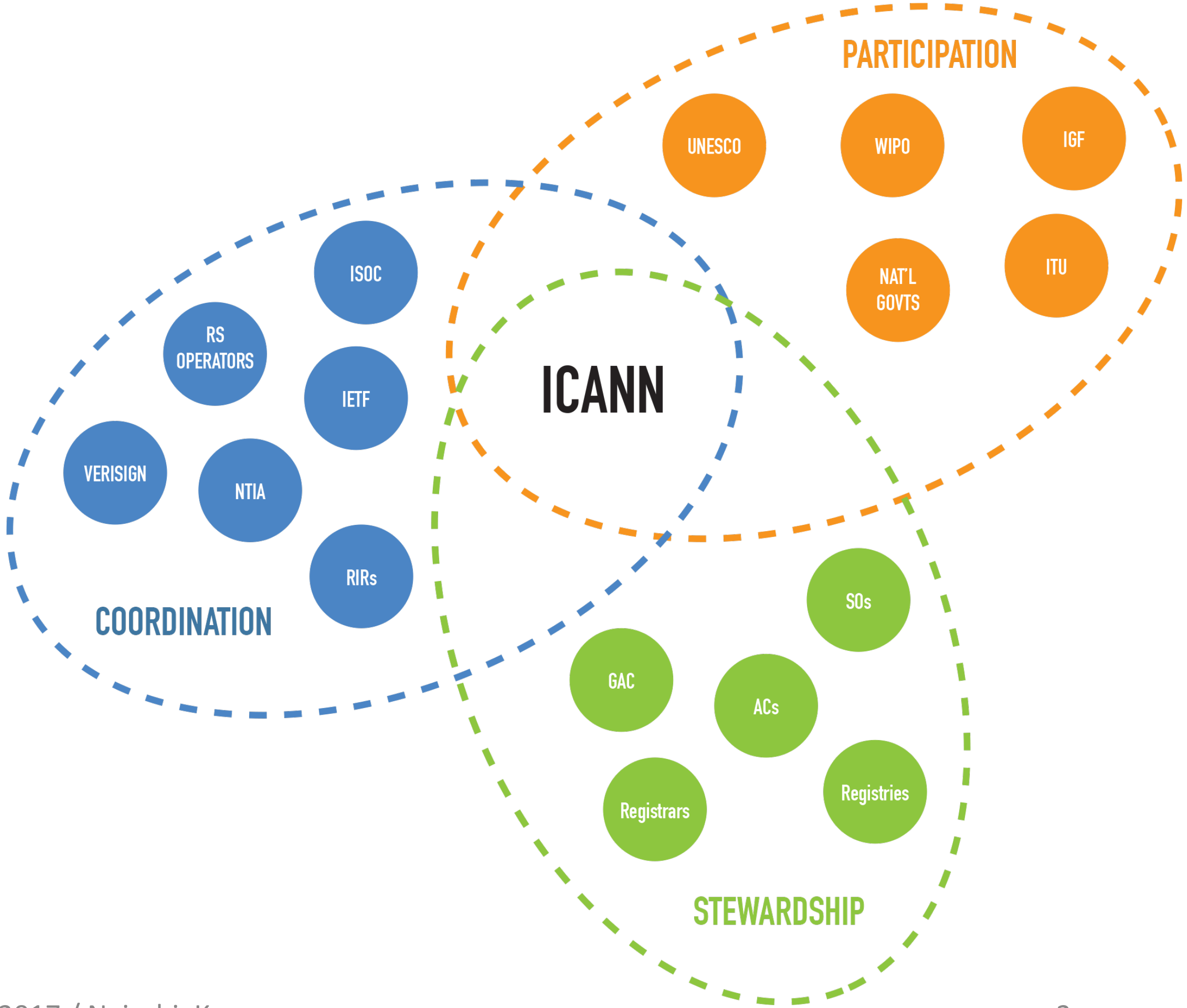
Cybersecurity and Cybersafety in the ICANN world

David Conrad
CTO, ICANN
david.conrad@icann.org

What is the Internet Corporation for Assigned Names and Numbers?

- A **Community**
  - Global, open, multi-stakeholder, bottom-up, consensus driven
- An **Organization**
  - US (California) not-for-profit, public benefit corporation with one member (the ICANN community)
  - As of 1 Oct 2016, no longer has a contract with the US Gov't for the "IANA Functions"
    - Now authorized by the ICANN community



What Does ICANN Do?

Community

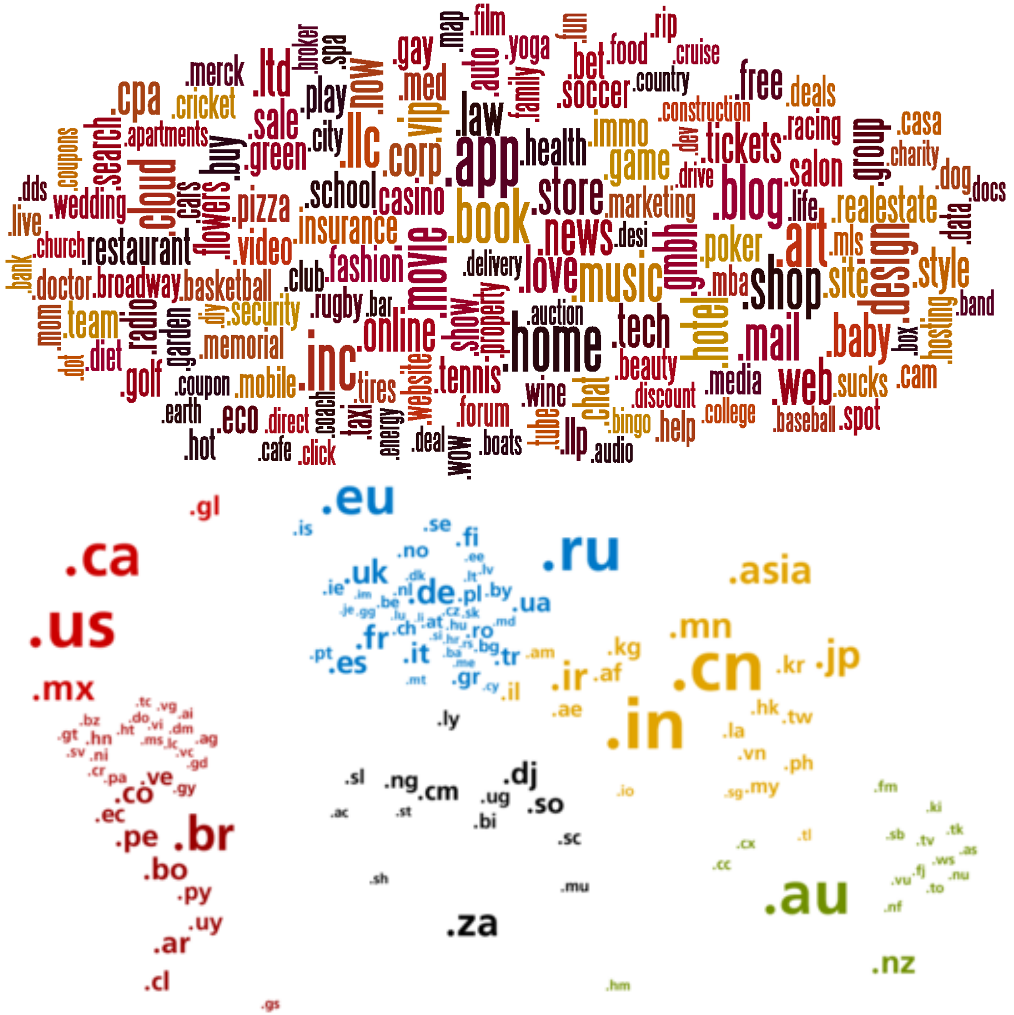
- Provides a venue for discussion
- **Defines policies** for
  - Creation of **top-level domains**
  - Operation of generic name registries
  - Accreditation of domain name registrars
- Holds the ICANN organization accountable

Organization

- **Implements policies defined by the community**
- Operates the "**IANA Functions**"
  - DNS Root Zone changes
  - Allocate address blocks to RIRs
  - Manage registries for IETF
- Facilitates discussions
  - Hold meetings and other events

Pragmatically Speaking…

- ICANN is (primarily) involved in the top-most levels of the domain name system
  - Create/change new TLDs
    - **.EXAMPLE**
  - Enforce contractual obligations on (non-country code) registries and registrars that sell 2nd level names
    - **ASANTE.EXAMPLE**
- ICANN also provides services to the RIRs and the IETF



Some Definitions

“Cybersecurity”

- “measures taken to protect **a computer or computer system** (as on the Internet) against unauthorized access or attack”

https://www.merriam-webster.com/dictionary/cybersecurity

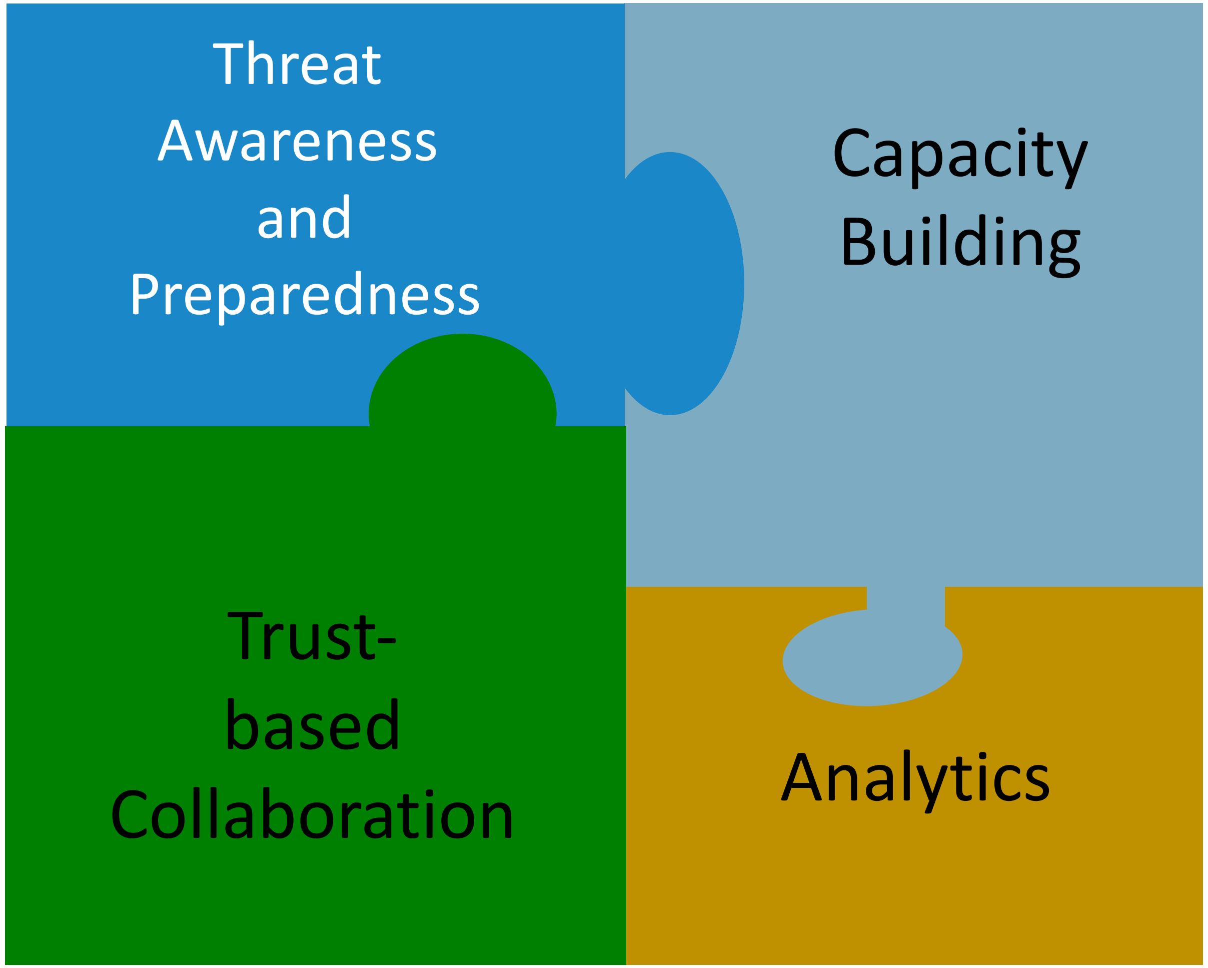
“Cybersafety”

- “the knowledge of maximizing **the user's personal safety** and security risks to private information and property associated with using the internet, and the self-protection from computer crime in general.”

https://en.wikipedia.org/wiki/Internet_safety

ICANN's Role in Cybersecurity & Cybersafety

- Identifying and helping the community be prepared for identifier-based threats
  - DNS, IP addresses, and similar technologies
- Working with the operational security community via trust networks
- Offering training and other capacity building services
- Providing neutral and unbiased data-backed analysis



Threat Awareness and Preparedness

Capacity Building

Trust-based Collaboration

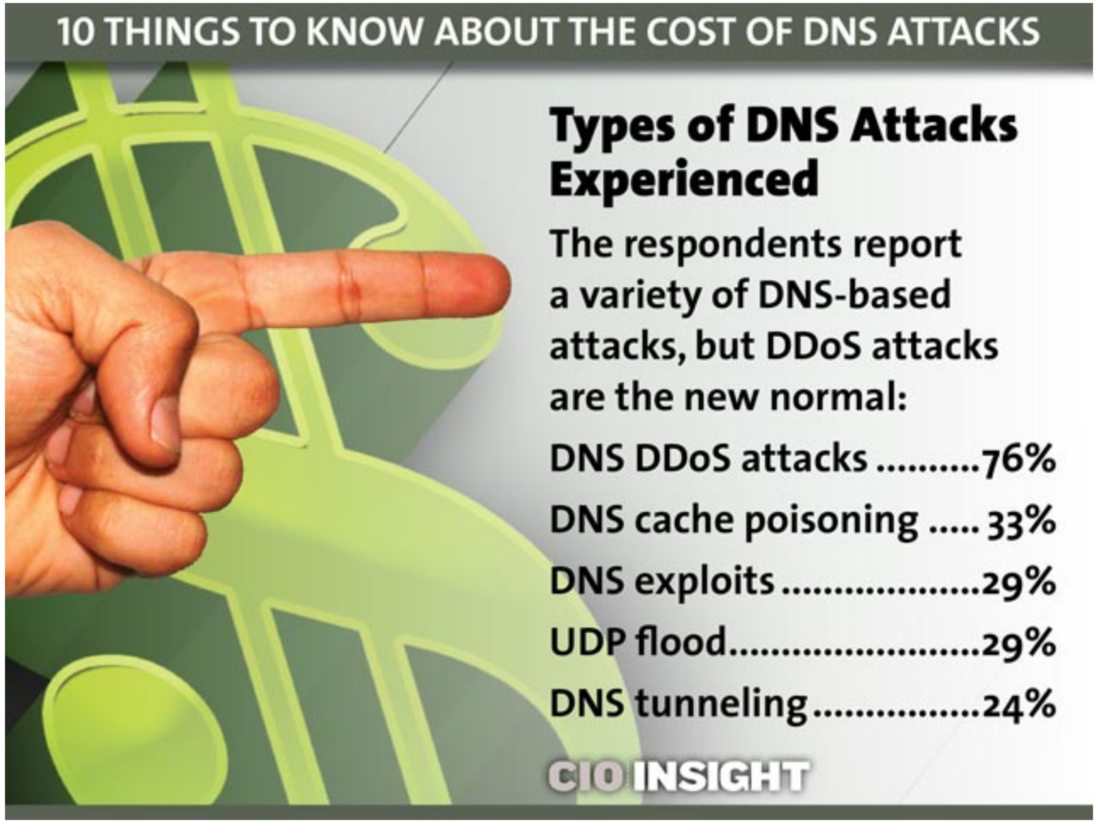
Analytics

Another Definition: “DNS Abuse”

- Using the Internet’s naming system for malicious purposes.

Examples:

- Denial of service via DNS protocol
- Botnet command/control synchronization
- Spam-vectored threats:
  - Phishing for distribution of malware or fraud
- Infrastructure-vectored threats:
  - Cache poisoning
  - Resolver Redirection
  - DNS tunneling



10 THINGS TO KNOW ABOUT THE COST OF DNS ATTACKS

Types of DNS Attacks Experienced

The respondents report a variety of DNS-based attacks, but DDoS attacks are the new normal:

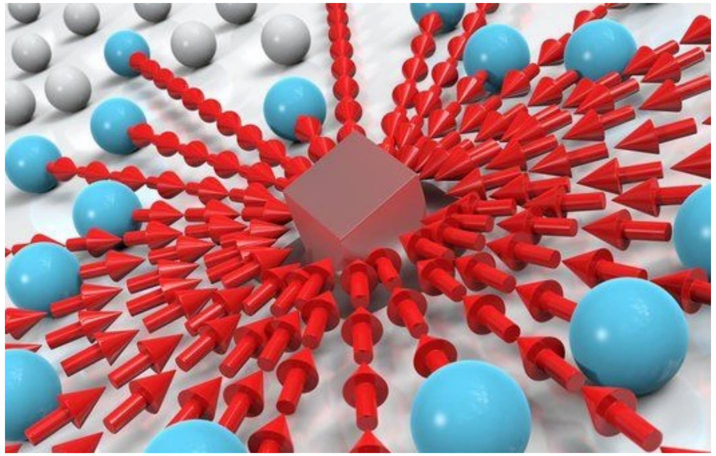
DNS DDoS attacks	76%
DNS cache poisoning	33%
DNS exploits	29%
UDP flood	29%
DNS tunneling	24%

CIO INSIGHT

http://www.cioinsight.com/security/slideshows/10-things-to-know-about-the-cost-of-dns-attacks.html

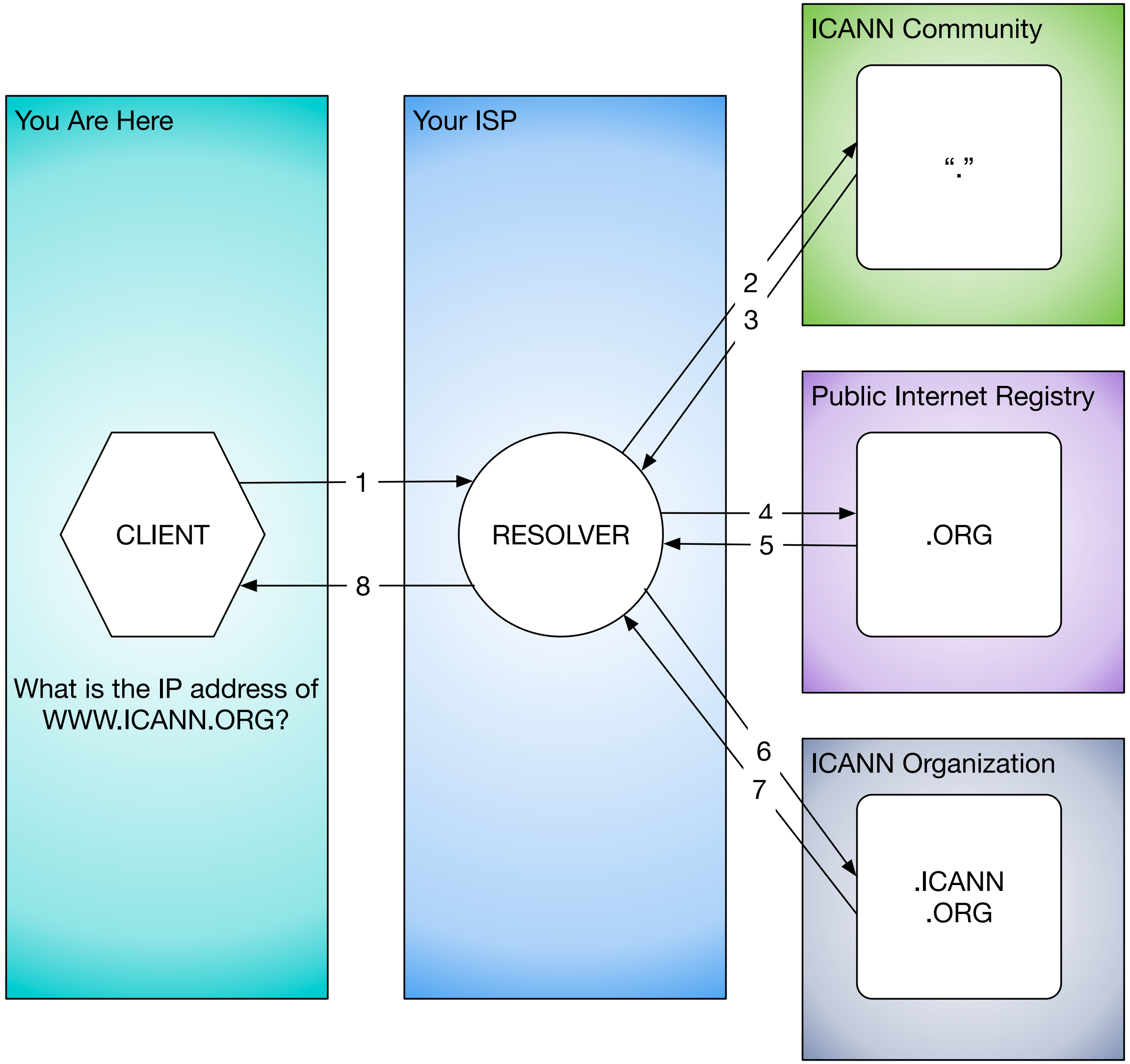
ICANN’s Efforts to Mitigate DNS Abuse

- DNSSEC
  - Signing TLD zones (90% signed)
  - Encouraging turning on validation (20% of Internet users protected)
  - **Updating the root key**
    - **11 October 2017**
- DNS Abuse Mitigation
  - Methodologies
  - Data collection and analysis
- Denial of Service targeting Root/TLDs
  - Vulnerabilities
  - Mitigation



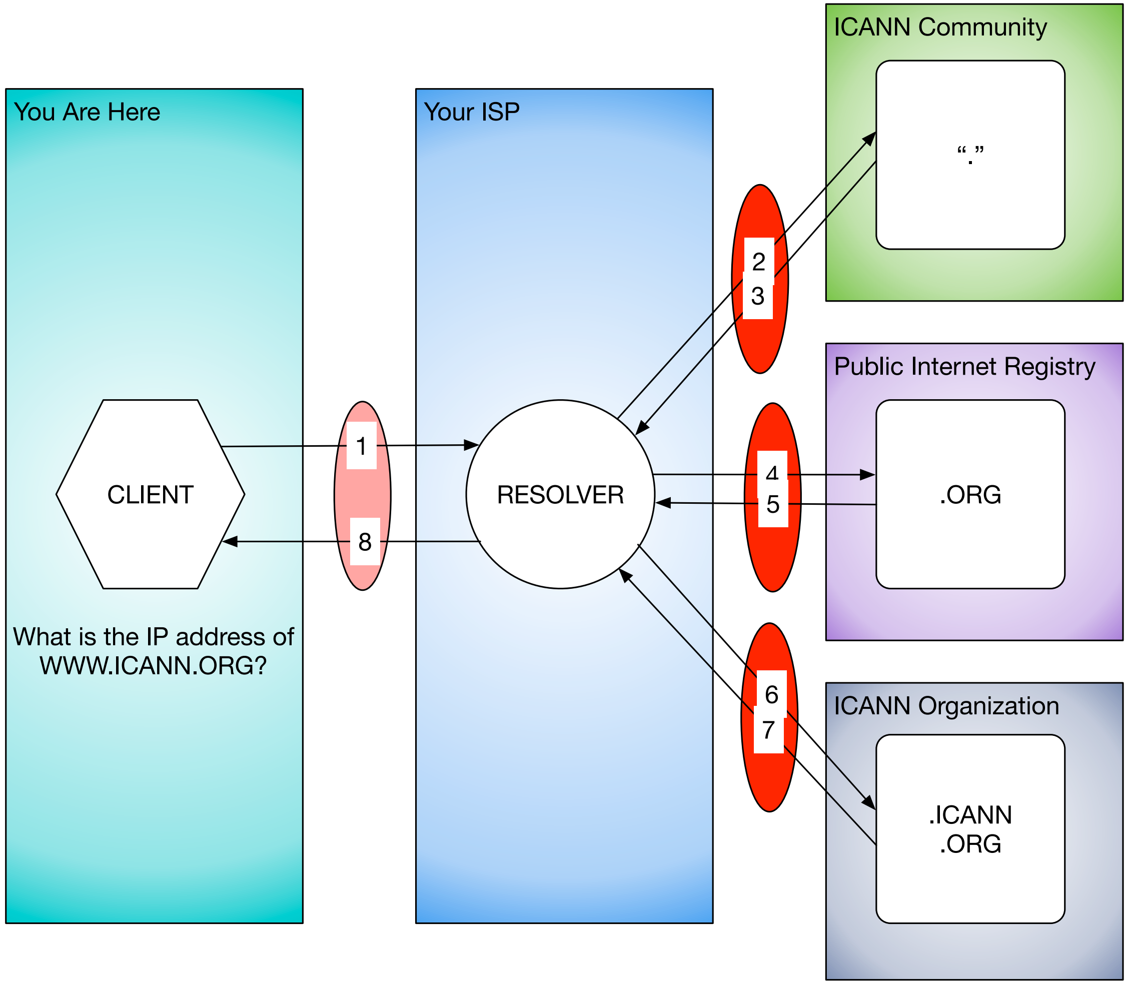
DNS at a (Very) High Level

- Three components
  1. Client
     - Built into applications
  2. “Resolver”
     - Run by network operators
  3. Authoritative Databases
     - Run by DNS registries



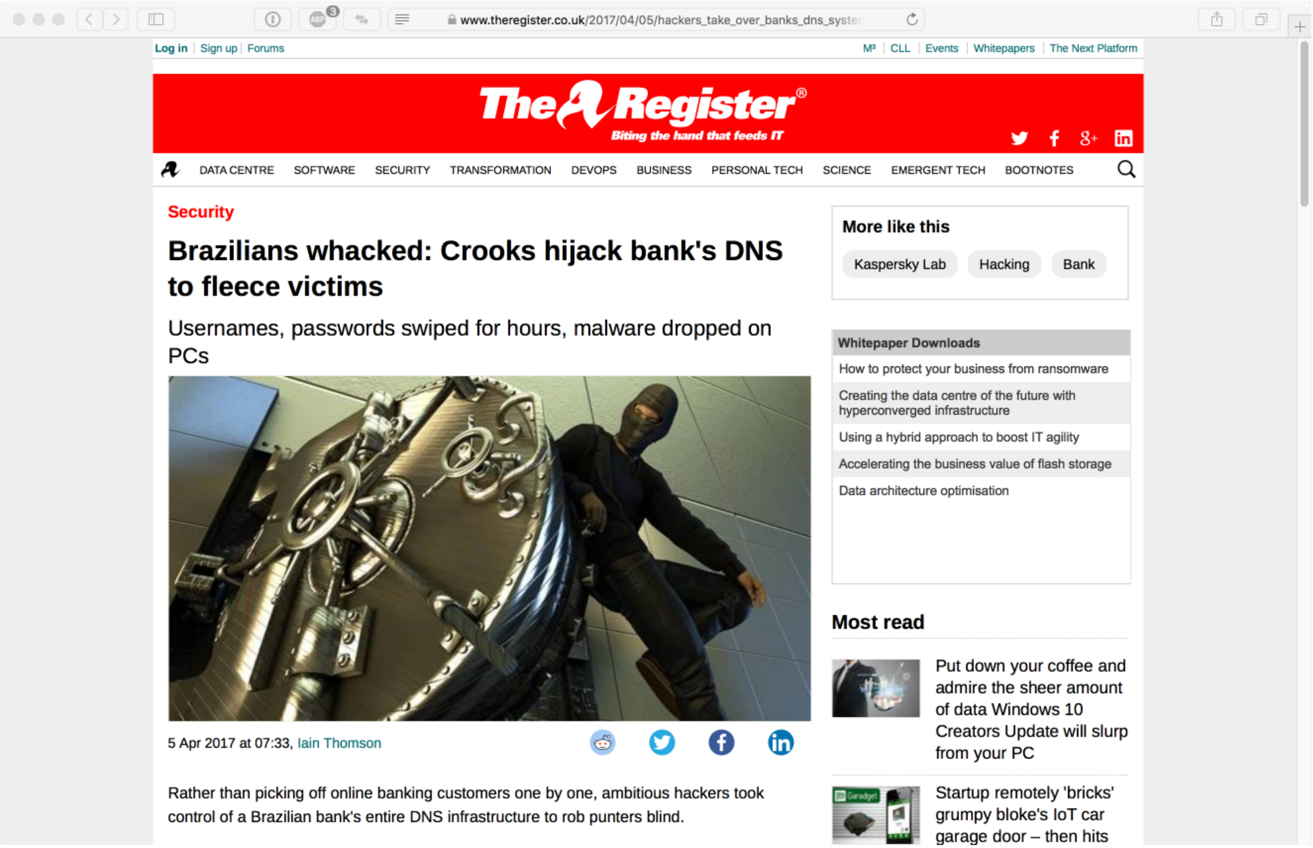
ICANN and Cybersecurity

- Encouraging:
  - Protecting the client/resolver links (1 and 8)
    - VPNs, running resolvers locally, etc.
  - Enabling DNSSEC validation in resolvers
    - Protects links 2 - 7
  - DNSSEC-signing zones
    - Protects databases
- Capacity building, training, information sharing, etc.



Why? A (Very) Recent Example...

- “[A] major Brazilian financial company with hundreds of branches, operations in the US and the Cayman Islands, 5 million customers, and more than $27 billion in assets.”
  https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/
- “[A]ccording to security researchers at Kaspersky, **the bank is just one of ten** around the world that has been almost **totally compromised** in a comprehensive cyber attack.”
- **“If DNS was under control of the criminals, you're screwed**.”
  http://www.computing.co.uk/ctg/news/3007938/brazilian-bank-customers-targeted-after-hackers-transfer-all-of-the-banks-domains-to-phony-websites


www.theregister.co.uk/2017/04/05/hackers_take_over_banks_dns_syste
Log in | Sign up | Forums
M³ | CLL | Events | Whitepapers | The Next Platform
The Register®
Biting the hand that feeds IT
DATA CENTRE
SOFTWARE
SECURITY
TRANSFORMATION
DEVOPS
BUSINESS
PERSONAL TECH
SCIENCE
EMERGENT TECH
BOOTNOTES

Security

Brazilians whacked: Crooks hijack bank's DNS to fleece victims

Usernames, passwords swiped for hours, malware dropped on PCs

5 Apr 2017 at 07:33, Iain Thomson

Rather than picking off online banking customers one by one, ambitious hackers took control of a Brazilian bank's entire DNS infrastructure to rob punters blind.

More like this

Kaspersky Lab | Hacking | Bank

Whitepaper Downloads

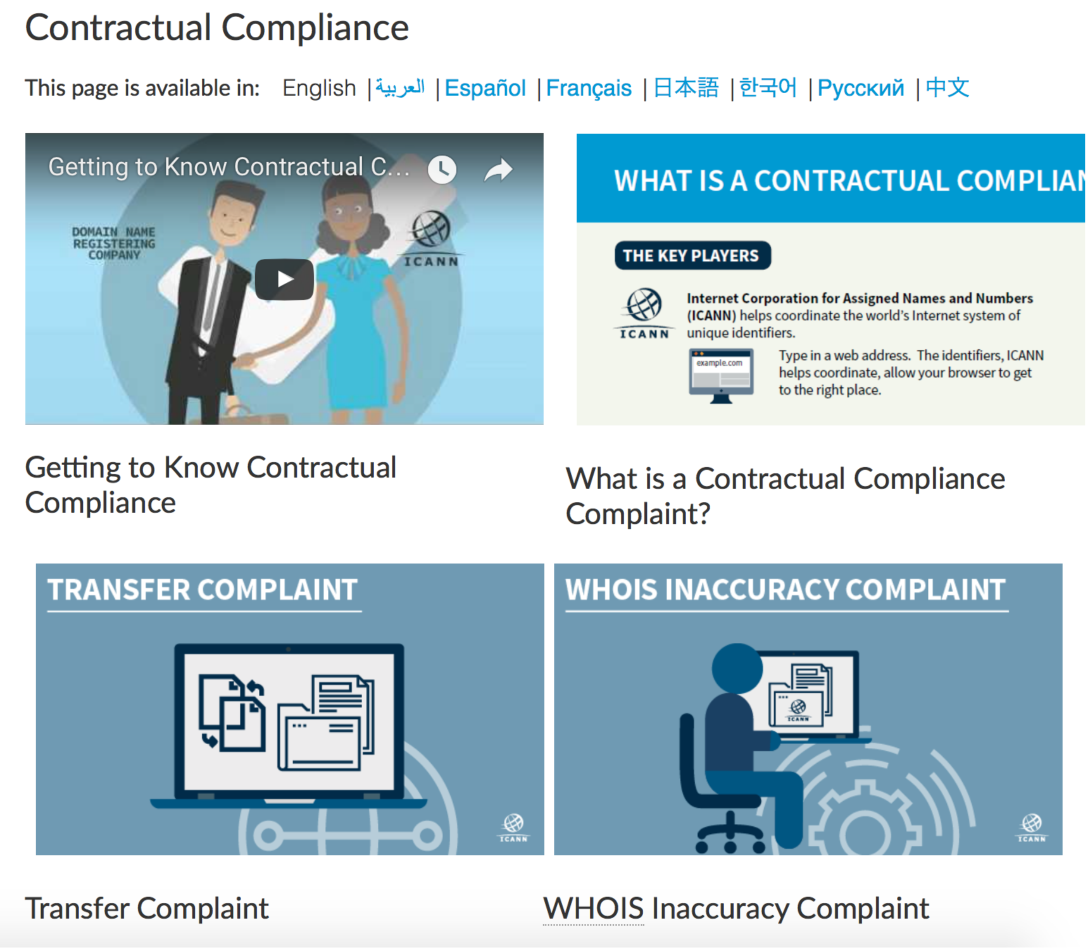
- How to protect your business from ransomware
- Creating the data centre of the future with hyperconverged infrastructure
- Using a hybrid approach to boost IT agility
- Accelerating the business value of flash storage
- Data architecture optimisation

Most read

- Put down your coffee and admire the sheer amount of data Windows 10 Creators Update will slurp from your PC
- Startup remotely 'bricks' grumpy bloke's IoT car garage door – then hits

ICANN and Cybersafety

- Contractual obligations on generic top-level domain registries and registrars
  - Require contact details of registrants
  - Force compliance with IETF standards
  - “Public Interest Commitments”
- Capacity building, training, information sharing, etc.



Contractual Compliance

This page is available in: English | العربية | Español | Français | 日本語 | 한국어 | Русский | 中文

Getting to Know Contractual C…
DOMAIN NAME REGISTERING COMPANY
ICANN
WHAT IS A CONTRACTUAL COMPLIAN
THE KEY PLAYERS
ICANN
example.com

Internet Corporation for Assigned Names and Numbers (ICANN) helps coordinate the world’s Internet system of unique identifiers.

Type in a web address. The identifiers, ICANN helps coordinate, allow your browser to get to the right place.

Getting to Know Contractual Compliance

What is a Contractual Compliance Complaint?

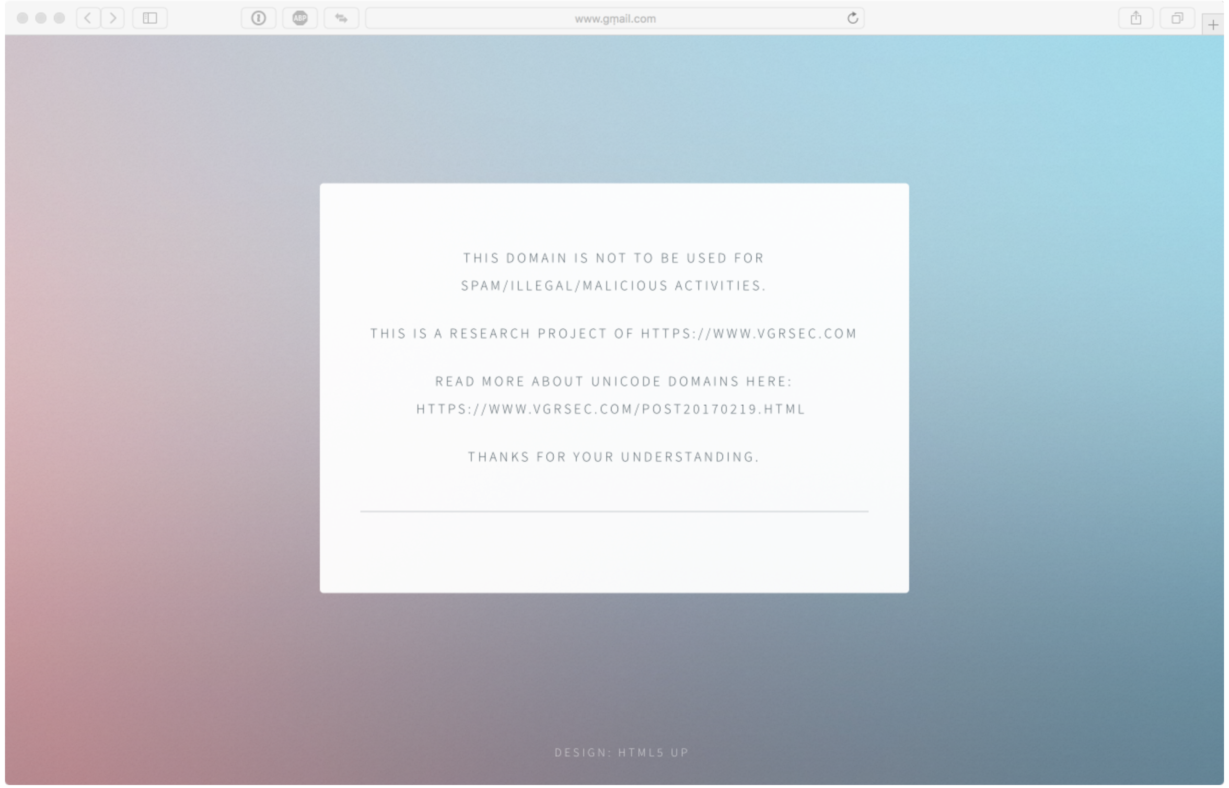
Transfer Complaint

WHOIS Inaccuracy Complaint

https://www.icann.org/resources/pages/compliance-2012-02-25-en

Why?

http://www.gṃail.com/



THIS DOMAIN IS NOT TO BE USED FOR SPAM/ILLEGAL/MALICIOUS ACTIVITIES.

THIS IS A RESEARCH PROJECT OF HTTPS://WWW.VGRSEC.COM

READ MORE ABOUT UNICODE DOMAINS HERE:
HTTPS://WWW.VGRSEC.COM/POST20170219.HTML

THANKS FOR YOUR UNDERSTANDING.

DESIGN: HTML5 UP

http://www.xn--gail-qd5a.com/

Ongoing DNSSEC Efforts

- DNSSEC: Security enhancements to the DNS
  - Fixes a known vulnerability, improves DNS trustability
- Two Inter-related Efforts
  1. DNSSEC-sign zones: **add cryptographic signatures** to DNS data
     - Done by domain name holders, i.e., IANA for root, Registries for TLDs, Registrants for 2nd-level domains, etc.
  2. Enable DNSSEC validation: **check those signatures**
     - Done by resolver/network operators, e.g., ISPs, enterprise network administrators

Changing the Root Key

- Root DNSSEC-signed in 2010
  - Commitment to update (“roll”) the key “after 5 years”

October 11, 2017

- Resolver Operators **MUST** update the root key in their servers
  - If they do not, all lookups in signed zones will fail

InfoWorld FROM IDG

ICANN's DNS Apocalypse

Changes to the DNS made by ICANN's CTO David Conrad h triggered what some are calling a 'DNS Apocalypse'

By George Marb

AP ASSOCIATED PRESS

BIG STORY TOP NEWS SPECIAL COVERAGE ARCHIVE ESPAÑOL VIDEO RADIO

Nov 27, 4:35 PM EST

INTERNET POLL: FIRE ICANN CTO

BY JENN BRYCE
ASSOCIATED PRESS

LOS ANGELES, California. (AP) -- 43,000 netizens have signed a petition urging the Internet Corporate for Assigned Names and Numbers (ICANN) to immediately fire Chief Technology Officer David Conrad. The petition comes just 2 days after a historic Internet outage caused by tweaks Conrad made to the Internet's architecture, known as the Domain Name System.

Conrad has remained silent on the global outage occurred, and ICANN has

TIME

DECEMBER 12, 2016

404 ERROR

How one man managed to bring the Internet to its knees

BY B.R. WHITE

LIVE

REAKING NEWS

ANN'S CTO BREAKS INTERNET

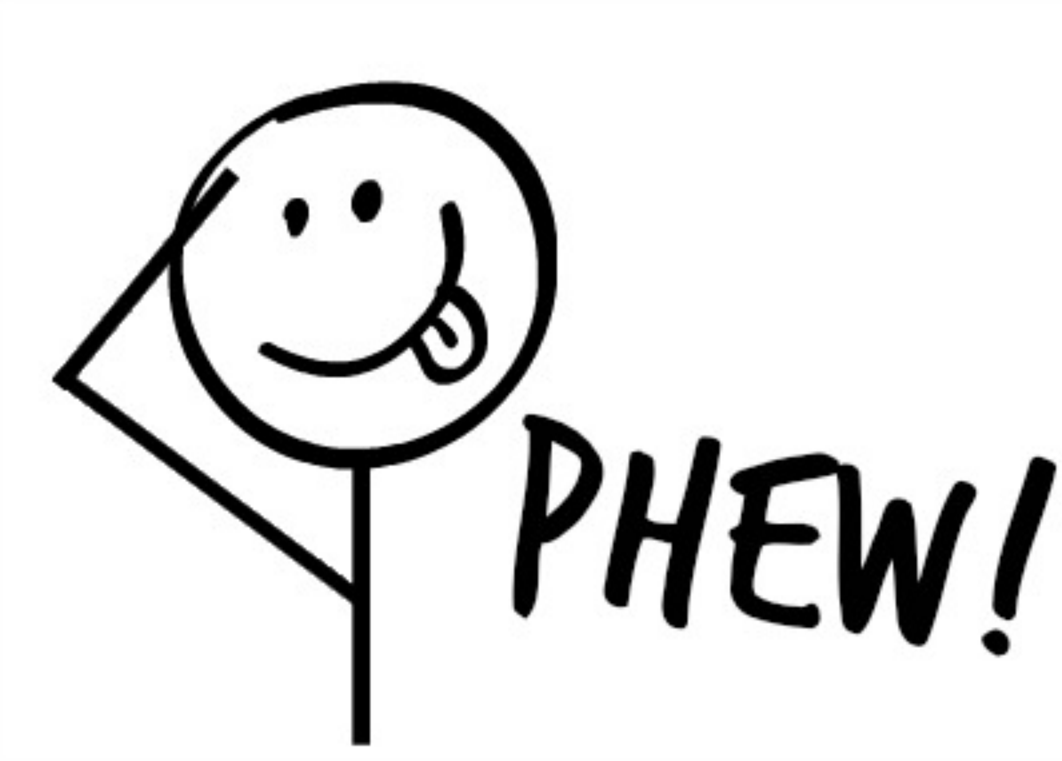
ELDERS OF INTERNET INCREASE BOUNTY TO $20K | PRESIDENT VOWS TO GIVE STERN

Internet not Doomed

- Failure to update the key: very bad.

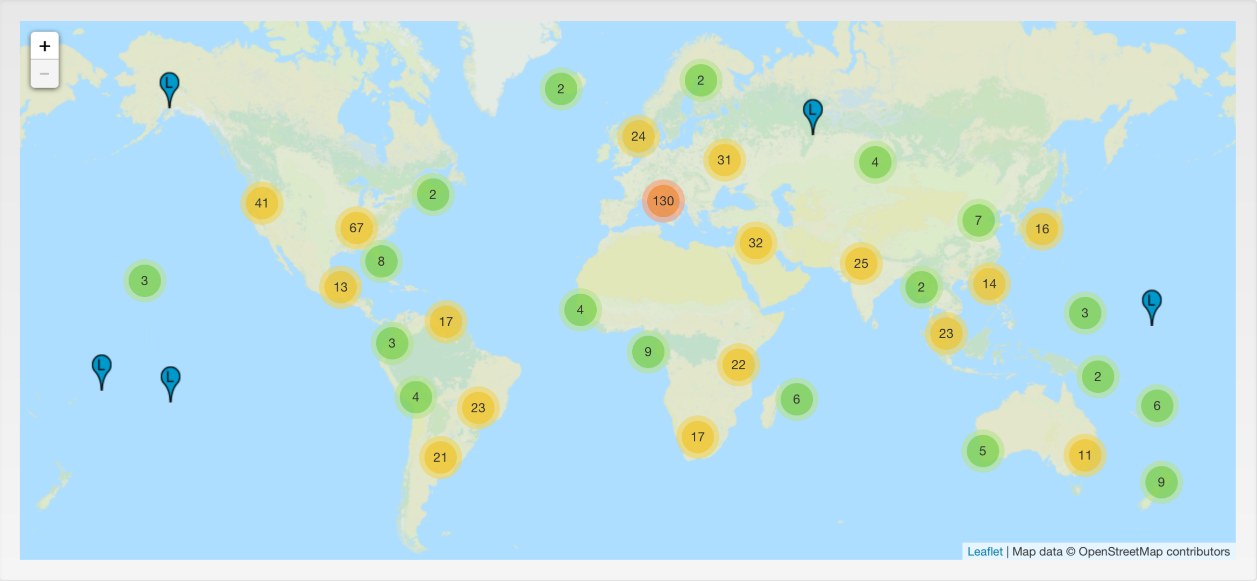
However....

- Most modern resolvers can handle the key change automatically
  - Should be tested: https://automated-ksk-test.research.icann.org
- Communication Plan: Let People Know
  - Outreach to network operations groups, RIRs, industry groups, governments



On the Topic of Root Servers

- 13 Root Server IP addresses
  - Labeled A – M.ROOT-SERVERS.NET
  - 12 organizations in 4 countries
- 600+ root server machines
  - 50+ economies
- ICANN (“L”) manages 157
  - If interested, contact me
- But…
  - Root has been DNSSEC-signed
    - Doesn’t matter from where you get it
- RFC 7706 provides a way **any** resolver operator can mirror the root
  - Reduces latency, increases resiliency
  - **Protects against root DDoS**



http://www.root-servers.org

What Can You Do?

Regulators/Governments

- Participate in ICANN
  - Government Advisory Committee
  - GAC's Public Safety Working Group
  - Engage in capacity building workshops
- Enquire about DNSSEC plans with your network operators
  - Ready for root key update?
- Support a national Computer Emergency Response Team (CERT)

Network Operators

- Participate in ICANN
  - Internet Service Providers and Connectivity Providers Constituency
  - Technical Experts Group
  - RSSAC Caucus
- Enable DNSSEC validation
  - Prepare for root key update
- Deploy DNSSEC
  - Sign all your zones
  - Encourage your customers to sign their zones
- Mirror the root zone
  - RFC 7706 is easiest

Asante!

ICANN

AFRICA INTERNET SUMMIT'17

NAIROBI - KENYA

21 MAY - 2 JUNE 2017

ICANN POLICY FORUM 59

JOHANNESBURG

26–29 June 2017