OCTO at the ISPCP Outreach Session

Adiel A. Akplogan
VP, Technical Engagement

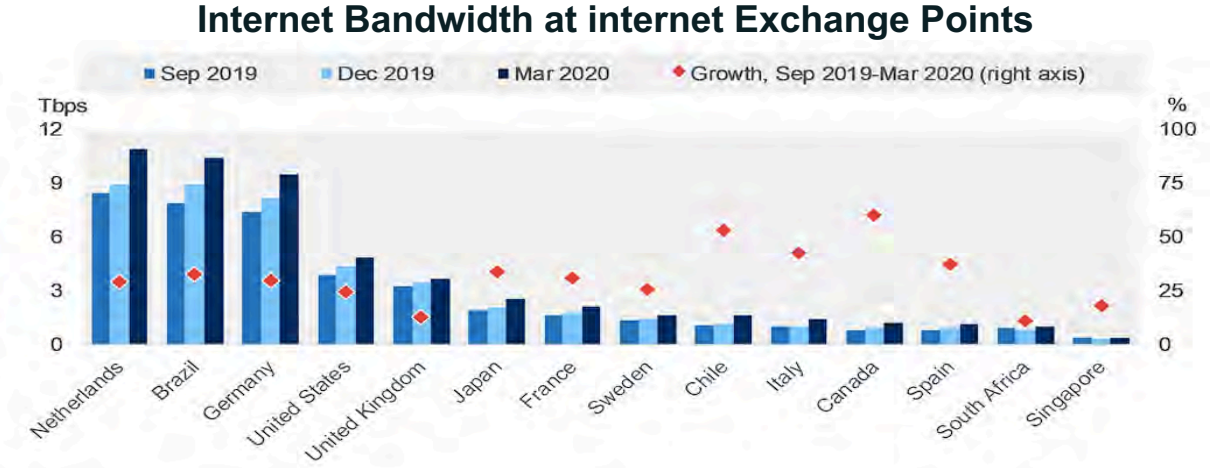
ISPCP Outreach Session – **ICANN69**
15 October 2020

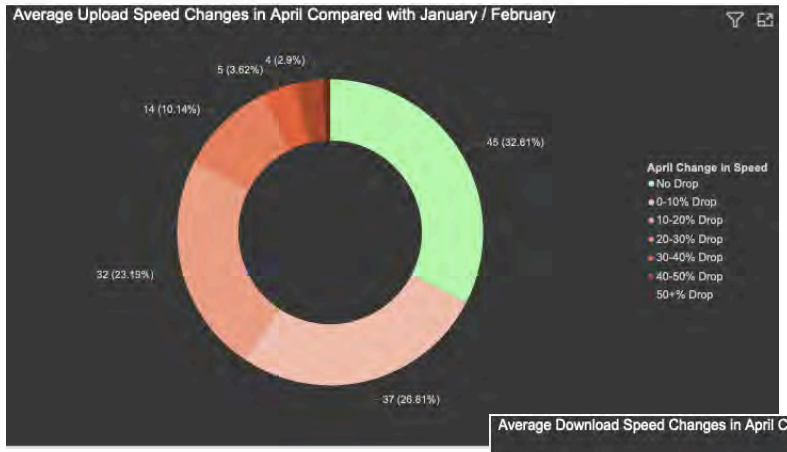
Global Impact on Infrastructure

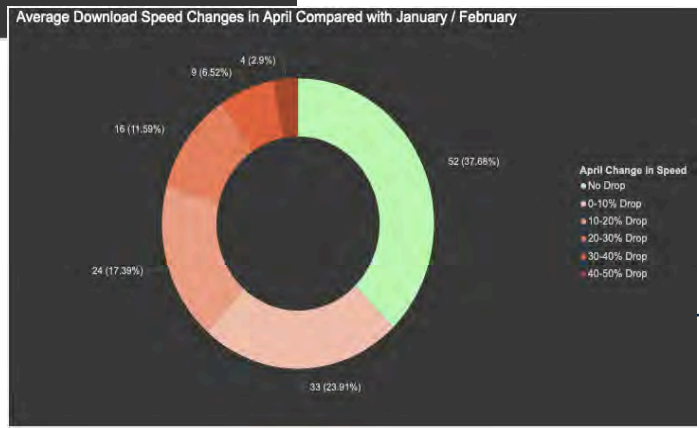
- Overall demand for broadband communication services has increased along with the Internet traffic compared to before the crisis (20% - 30% - with some operators reporting as much as a 60% increase).

- Change in traffic patterns with Significant increase in upstream traffic. Significant growth as well in residential areas (down in downtown) with the usual peak hours evolving from 5 pm-11 pm to 8 am-11 pm.

- Not quiet surprisingly some operators have also reported increases in security threats: Nokia has measured and reported about 40% increase in daily DDoS attacks between February and March.





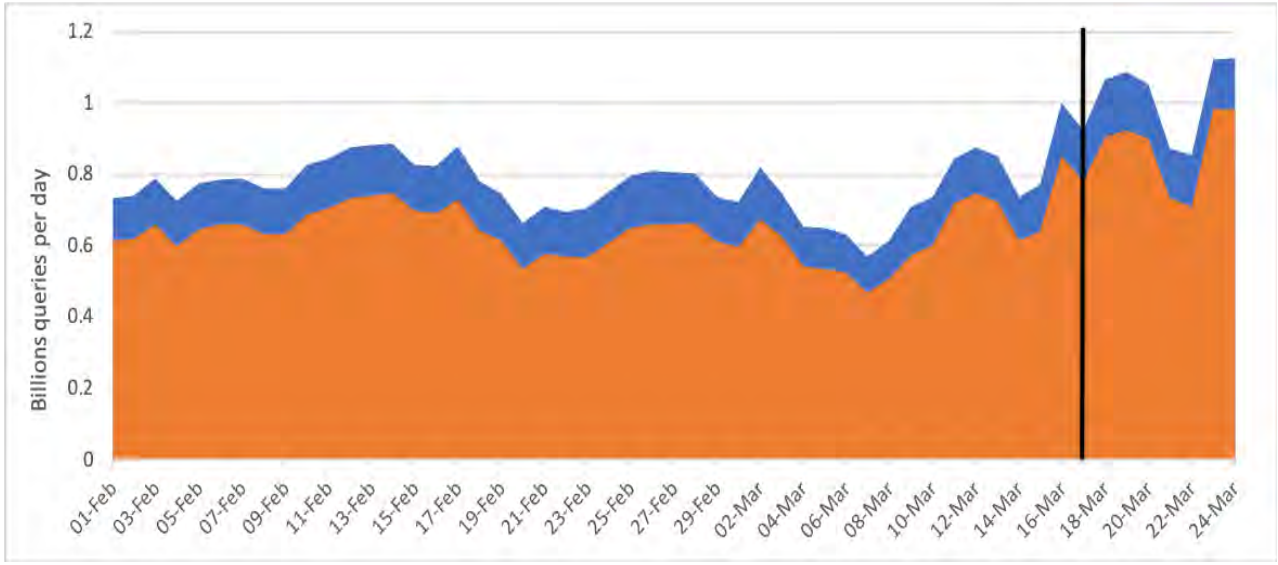


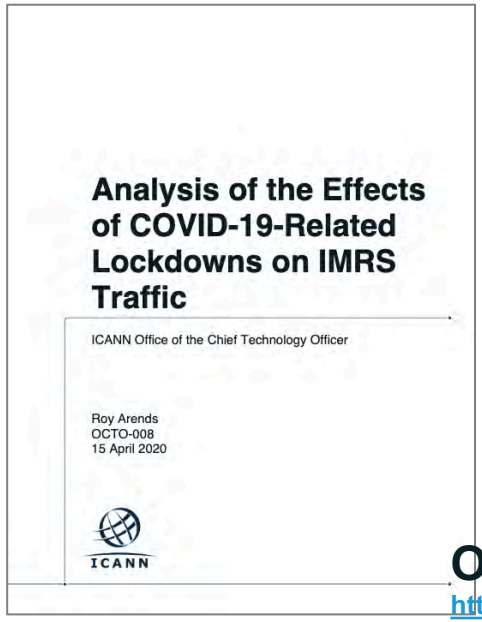
→ Network operators and content providers have overall been successful in maintaining services even if in many countries the upload and download speed has been impacted negatively

ICANN Study: Traffic at the Root

- Increase in DNS queries starting at the black line on 18 March 2020.
- The orange area shows the number of failures (TLDs queried at the root, but which do not actually exist), which increase in direct proportion to the increased number of queries.

** You have probably noticed that most root server traffic is “noise” (Non existing domain names)




Analysis of the Effects of COVID-19-Related Lockdowns on IMRS Traffic

ICANN Office of the Chief Technology Officer

Roy Arends
OCTO-008
15 April 2020

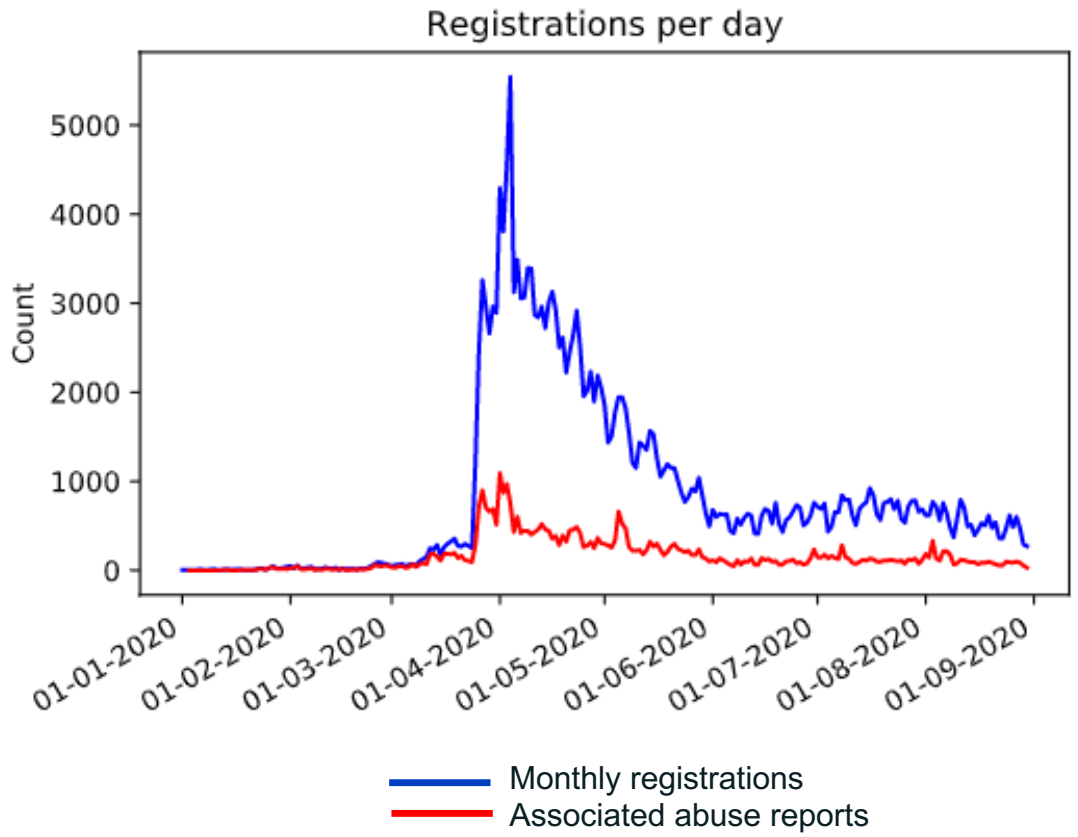
ICANN

OCTO-008

https://www.icann.org/en/system/files/files/octo-008-15apr20-en.pdf

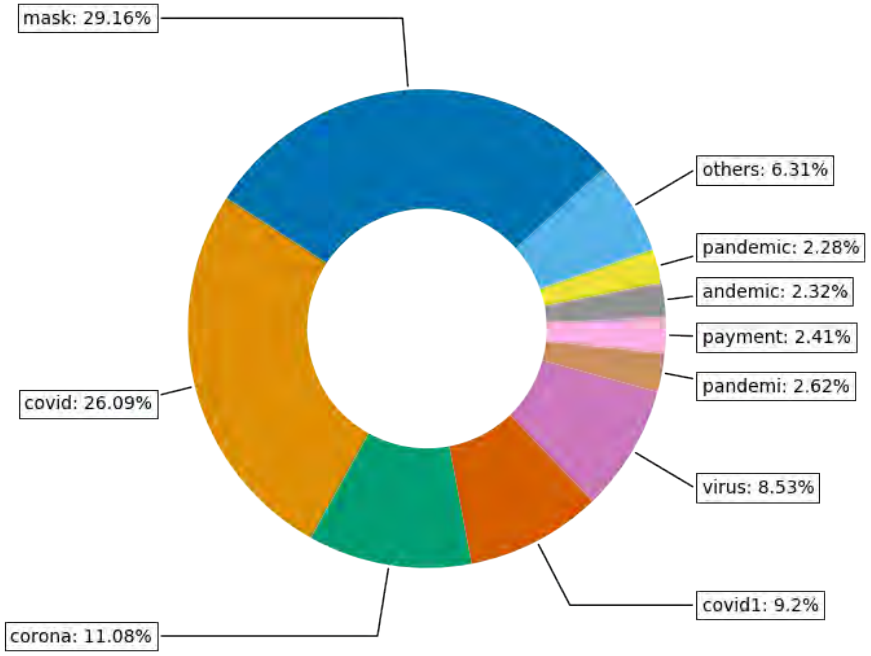
ICANN Study: CoViD-19 Domain Name Registrations Abuse

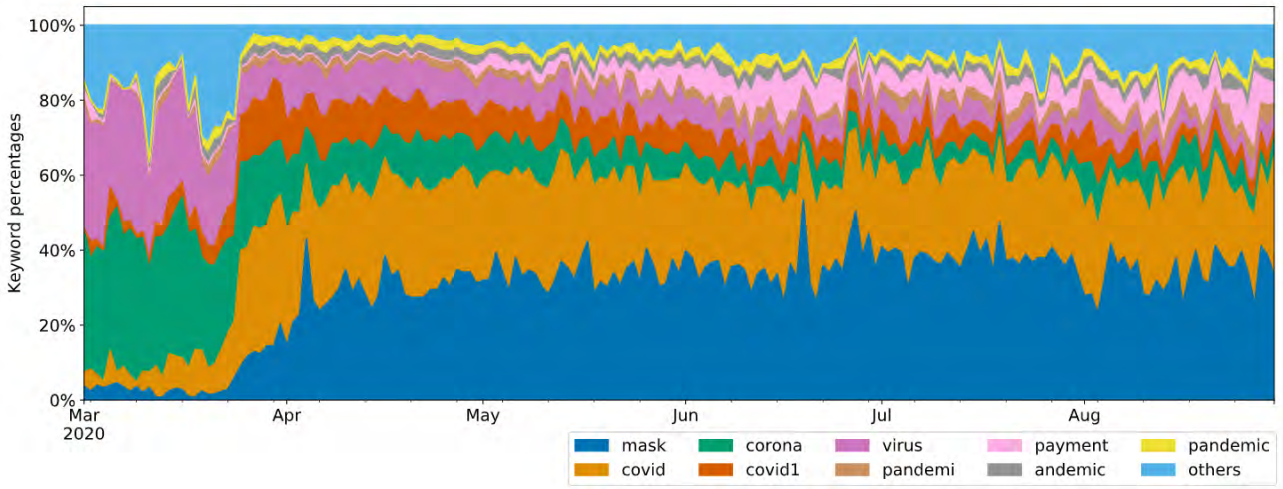
- 121,950 registrations (May-Aug)
- 8,073 had reports (and some DNS, May-Aug)
- 1,747 worth a second look (i.e. multiple credible reports)
- 126 reports sent since June (many above are likely malicious but not covid-related)



What keywords do these domains contain?

- Most of the domains related to 3 keywords
  - 4 keywords account for 73% of the domains
  - Different keywords categories:
    - Disease name (covid, ncov, sars, …)
    - Pandemic countermeasures (mask, lockdown, quarantine,…)
    - Collateral (zoom, webex, conference, …)
  - Significant number of domains matches non-English terms





THANK YOU!

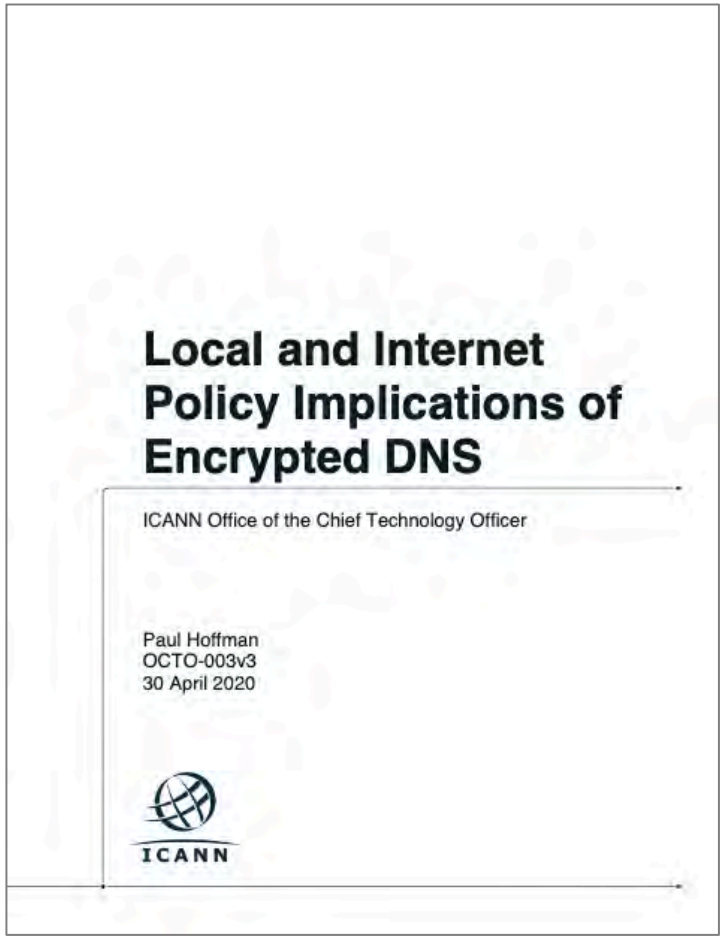
On the Horizon – Encrypted DNS (DoH)

Where are we with DNS encryption (DoH)

- DoH is a well-defined standard since 2018 now and the attention is now more on its optimum implementation.

- Vendors and operators are learning and documenting related operational considerations. As experience in implementation grow, several of the early challenge are being addressed.
  - i.e: *Discussion are on the way within the IETF to make DoH service discoverable within the scope of a service provider (ADD*)

- ICANN position has always been neutral on technology standards. However we adhere to the underlining principle that preserving the privacy of DNS users is a good things. We have published OCTO-003 that highlighted some of the potential local and policy risk associated with Encrypted DNS.
  - **Measurement of Resolver Concentration**: *As of October 2020, it takes 212 resolvers to see 50% of all Internet users. It takes 2149 resolvers to see 90% of them. These numbers have been relatively stable over the last twelve months. For context, there are millions of resolvers in the world (**ITHI Metric 5.6**)*



Ways to Help Secure and Improve the DNS **- Getting Involved**

Axes of our Technical Engagement

1. Technical Capacity Development

- Readapt training Training Catalogue to better align regional needs with ICANN Strategic Goals
- Regionalize trainings
- Develop more Online Technical Training Content
- Training Partnerships (NSRC, USTTI, CDAC …), Train the Trainers Program

2. Promoting Best Practices and Technical work

- Promoting OCTO/ICANN technical initiatives & Evolution of DNS related Technologies
- Technical assessment of policies, regulations projects and technology trends
- Provide Support to regional communities on technical topics (IDN, DNS/SEC, Security Best practices for Internet Identifiers System)
- Improve knowledge about ICANN technical advising constituencies work beyond ICANN meetings (SSAC, RSSAC, UA-SG and other …).
- Organize & Promote events and initiatives: ICANN DNS Symposium (IDS), DNS-OARC, RoW … etc

3. Facilitate Regional Contribution to Research Projects (Regional Cooperation)

- Data collection from regional Operators: DAAR (ccTLDs), ITHI, DNS Demographics, …

Current Training catalogue & Other initiatives

Course	Topic	Description	Audience	Duration (*)	Prerequisites
TE2020-1	ICANN's Technical Mission	This course will provide an overview of ICANN technical mission. Beyond the policy development coordination role for the community, ICANN plays a significant role coordinating the technical aspects of the Internet's unique identifier system (Course Outline)	General Public, Newcomers, Policy Makers.	1 hr	None
TE2020-2	DNS 101	This course will provide participants with basic knowledge of how the Domain Name System (DNS) works and how the different components interact with each other (Course Outline)	General Public, Newcomers, Policy makers with technical background, Network Engineers.	2 hrs	None
TE2020-3	DNSSEC 101	This course will discuss the DNSSEC concepts in detail covering the signing and validation of DNS data.	DNS Administrators, Policy Makers with technical background, Network Engineers.	2 hrs * 2 sessions (total 4 hrs)	DNS 101
TE2020-4	Advanced DNS	This course will discuss the DNS operations, configurations and security in detail. Participants will be involved in lab exercises to configure DNS servers and apply various security considerations.	Technical staff who are involved in the operation of DNS and managing, administering DNS servers.	2 hrs * 3 sessions (total 6 hrs)	DNS 101
TE2020-5	Advanced DNSSEC	This course will discuss the DNSSEC concepts in detail. The course also provides an understanding of DNS-based Authentication of Named Entities (DANE) protocol. Participants will be involved in lab exercises to configure DNSSEC.	Technical staff who are involved in the operation of DNS and managing, administering DNS servers.	2 hrs * 3 sessions (total 6 hrs)	DNS 101 DNSSEC 101
TE2020-6	Registry Operations for ccTLDs	This course will discuss the DNS registry operations, best practices and management aspects focusing ccTLDs.	ccTLD managers and operational staff who are involved in the registry operations.	2 hrs * 2 sessions (total 4 hrs)	DNS 101
TE2020-7	OSINT: Fighting DNS Abuse (DNS Abuse for LEAs)	This course will discuss the best practices in handling DNS abuse and various tools to identify such abuses related to DNS. The course also covers how law enforcement authorities can engage with ICANN.	Law Enforcement, CERT and CSIRT personnel who are involved in handling abuses related to Internet Identifiers.	2 hrs	DNS 101
	Security	infrastructure.	networks		
TE2020-13	UA: Email Address Internationalization	This course will discuss the Email Address internationalization (EAI) concepts and mail server compliance.	Mail Server Administrators, System Administrators, Network Engineers	2 hrs	DNS101

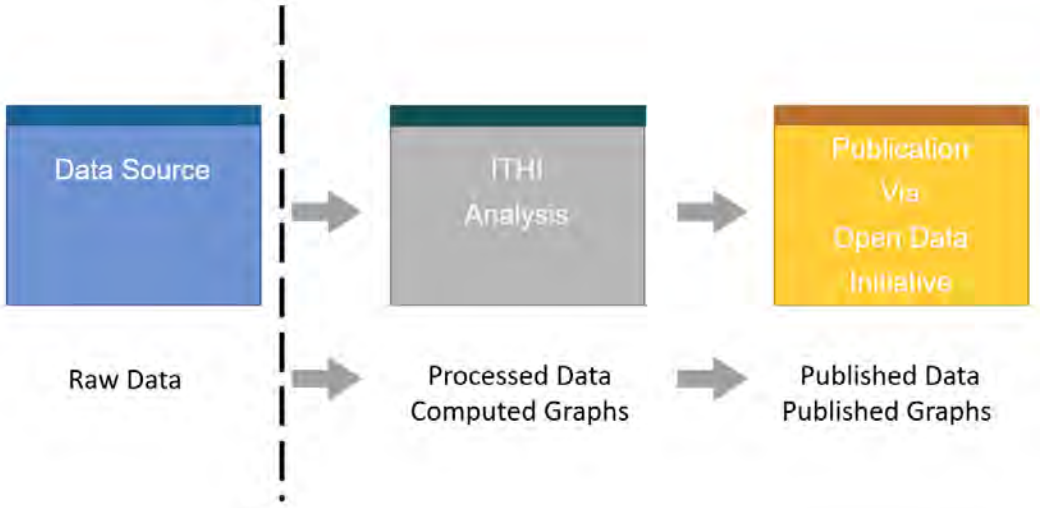
- **Promoting Hyperlocal** - Simplify hyperlocal configuration in popular resolvers (Outcome of Root zone Distribution service).
- **Roadmap for Enhance Engagement with the Public Safety Community**
- **DNS Ecosystem Observatory:** To maintain a 360º Assessment of DNS/DNSSEC implementation by operators (Countries/Region's maturity level)
- **DNS Demographics**: To provide a comprehensive dashboard to understand the demographics of the DNS components by region and country.
- **Domain Name Security Threat Identification, Collection and Reporting (DNSTICR): S**olution to identify, document and report domain names that are being actively abused.

Identifier Technologies Health Indicators (ITHI)

- **ITHI:** An initiative lunched in 2017 to measure the health of the identifiers that ICANN helps coordinate.
  - **Goal:** To produce a set of indicators that will be *measured and tracked over time* that will help determine if the set of identifiers is overall doing better or worse. It is a long-term project that is expected to run for many years.

https://ithi.research.icann.org

Metrics	Data source
M1: **Inaccuracy of Whois Data**	ICANN compliance dept.
M2: **Domain Name Abuse**	ICANN's DAAR Project
M3: **DNS Root Traffic Analysis**	Scans of DNS root traffic
M4: **DNS Recursive Server Analysis**	Summaries of recursive resolvers traffic
M5: **Recursive Resolver Integrity**	APNIC
M6: **IANA registries for DNS parameters**	Scan of recursive resolvers traffic
M7: **DNSSEC Deployment.**	Snapshots of DNS root zone
M8: **DNS Authoritative Servers Analysis**	Scans of authoritative servers traffic



How to contribute to ITHI

- **M4, M6 and M8** – In addition to global measurement we are also computing the value of these metrics as seen by cooperating partners (UNLP, Argentina, UCC, Ghana, TWNIC, Taiwan, …)

- Metrics **M4 and M5** rely on statistics collected at recursive resolvers and the traffic observed at different point of the network may vary due to many factors. We are also interested in collecting data at authoritative servers which can help understand the type of load observed by these servers.

- How to participate:
  1. Install the DNSCAP utility (maintained by DNS-OARC)
  2. Download and build the ITHI tools and run a test script to verify that the capture tools work.
  3. Obtain an SSH account on the staging server, ithi.privateoctopus.com
  4. Set up a "cron" job that capture statistics several times a week and upload them to the staging server using scp

- More about the process at https://ithi.research.icann.org/participating.html. If you still need help to go though this process you can write to us at octo@icann.org and we will be happy to help.

THANK YOU!

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: octo@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann