ICANN and the Identifier Technology Health Initiative (ITHI)
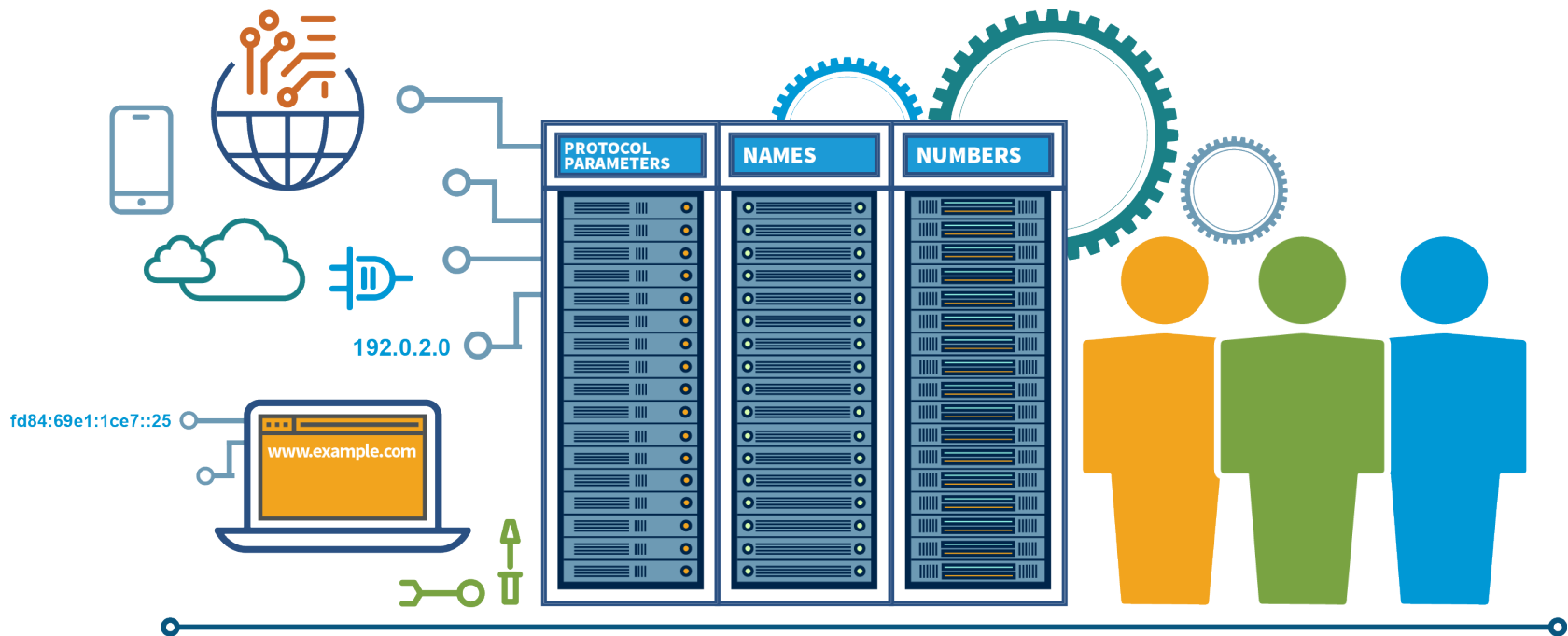
Yaovi Atohoun;
Manager for Stakeholder Engagement and operations - Africa

WACREN 2019
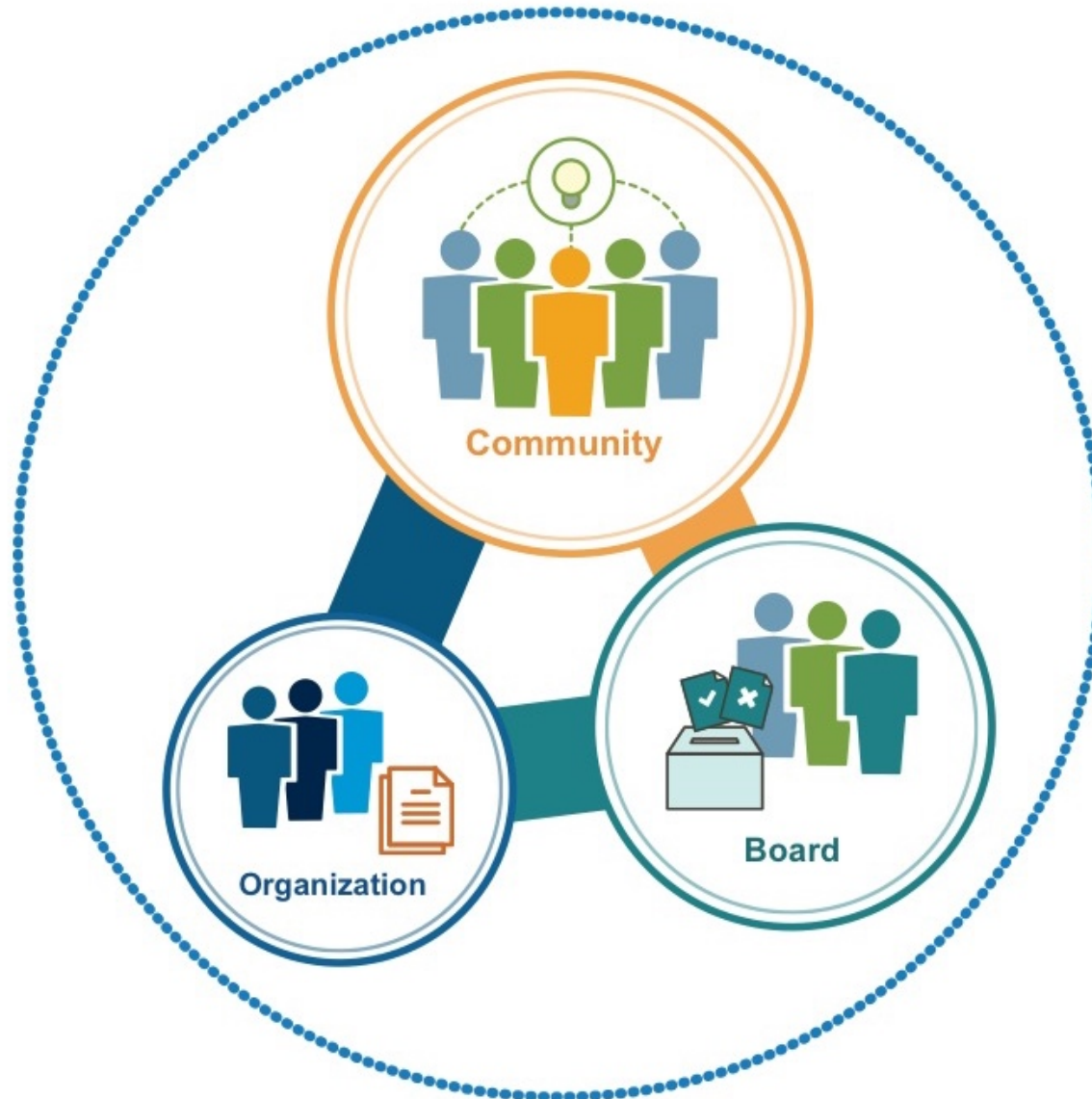15 March 2019, Accra - Ghana

ICANN

What Is ICANN?

Coordinating with our partners, we help make the Internet work.

ICANN Ecosystem

Exploring ICANN's Multistakeholder Community

ICANN | ASO
Address Supporting Organization

ICANN | ccNSO
Country Code Names Supporting Organization

ICANN | GNSO
Generic Names Supporting Organization

Supporting Organizations (SOs)

Three SOs in the ICANN community are responsible for developing policy recommendations in the areas they represent.

Address Supporting Organization (ASO)

Country Code Names Supporting Organization (ccNSO)

Generic Names Supporting Organization (GNSO)

Advisory Committees (ACs)

Four ACs give advice and make recommendations on ICANN topics.

At-Large Advisory Committee (ALAC)

Governmental Advisory Committee (GAC)

Root Server System Advisory Committee (RSSAC)

Security and Stability Advisory Committee (SSAC)

ICANN AT-LARGE

ICANN | GAC
Governmental Advisory Committee

ICANN | RSSAC
Root Server System Advisory Committee

ICANN | SSAC
Security and Stability Advisory Committee

Get Involved and Informed

Attend an ICANN Public Meeting. Three times a year, ICANN holds free and open public meetings in different regions around the world. Visit **meetings.icann.org** to learn more.

Visit **go.icann.org/journey** to learn how you can attend an ICANN Public Meeting as part of the NextGen@ICANN or ICANN Fellowship programs.

Take a free online course at **learn.icann.org**.

Attend events in your region.

Find and participate in an ICANN community group by visiting **icann.org/community**.

Sign up for ICANN news alerts and regional newsletters.

Mailing list AFRICANN: https://lists.afrinic.net/mailman/listinfo.cgi/africann

Support to the community

Fellowship	https://www.icann.org/fellowshipprogram

NextGen	https://www.icann.org/public-responsibility-support/nextgen

Newcomer	https://www.icann.org/newcomers

10 Open Leadership Positions to be filled by the 2019 NomCom

Internet Corporation of Assigned Names and Numbers (ICANN)
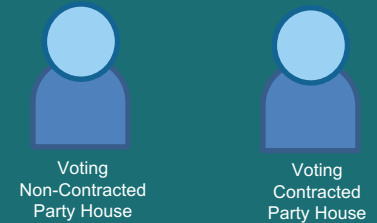
Public Technical Identifiers (PTI)
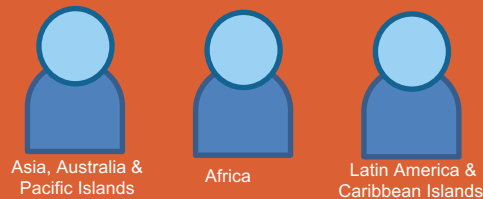
PTI Board of Directors
1 seat | 3 year term

ICANN Board of Directors
3 seats | 3 year term

GNSO Council
2 seats | 2 year term

Voting
Non-Contracted
Party House

Voting
Contracted
Party House

At Large Advisory Committee
3 seats | 2 year term

Asia, Australia &
Pacific Islands

Africa

Latin America &
Caribbean Islands

ccNSO Council
1 seat | 3 year term
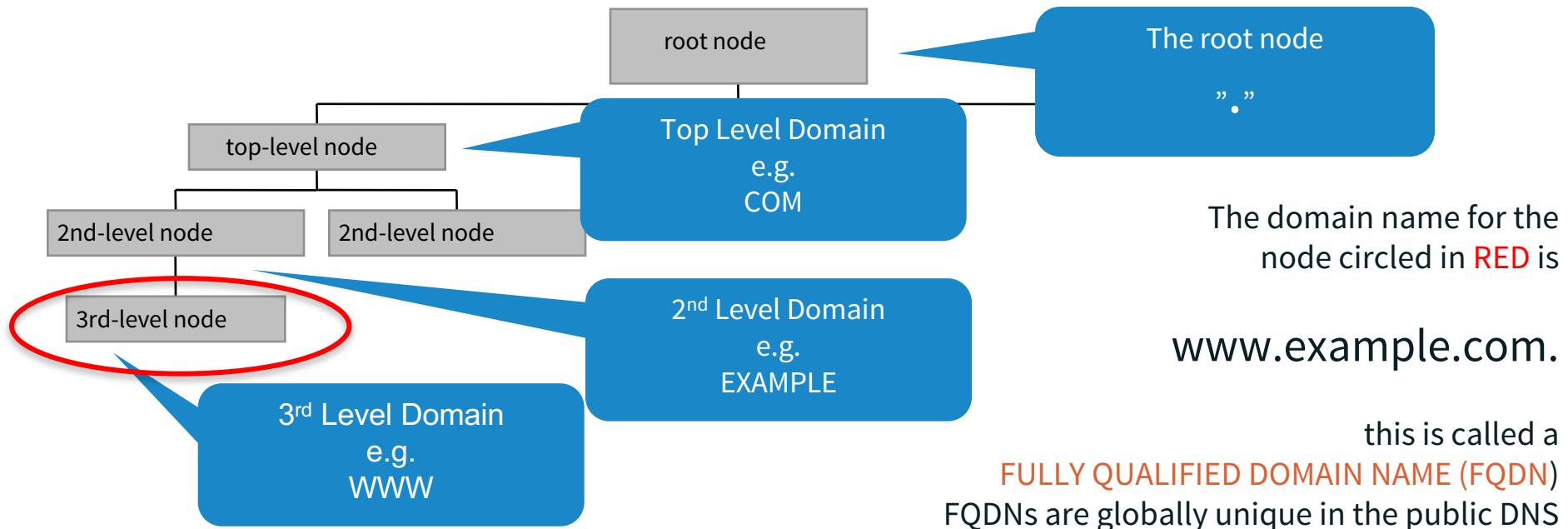
8

2019 NomCom Timeline
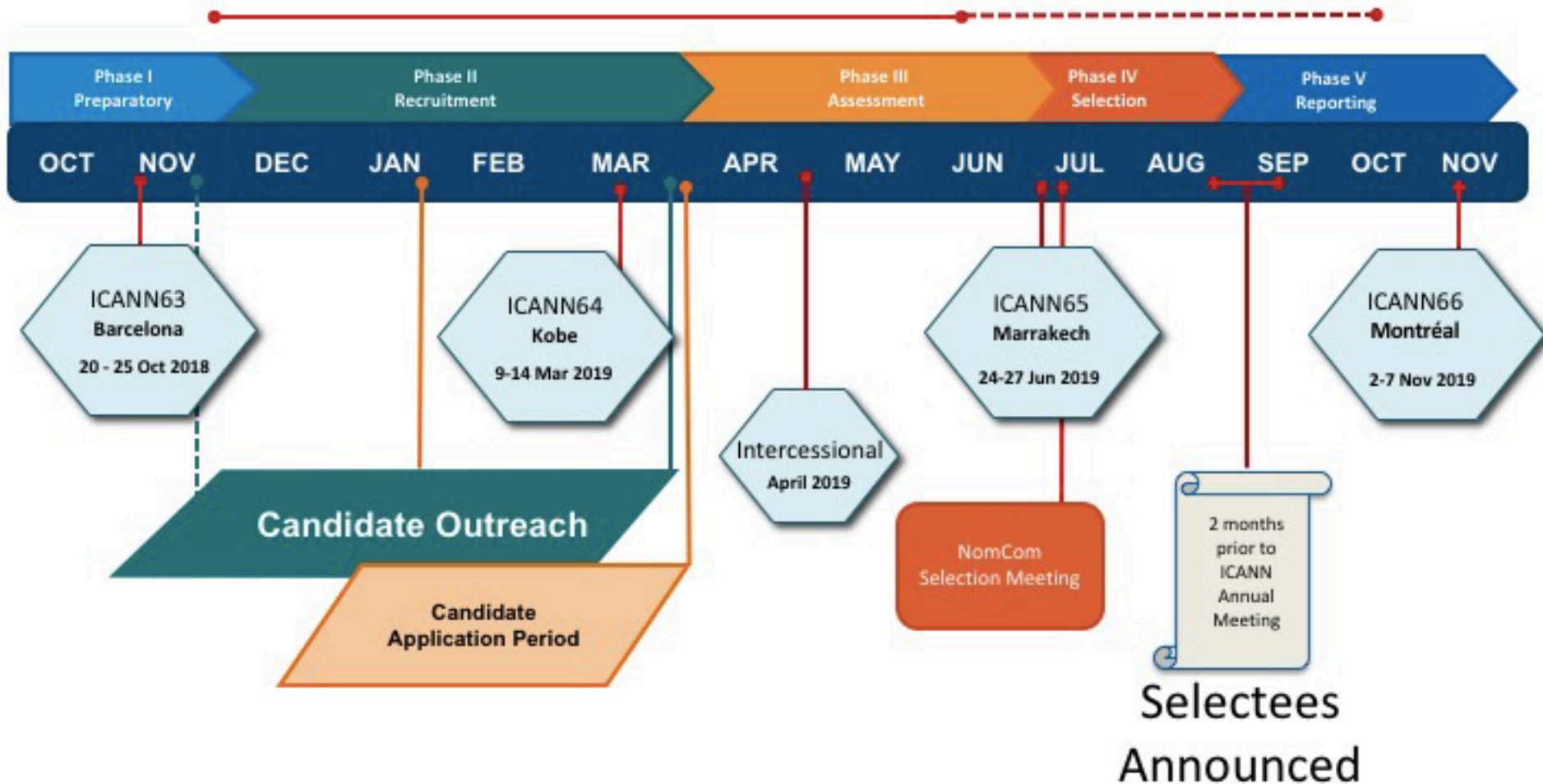
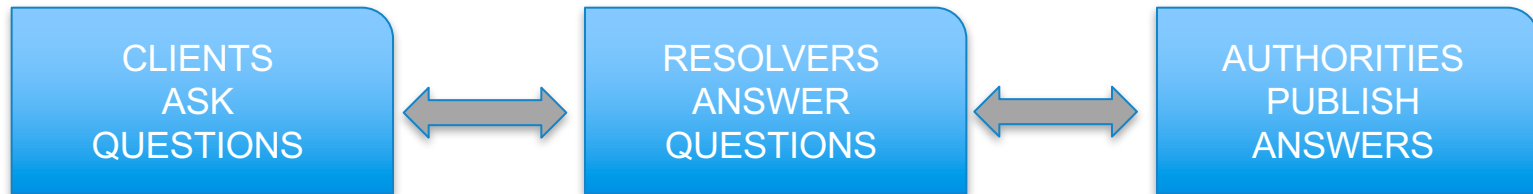# Identifier Technology Health Indicator (ITHI)

Definitions: Labels and Domain Names

Each node in the DNS name space has a label
The domain name of a node is the list of the labels on the path from the node to the root of the DNS

root node

top-level node

2nd-level node   2nd-level node

3rd-level node

The root node

"."

Top Level Domain
e.g.
COM

2nd Level Domain
e.g.
EXAMPLE

3rd Level Domain
e.g.
WWW

The domain name for the node circled in RED is

www.example.com.

this is called a
FULLY QUALIFIED DOMAIN NAME (FQDN)
FQDNs are globally unique in the public DNS

ICANN

Operational elements of the DNS

CLIENTS ASK QUESTIONS	⟷	RESOLVERS ANSWER QUESTIONS	⟷	AUTHORITIES PUBLISH ANSWERS

- **Authoritative** Name Servers host zone data
  - The set of "DNS data" that the registrant publishes
- **Recursive** Name Resolvers ("resolvers")
  - Systems that find answers to queries for DNS data
  - **Caching** resolvers find and store answers locally for "TTL" period of time
- **Client** or "**stub**" resolvers
  - Software in applications, mobile apps or operating systems that query the DNS and process responses

ITHI Phases

- **Phase 1: Analysis (2015-2016)**
  - Strategic choice to define problem areas first
  - Many discussions with the larger community
  - Split of project ICANN / RIR

- **Phase 2: Development**

- Building platform
  - Finding partners
  - Getting data

We are here now

Simplified Dashboard

Home	Metrics	Participate	About

ITHI by ICANN		Full table
Identifier Technology Health Indicator		**As of Jan 2019**
% No Such Domain queries seen by root servers		**70.63%**
% of resolvers that perform DNSSEC validation		**28.10%**
%requests to top name at the root	.HOME	**3.09%**
%requests to top name at resolvers	.MAIL	**2.80%**
Number of resolvers accounting for 50% of eyeballs		Coming soon
Phishing Domains per 10,000 registered names		**2.51**

The home page at ithi.research.icann.org provides a quick view of chosen indicators.

Complete Dashboard

ITHI by ICANN	Identifier Technology Health Indicator		As of Jan 2019	Past 3 months	Historic Low	Historic High
Root Server Health	% No Such Domain queries seen by root servers		70.63%	68.39%	62.95%	69.40%
DNSSEC Deployment	% of resolvers that perform DNSSEC validation		27.67%	24.72%	23.43%	27.29%
Name collision	%requests to top 3 names at the root	.HOME	3.09%	3.15%	2.90%	3.67%
		.LOCAL	2.82%	3.70%	2.52%	4.47%
		.IP	0.82%	0.84%	0.54%	0.92%
	%requests to top 3 names at resolvers	.MAIL	2.00%	0.99%	0.00%	2.55%
		.UNIFI	0.07%	0.05%	0.03%	0.07%
		.LOCAL	0.03%	0.04%	0.00%	0.06%
Resolver Concentration	Number of resolvers accounting for 50% of eyeballs		Coming soon			
	Number of resolvers accounting for 90% of eyeballs		Coming soon			
Dns Abuse (as of Nov 2018, measured on 1210 GTLD and 2280 registrars)	Abuse Domains per 10,000 registered names	Phishing	2.51	2.57	2.31	2.87
		Malware	1.62	1.67	1.10	1.83
		Botnets C&C	0.15	0.16	0.11	1.48
		Spam	42.03	41.15	40.47	61.89
	Number of GTLD to account for 50% of abuses	Phishing	1	1.00	1	2
		Malware	2	2.33	1	3
		Botnets C&C	1	2.00	2	2
		Spam	4	4.00	3	4
	Number of GTLD to account for 90% of abuses	Phishing	13	15.00	11	16
		Malware	10	10.33	7	11
		Botnets C&C	5	5.00	4	5
		Spam	25	24.33	18	25

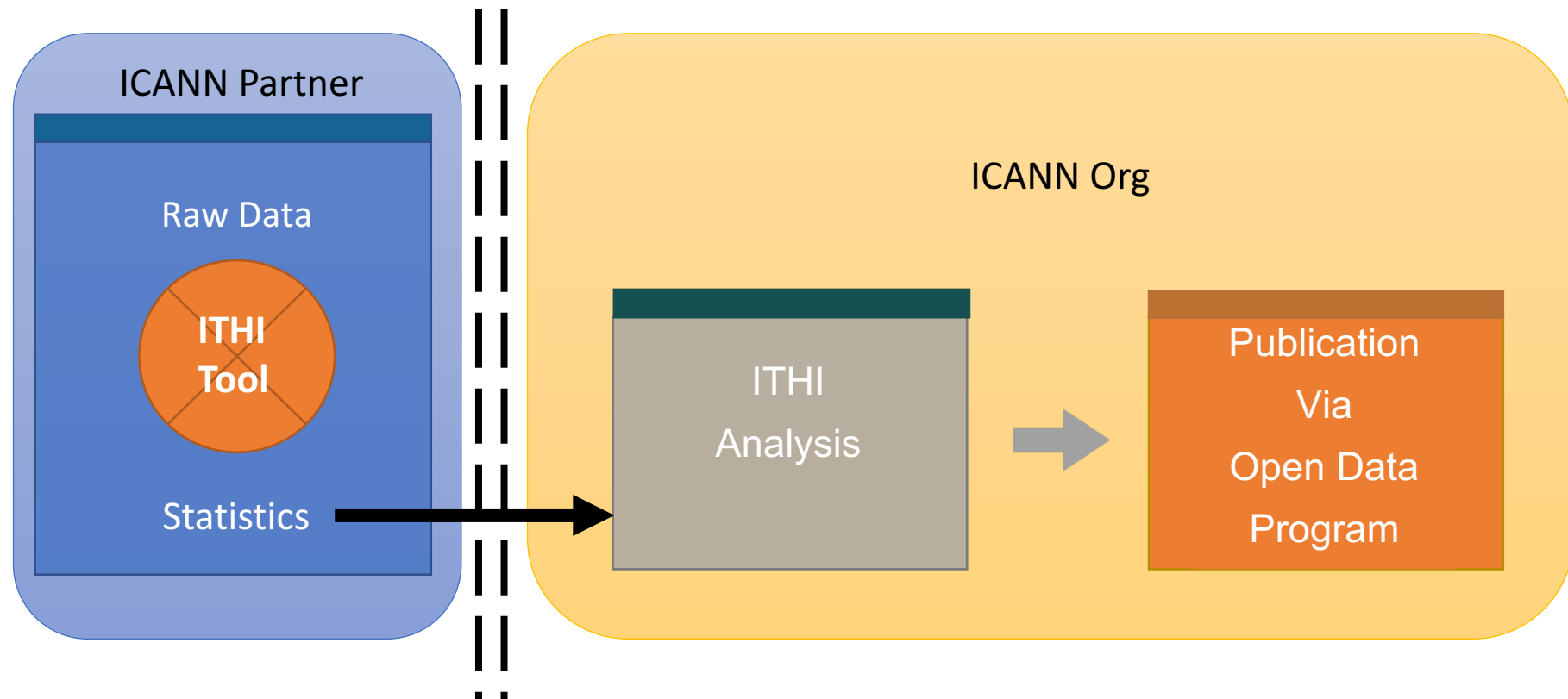| Metric	Name	Data Source
M1:	Inaccuracy of Whois Data	ICANN compliance dept.
M2:	Domain Name Abuse	ICANN's DAAR Project https://www.icann.org/octo-ssr/daar
M3:	DNS Root Traffic Analysis	Samples of DNS root traffic
M4:	DNS Recursive Server Analysis	Summaries of recursive resolvers traffic
M5:	DNS Resolver Behavior	APNIC
M6:	IANA registries for DNS parameters	Scan of recursive resolvers traffic
M7:	DNSSEC Deployment	Snapshots of DNS root zone
M8:	DNS TLD Traffic Analysis	Summaries of TLD traffic

Strategic Choice: From Problems to Measurements

⊙ Technical focus

⊙ **Problem areas → Metrics → Measurement**

⊙ Current value and trend over time
  ○ Automated process to collect & analyze data

⊙ Measurement, not interpretation

Strategic choice: ICANN Data + Partners + Contracts

- ⊙ **ICANN (Internal Data)**
  - ○ Compliance department (M1)
  - ○ DAAR (M2)
  - ○ L-Root data (M3)
  - ○ Root zone (M7)

- ⊙ **measurements with partners**
  - ○ Measurements at recursive & authoritative servers
  - ○ M4, M6, M8

- ⊙ **Outside measurement**
  - ○ APNIC/Google Ads platform
  - ○ Eyeball view of resolvers M5

Strategic Choice: Privacy

ICANN Partner

Raw Data

ITHI Tool

Statistics

ICANN Org

ITHI Analysis

Publication Via Open Data Program

No PII, only statistics, are sent to ICANN org

No "naming and shaming"

Partner's Role

- ⊙ **Keep partners in control of their data**
  - ○ They run the tools on their machines
  - ○ They upload data on the staging server
  - ○ We provide assurance about tool quality, privacy
  - ○ We also provide "local view" of the statistics

- ⊙ **Early Warning System**
  - ○ Partners can decide to share their data with others in exchange for reciprocity
  - ○ Comparing results can serve as an early warning system
  - ○ if a collection point observes a divergence from its baseline but others point don't, it might be an indicator that an attack is under way.

ITHI Software

- ⊙ **DNSCAP Plug-in (running at partner's site)**
  - ○ Leverage existing code
  - ○ Extract information from DNS transactions
  - ○ Processes at line rate, create small summaries

- ⊙ **Tools (running on project VM)**
  - ○ Summarize the summaries, compute metrics
  - ○ From metrics, prepare data for web pages

- ⊙ **Designed for speed (C++), reliability, privacy**
  - ○ Open source (github.com/private-octopus/ithitools)
  - ○ Code: 23 KLOC, tests: 7 KLOC
  - ○ Code reviewed performed by NLLab

ITHI Operation at Partners

- **Agree** to work with us (outreach effort)

- **Install** tools

- **Get account** on staging server (SSH)

- **Set up captures**:
  - At least 4 times a week
  - Typically 1 million transactions per session

- **Set up upload scripts**

- **Verify behavior** with "partners only" pages on web server

Current Partners

- ⊙ **Active partners:**
  - ○ [National University of La Plata (UNLP), Argentina](#),
  - ○ [University of Cape Coast, Ghana](#),
  - ○ [DNS Nawala, Indonesia](#),
  - ○ Kaznic, Kazakhstan (.KZ)
  - ○ TWNIC, Taiwan

  - ○ To become a partner
    Please contact   ithi-info@icann.org

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: email

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg

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

instagram.com/icannorg

Contact GSE Africa team: queries.nairobiec@icann.org