Cybersecurity and Cybersafety in the ICANN world

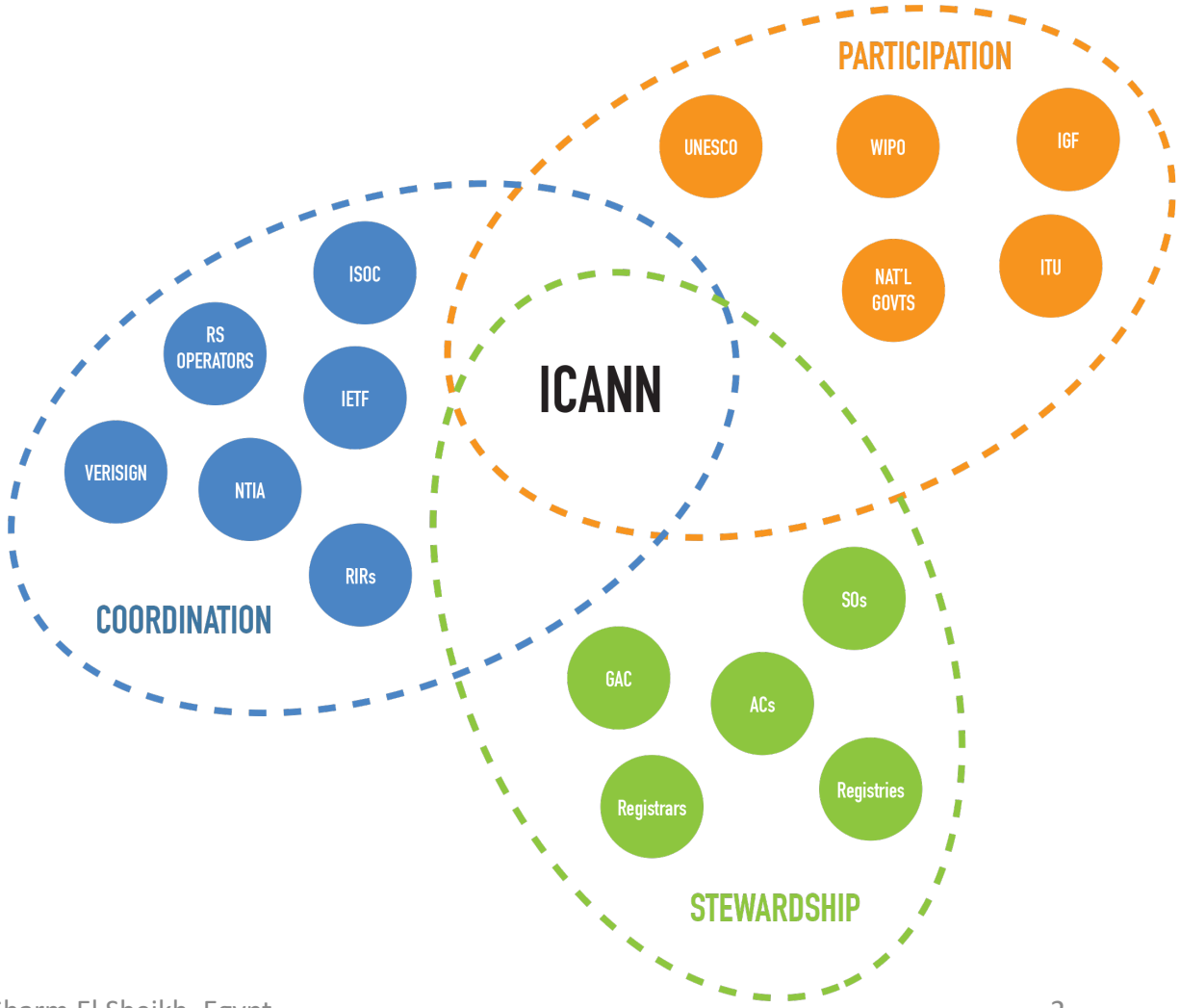
Empowering Global Cooperation on Cybersecurity for Sustainable Development and Peace

Africa IGF 2017
Sharm El Sheik – Egypt
Dec 05, 2017

Yaovi Atohoun

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

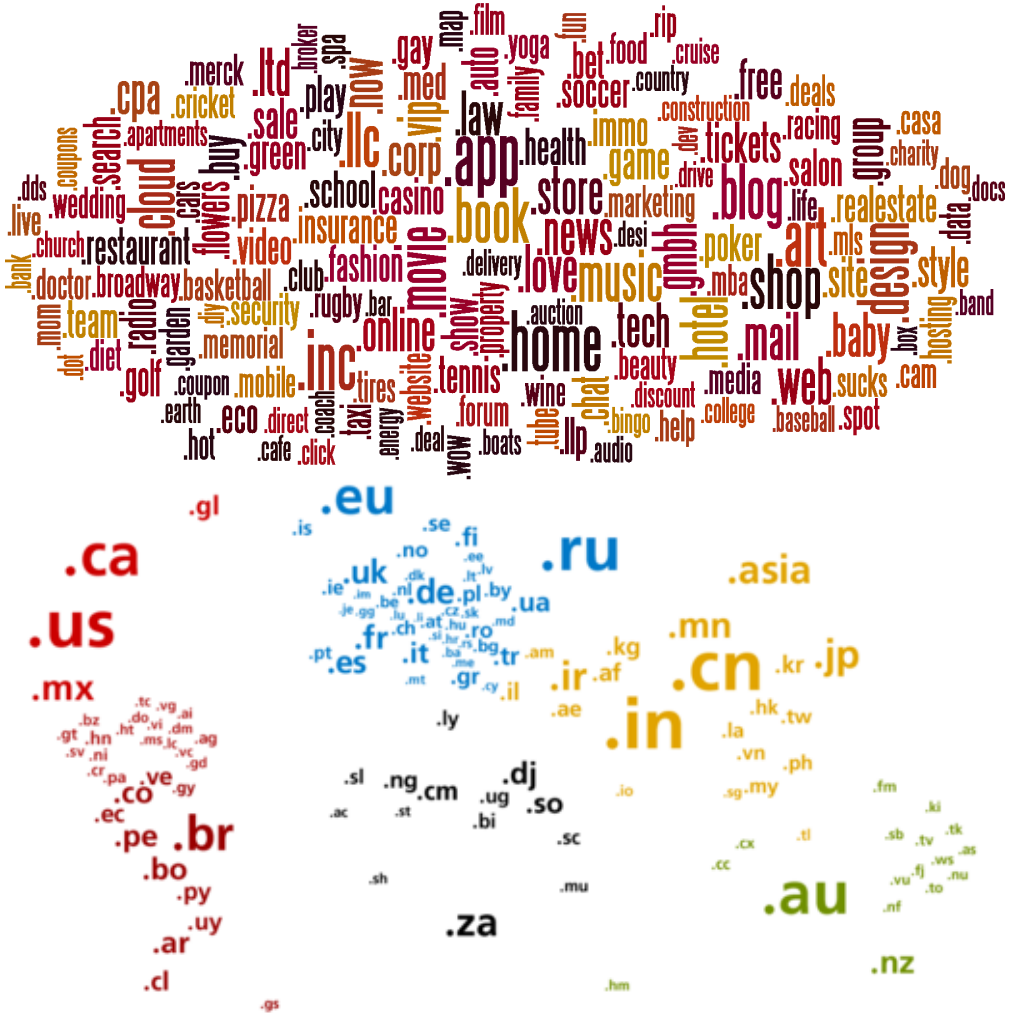
- Provides a venue for discussion
- **Defines policies** for
  - Creation of **top-level domains**
  - Operation of generic name registries
  - Accreditation of domain name registrars
- Holds the ICANN organization accountable

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

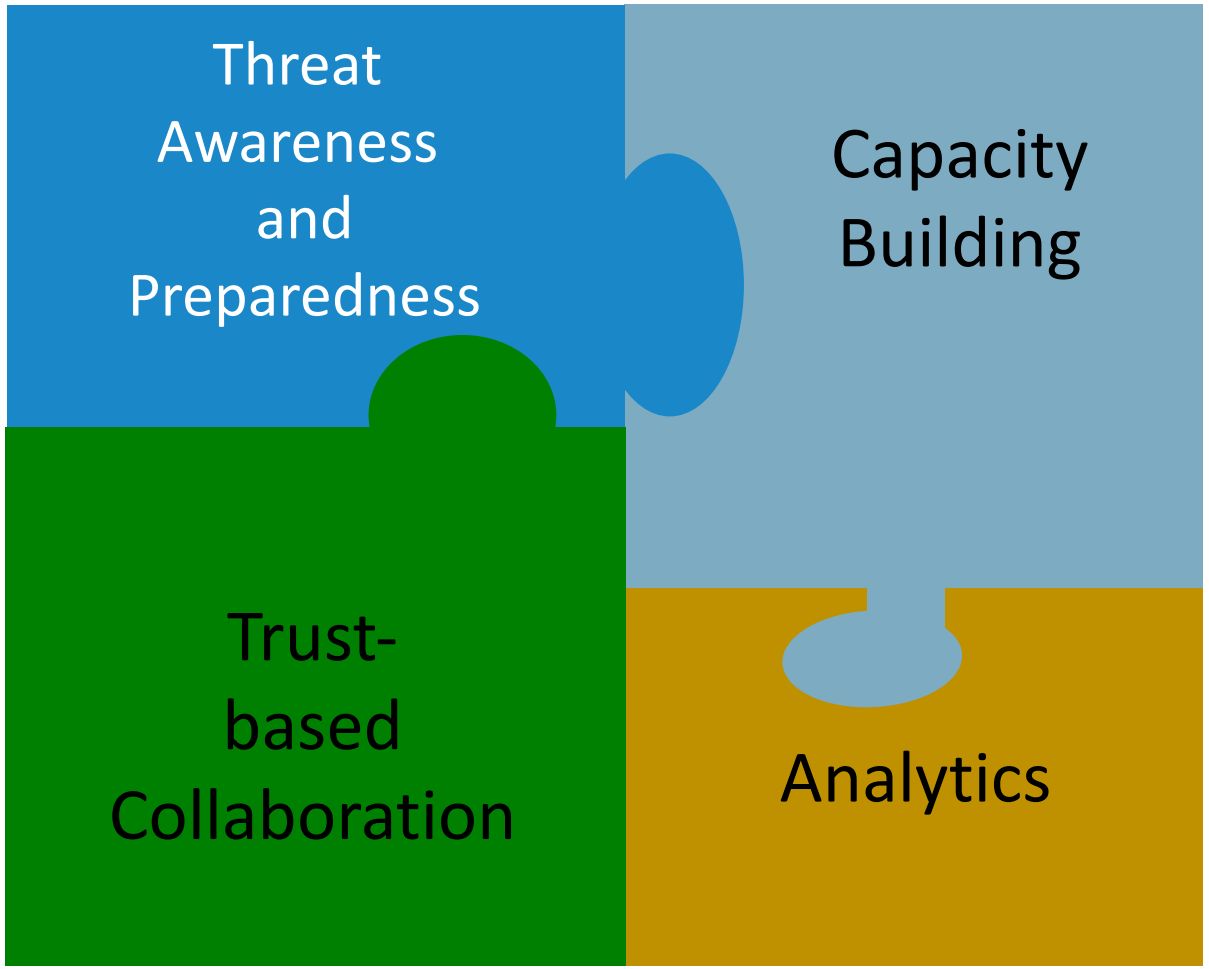
"Cybersafety"

- "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

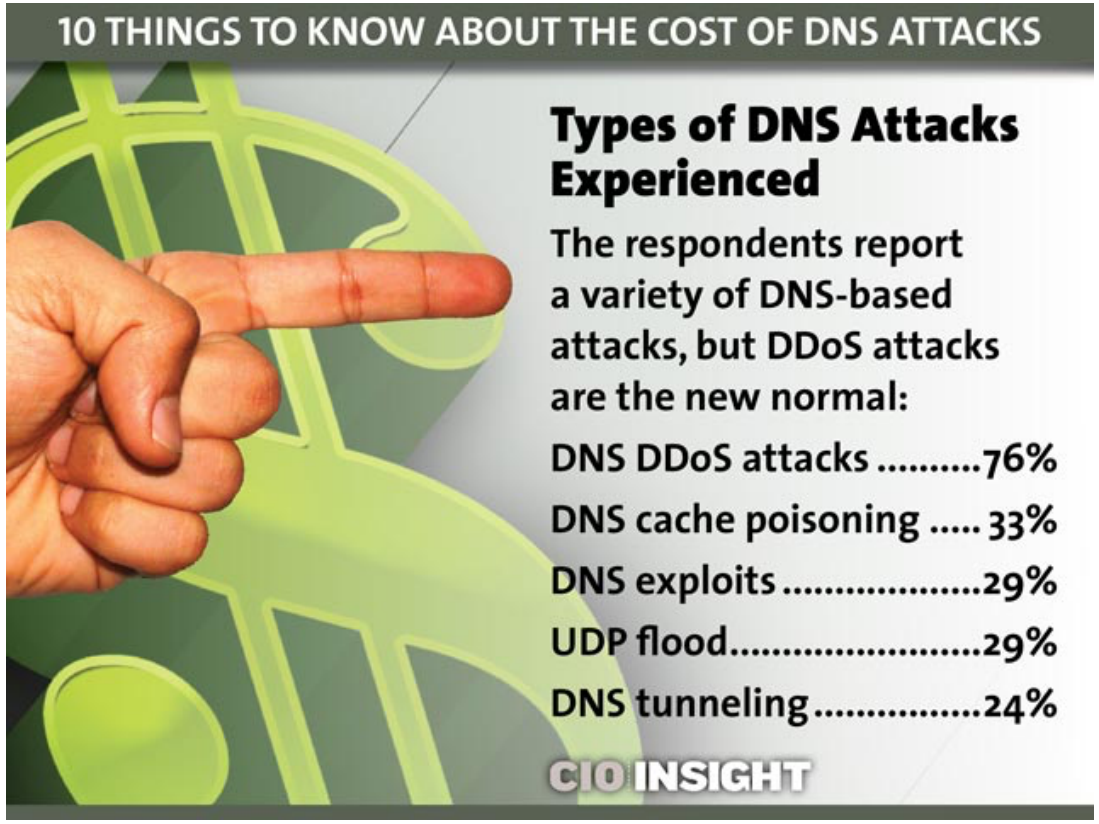


Another Definition: "DNS Abuse"

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

Examples:

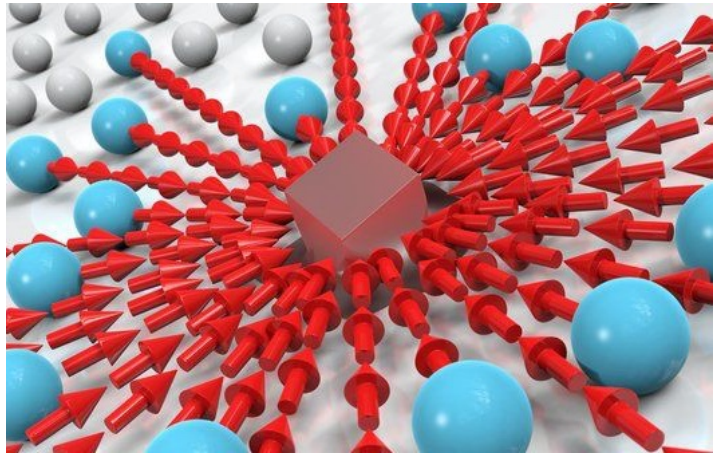
- Denial of service via DNS protocol
- Botnet command/control synchronization
- Spam-vectored threats:
  - Phishing for distribution of malware or fraud
- Infrastructure-vectored threats:
  - Cache poisoning
  - Resolver Redirection
  - DNS tunneling



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

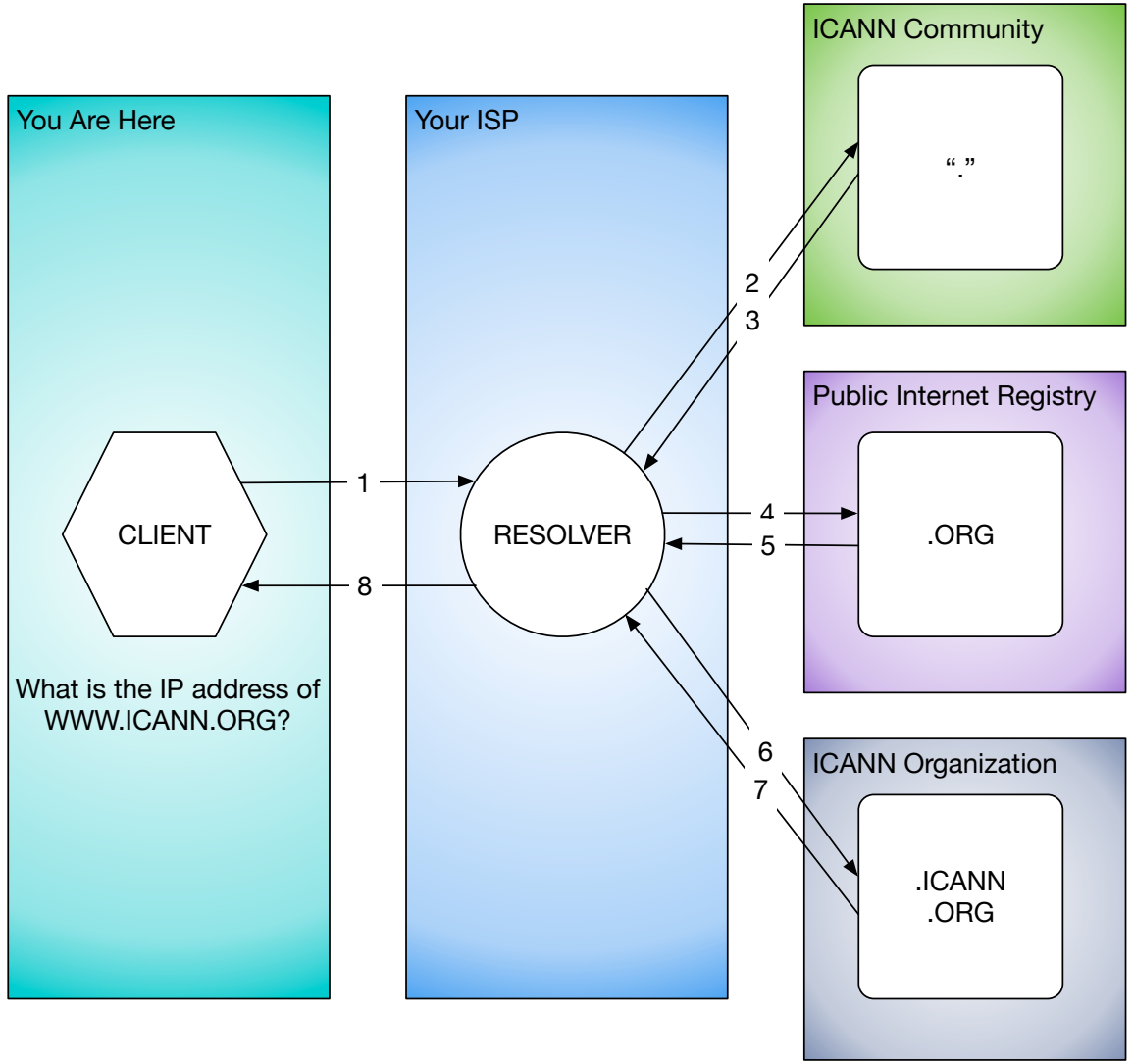
ICANN's Efforts to Mitigate DNS Abuse

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



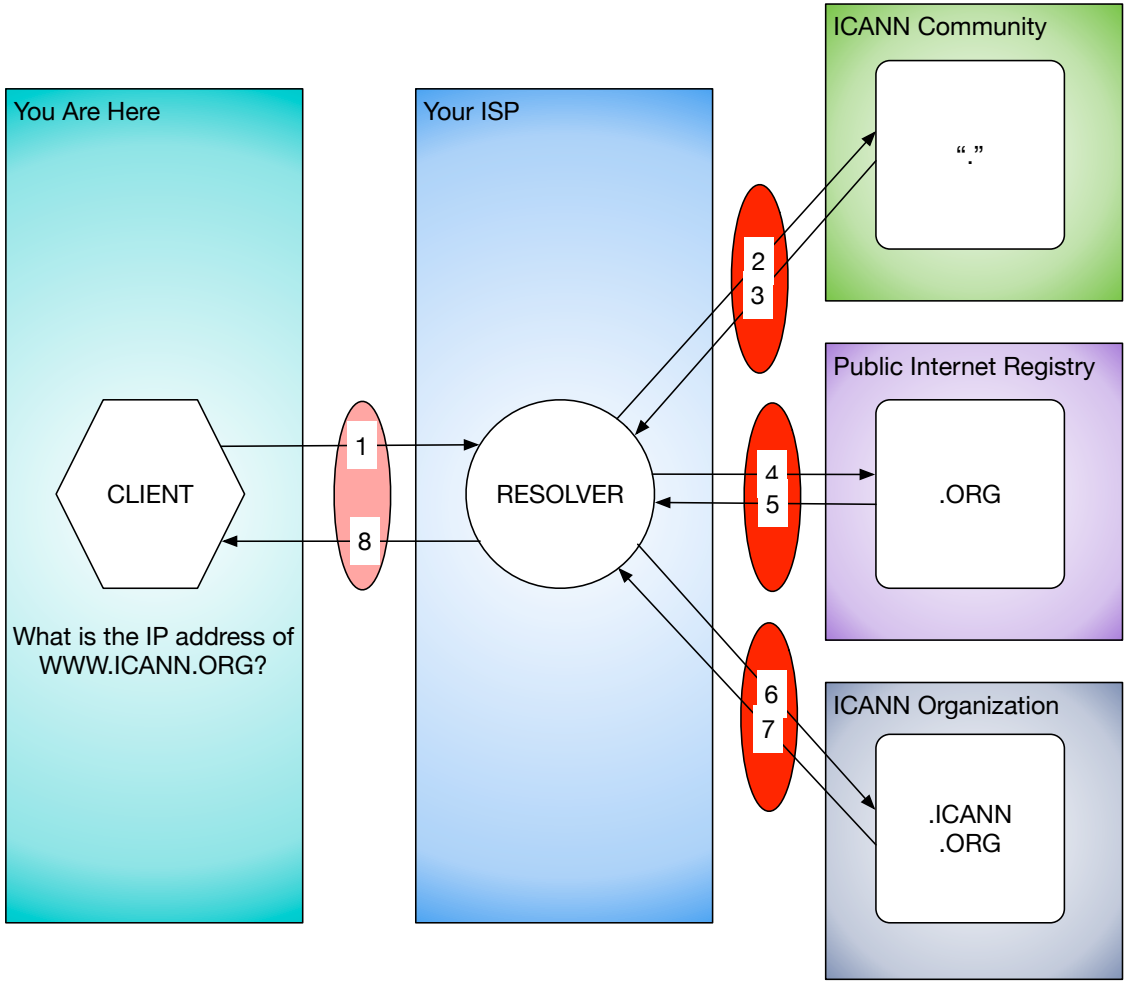
DNS at a (Very) High Level

- 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.



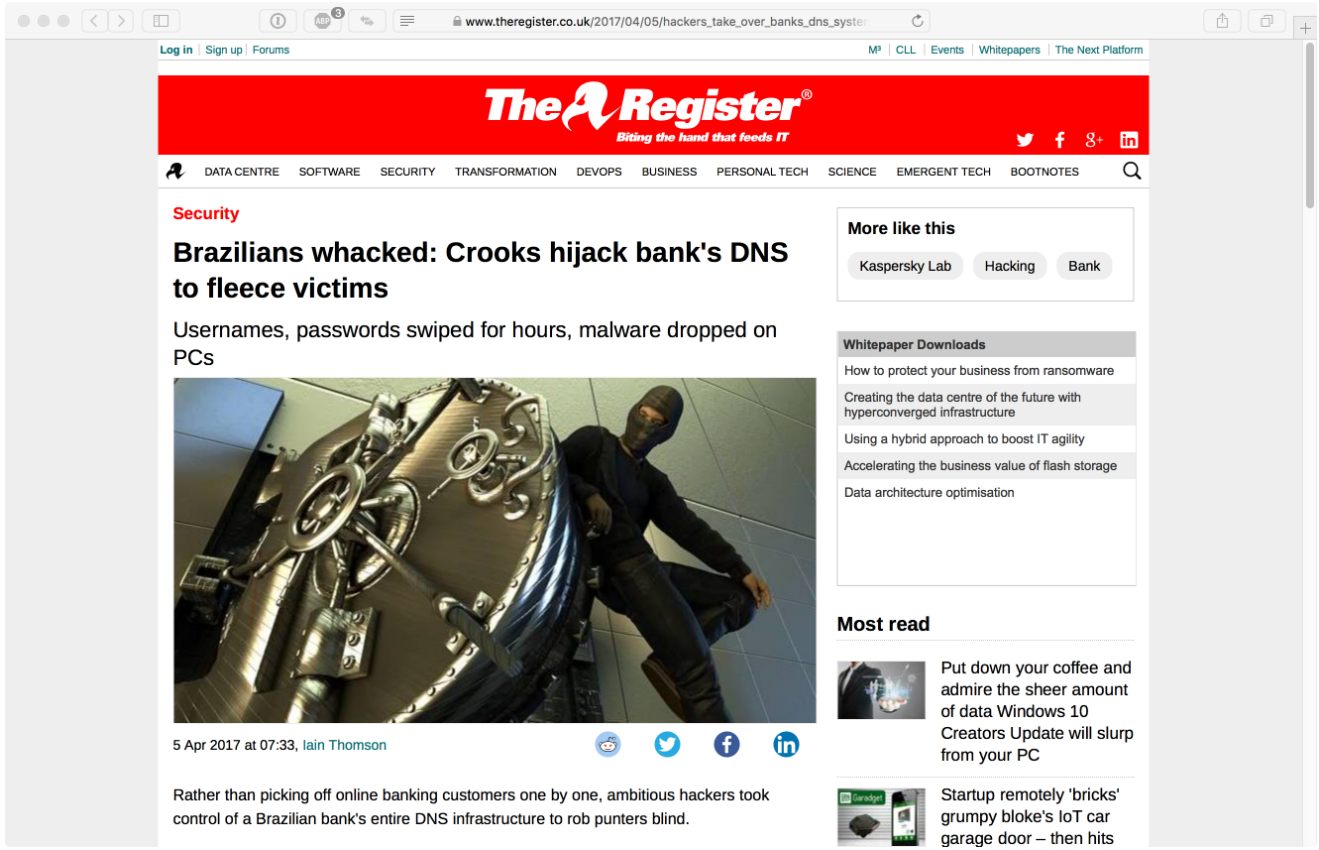
Why? A (Very) Recent Example…

- "[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



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.

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

Ongoing DNSSEC Efforts

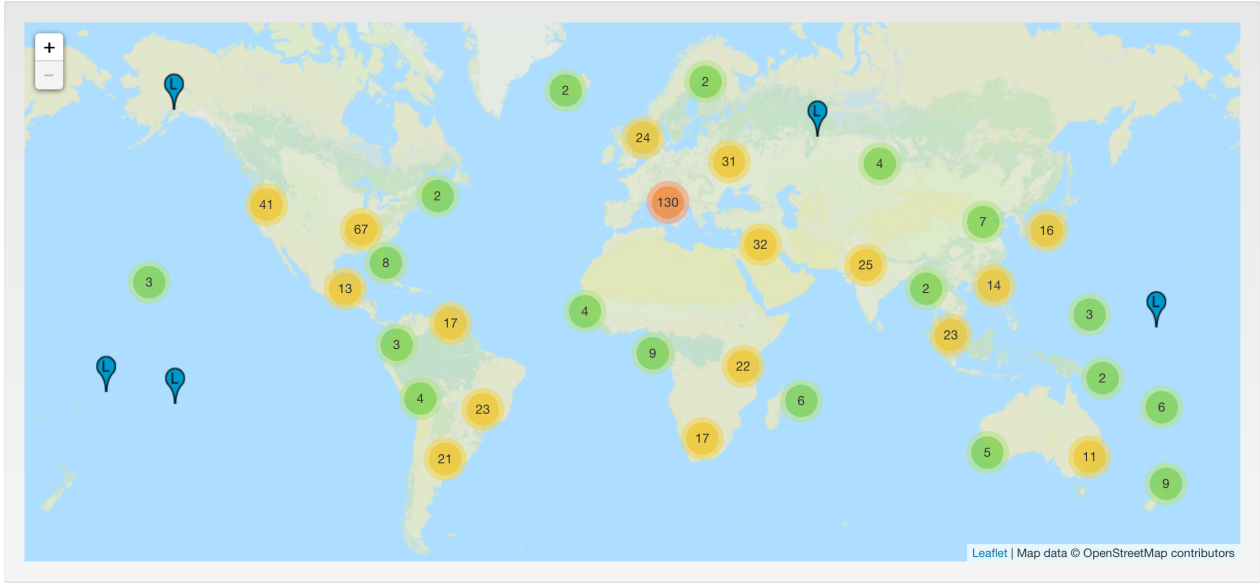
- DNSSEC: Security enhancements to the DNS
  - Fixes a known vulnerability, improves DNS trustability
- Two Inter-related Efforts
  1. DNSSEC-sign zones: **add cryptographic signatures** to DNS data
     - Done by domain name holders, i.e., IANA for root, Registries for TLDs, Registrants for 2nd-level 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"
- Process to roll the key underway
- Postponed due to new data suggesting unexpectedly high misconfiguration
- New date for roll not yet identified
- Resolver Operators MUST update the root key in their servers
- If they do not, all lookups in signed zones will fail

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

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann