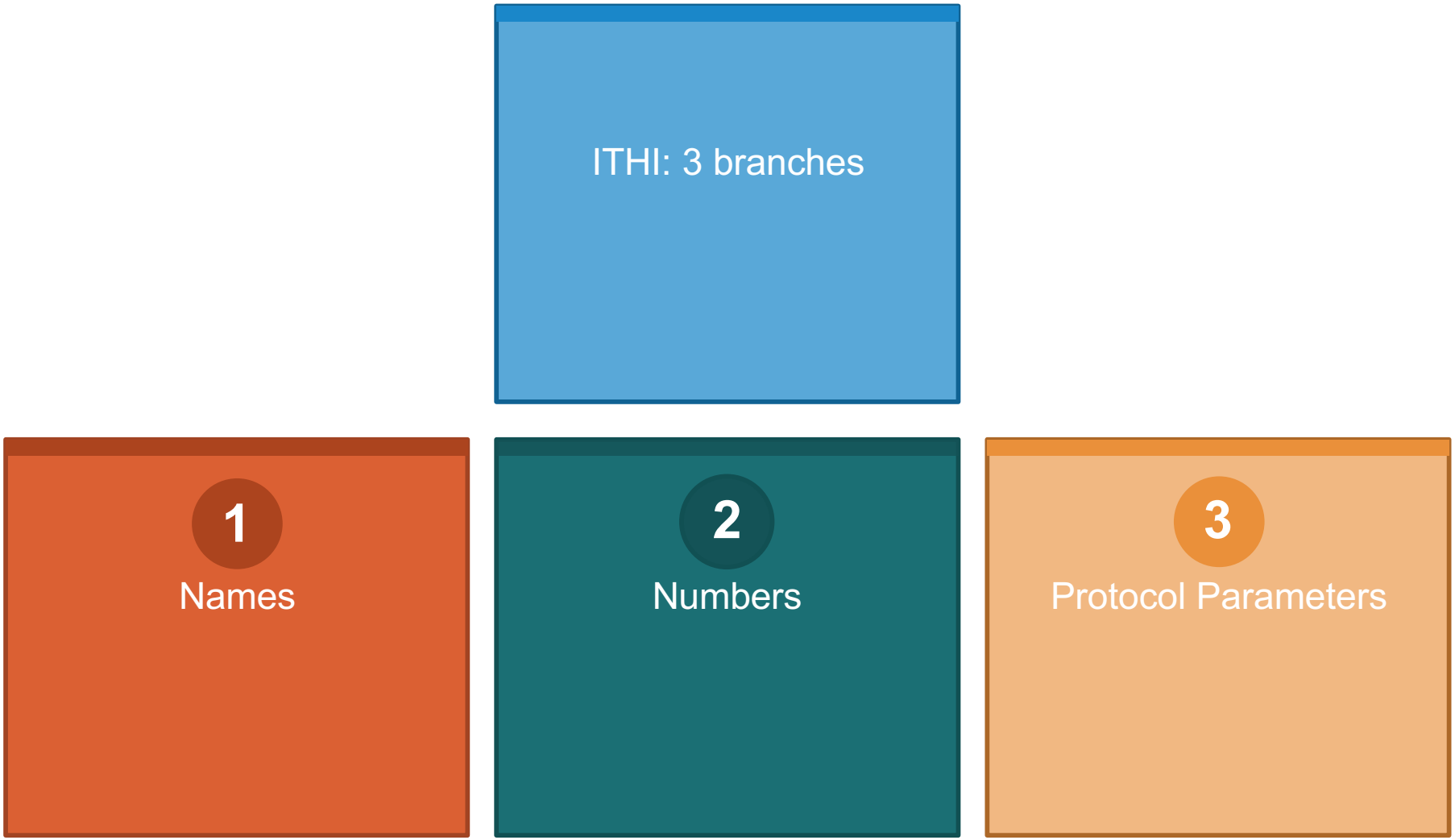
ITHI Update

Alain Durand

TLDCon
September 2017

ITHI Branches



ITHI GOAL

- ITHI: Identifier Technology Health Indicators
- Track over time a set of indicators that reflect the “health” of the system of identifiers ICANN
- The “actual” value of any of those indicators may not as important to us as the trend they are on.
- ITHI work will stop at presenting the data and leave it to the community to take any action deemed necessary (e.g. new policy).

ITHI: 3 sets of Identifiers

- ICANN helps coordinate 3 sets of identifiers:
  - Names
  - Numbers
  - Protocol Parameters

- As such, we have 3 different initiatives:
  - ICANN office of the CTO, looking at Names
  - NRO, looking at Numbers
  - ICANN office of the CTO, looking at IANA Protocol Parameters registries linked to the DNS

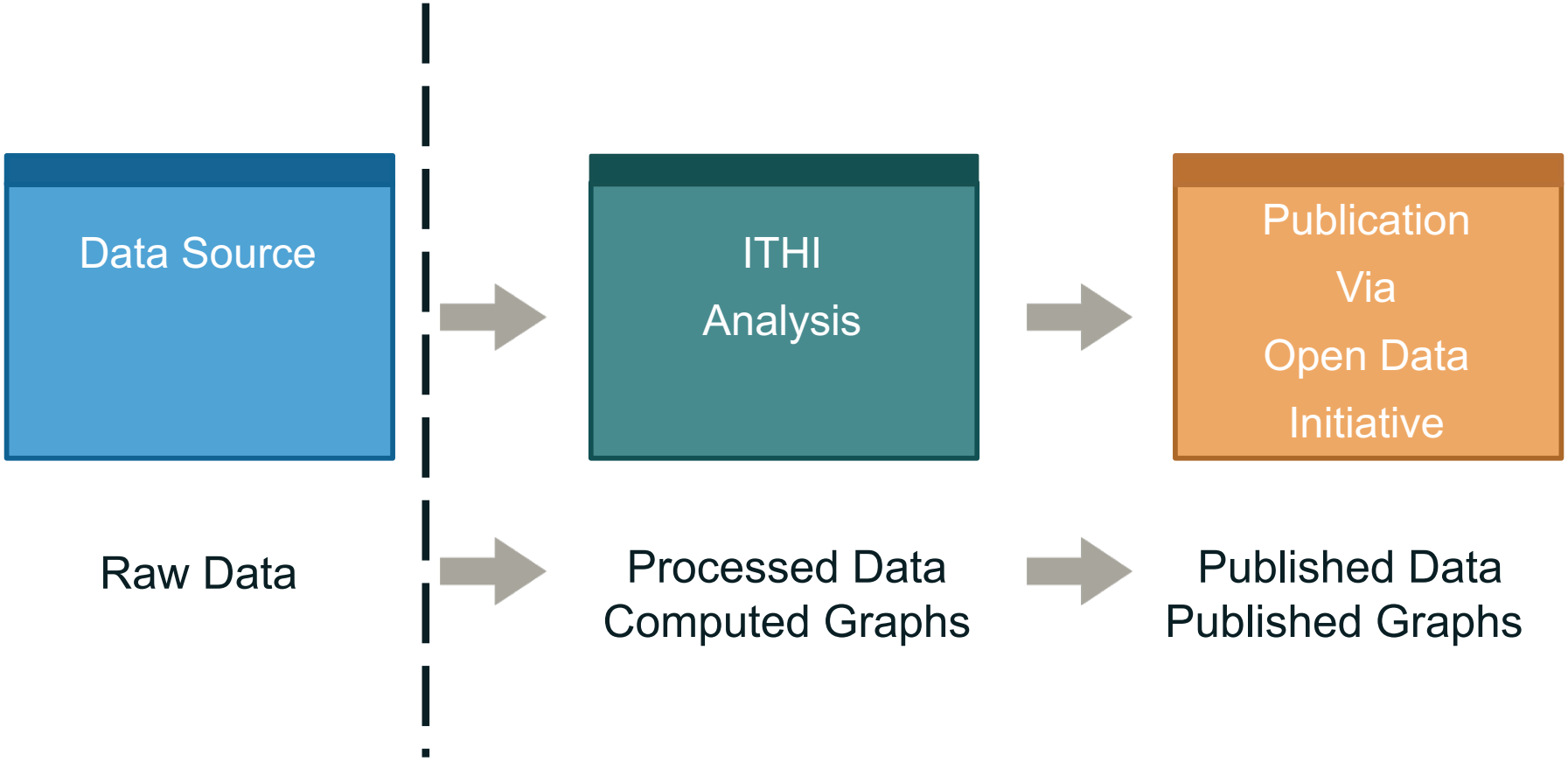
ITHI: Names

- We have identified 5 “Problem Areas”:
  - Data (In-)Accuracy
  - Abuse
  - Overhead in Root Traffic
  - Leakage
  - Lies

- Over time, new problem areas could be defined, and/or some could removed.

ITHI Names: Process

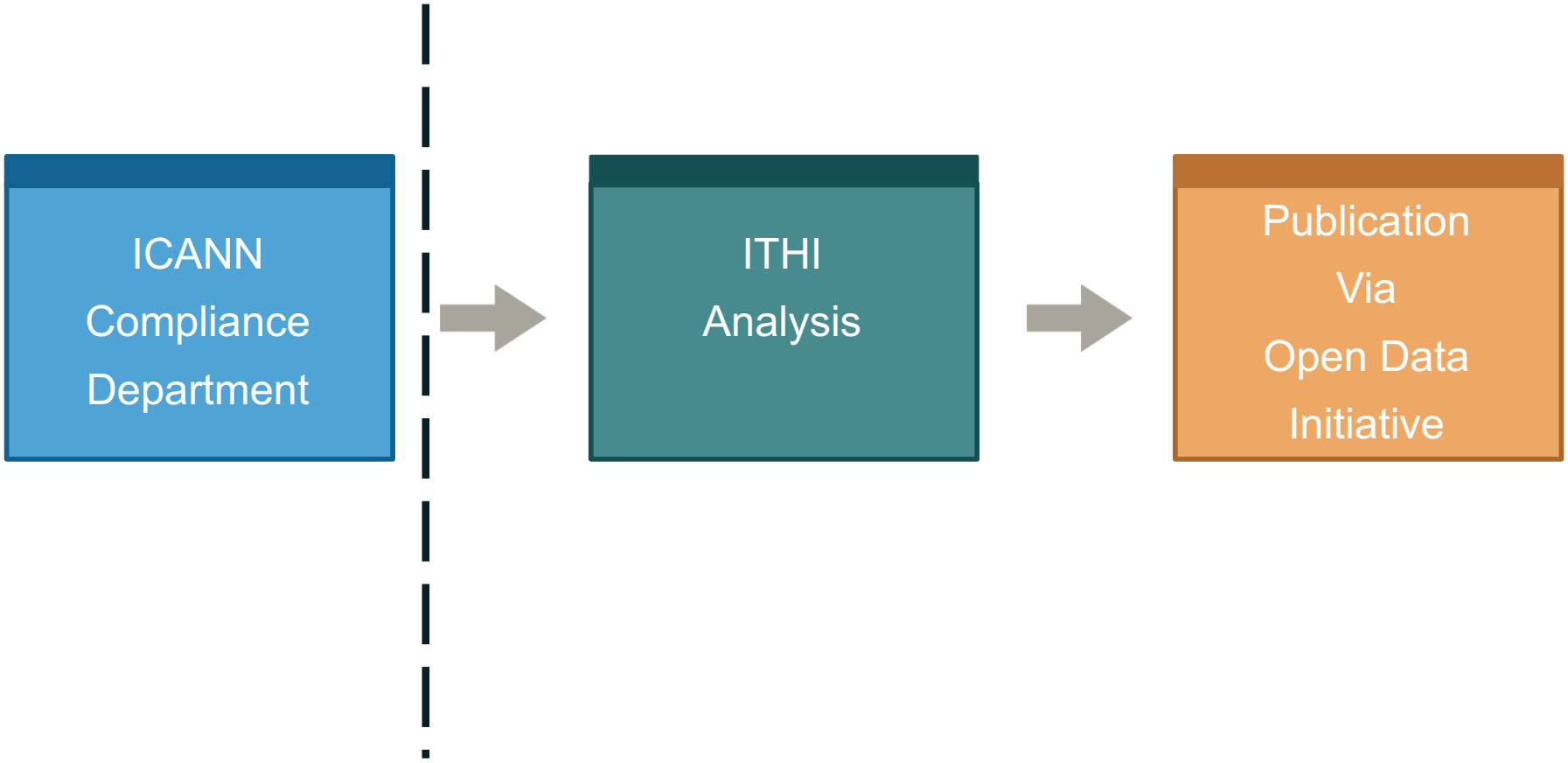
- For each “Problem Area”, we will put in place a 3-stage pipeline



ITHI Names

Data (In-)Accuracy

ITHI Names: Data (In-)Accuracy Process



ITHI Cooperation with ICANN Compliance Department

We asked ICANN compliance department for sample data on whois inaccuracy complaints it receives to build a **prototype of a candidate metric M1**.

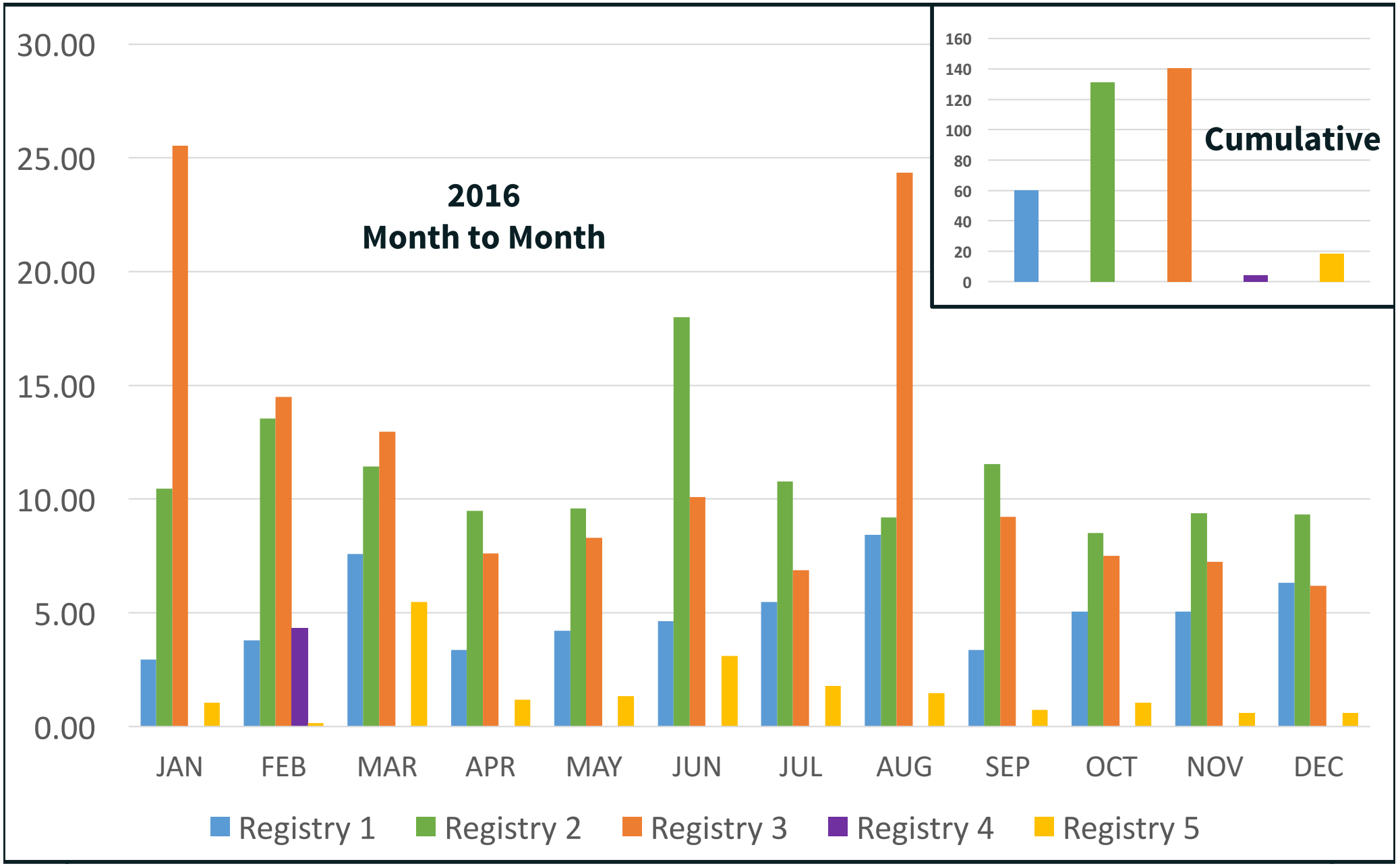
- We asked monthly data for 5 registrars and 5 registries covering 2016.
- The choice of registrars and registries was “random”, but covering both established and newer actors.
- Because this is only a limited sample and the methodology is still under development, we have anonymized the data to avoid singling out anybody.

Candidate Metric Related to Data (in-)Accuracy

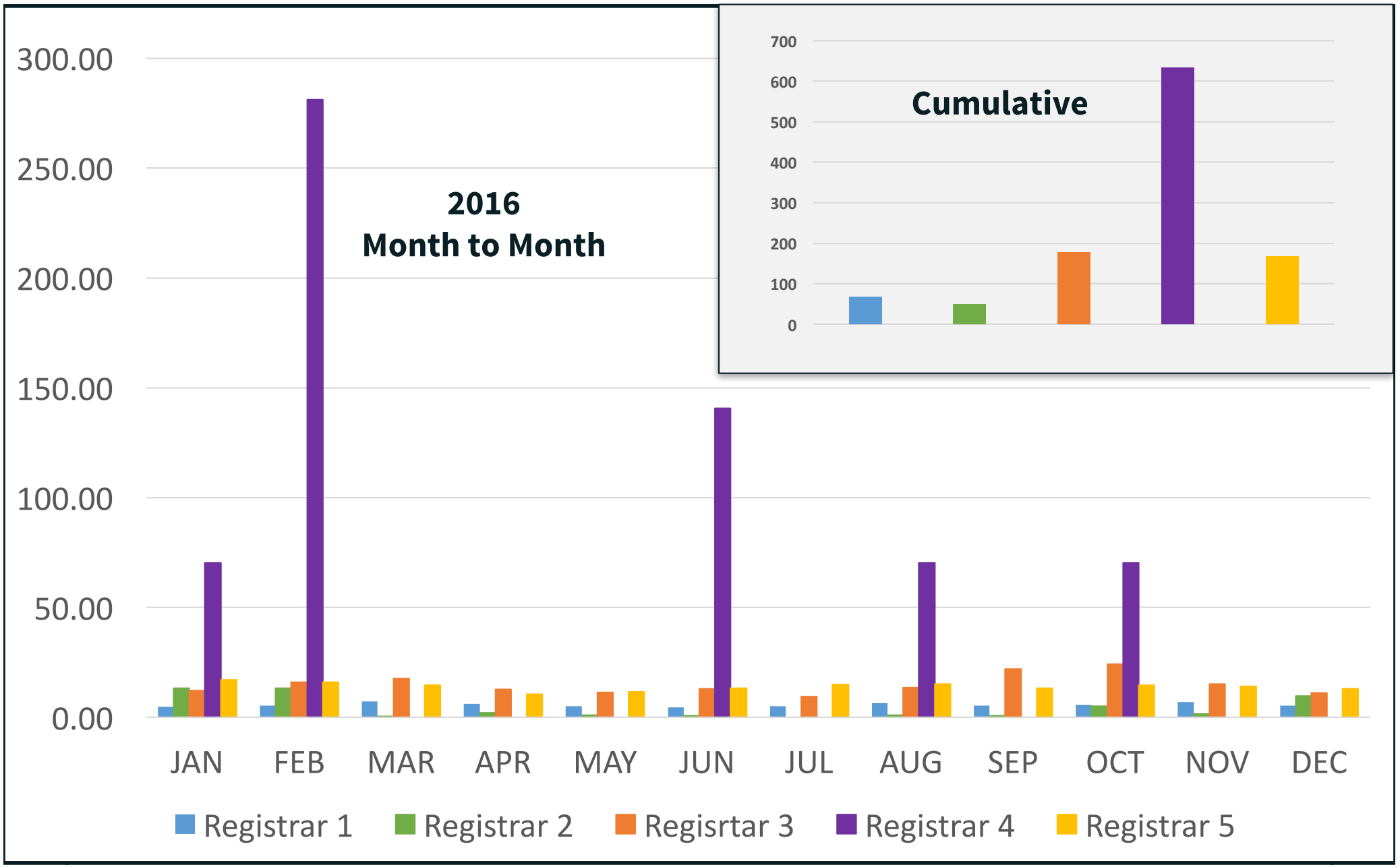
M1	Number of “validated complaints” per million registrations

A “validated complaint” is a complaint received by the ICANN compliance department that has been acted on. In other words, this is not an obviously frivolous complaint.

Registries: Complaints per Million Registrations



Registrars: Complaints per Million Registrations



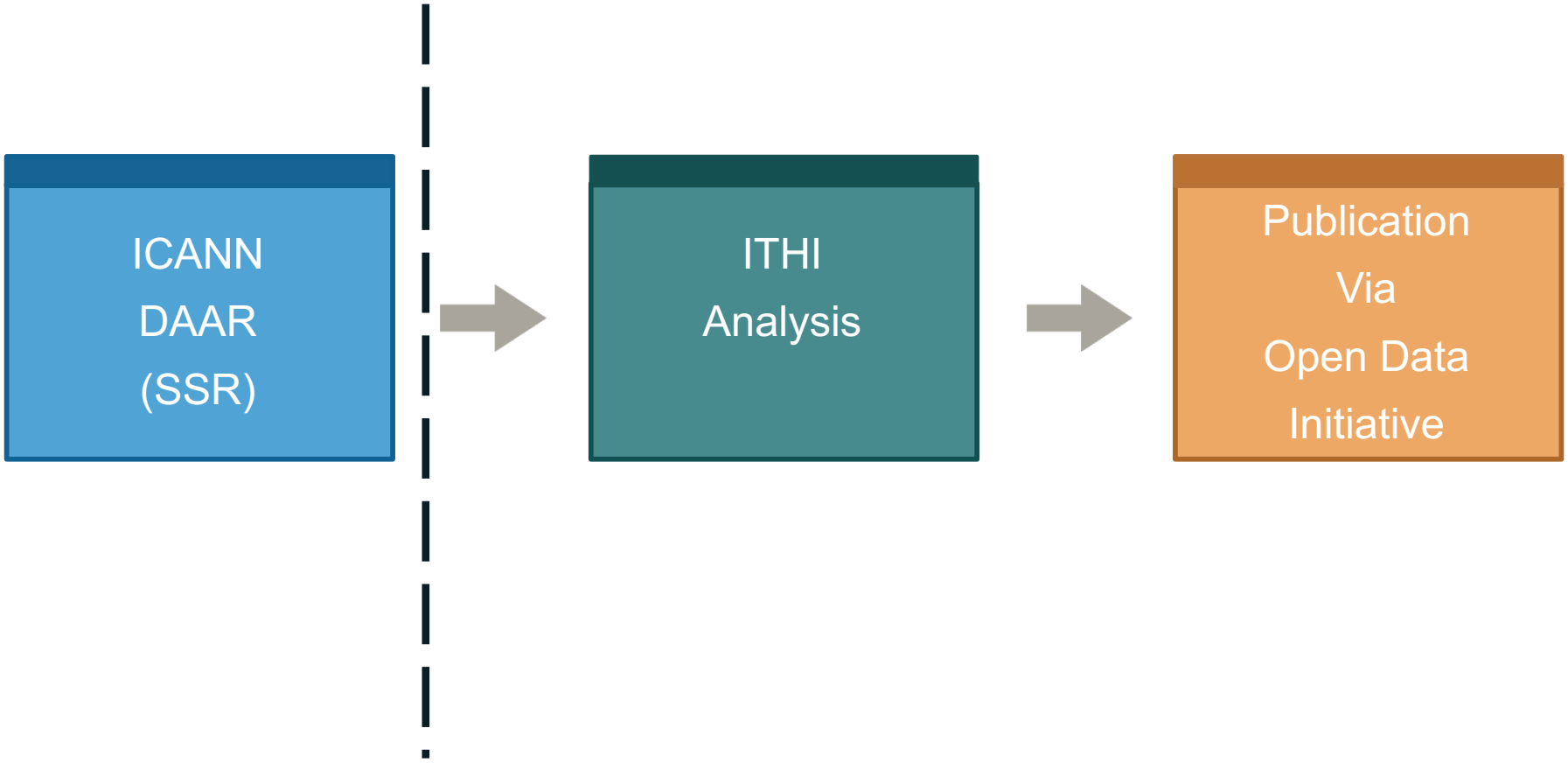
Observations

- The number of complaints received per registrar or registry is relatively small. Typically less than 1 per day or a couple per week on a monthly average.
- There are some exceptions, where we see peaks up to 10 per day on a monthly average.
- We tend to see more differences among the registrars than among the registries.
- This is only a sample of 5 Registries and 5 Registrars.
- Will extend to full set of registries and registrars

ITHI Names

Domain Name Abuse

ITHI Names: Domain Name Abuse Process



ITHI Cooperation with SSR

We worked in conjunction with the DNS Abuse Activity Reporting Tool (DAAR) to develop a set of domain name abuse candidate metrics M2.

DAAR is based on a number of industry accepted feeds.

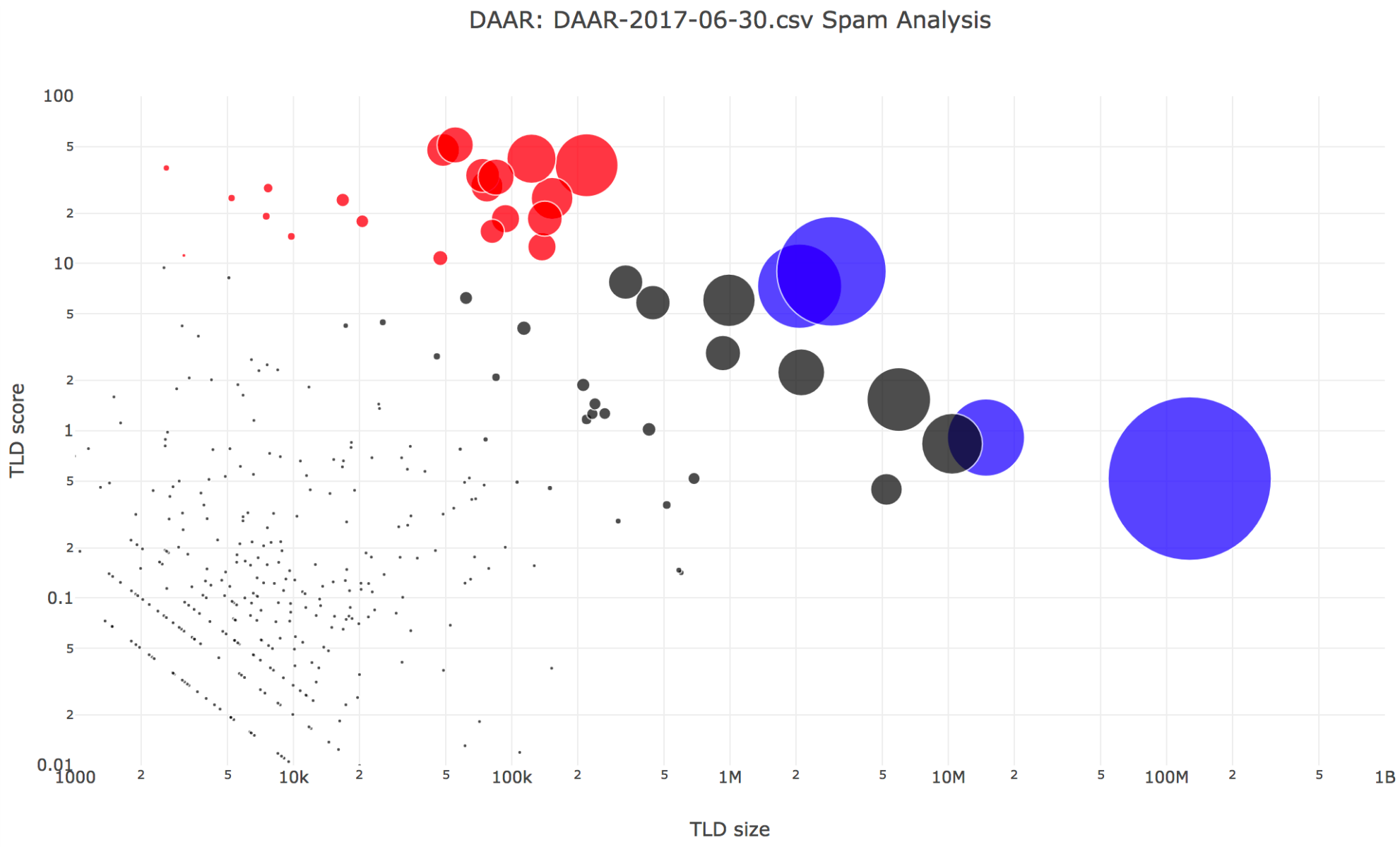
Data is available since November 2016. In this prototype, we use only one data point for the same registrars/registries as previous study.

Because this is only a limited sample and the methodology is still under development, we have anonymized the data to avoid singling out anybody.

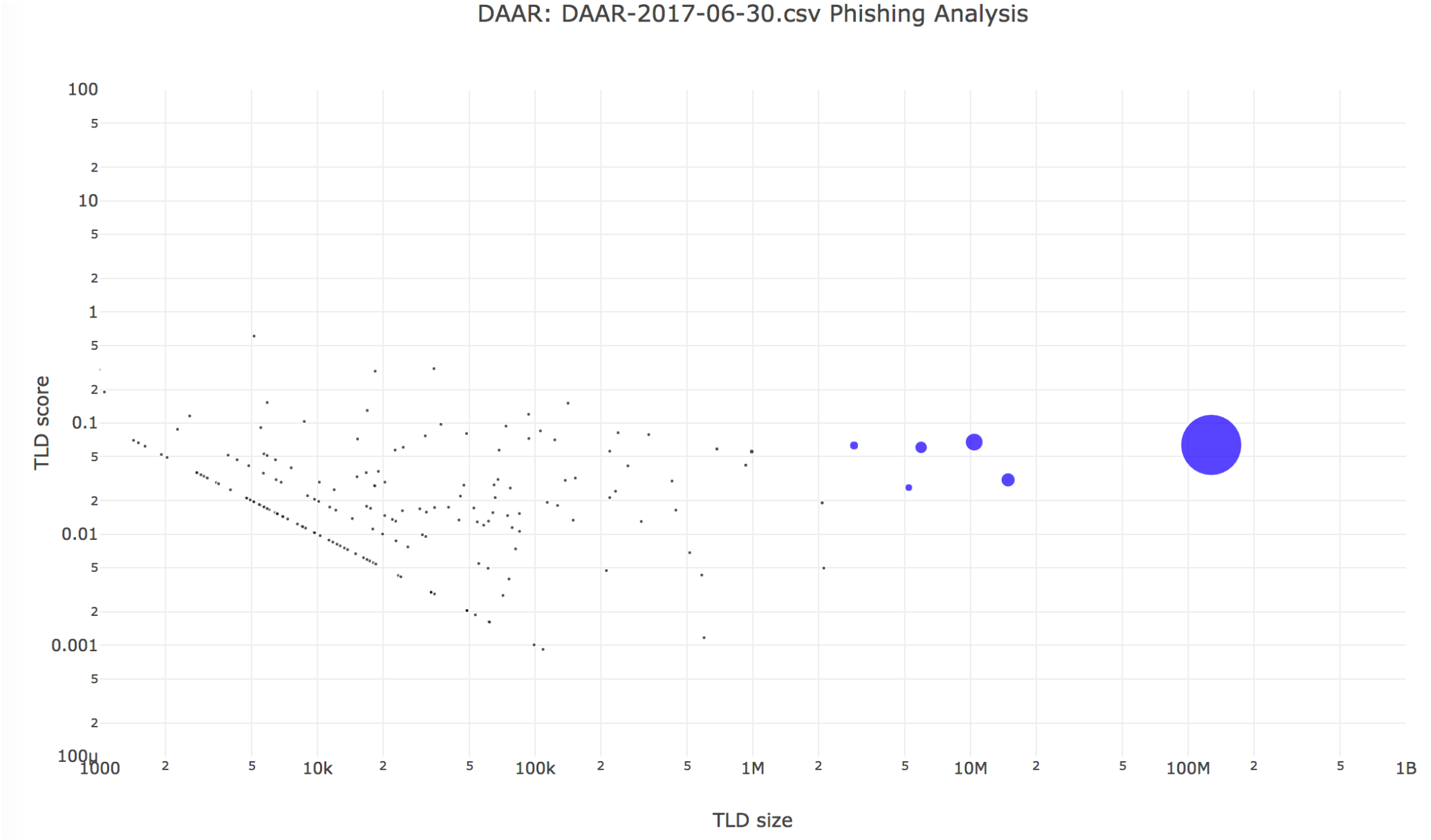
Candidate Metrics Related to Abuse

M2	Number of abuses in the feeds per 10,000 registrations
M2 encompass 4 sub-metrics	
M2.1	Spam
M2.2	Phishing
M2.3	Malware
M2.4	Botnet

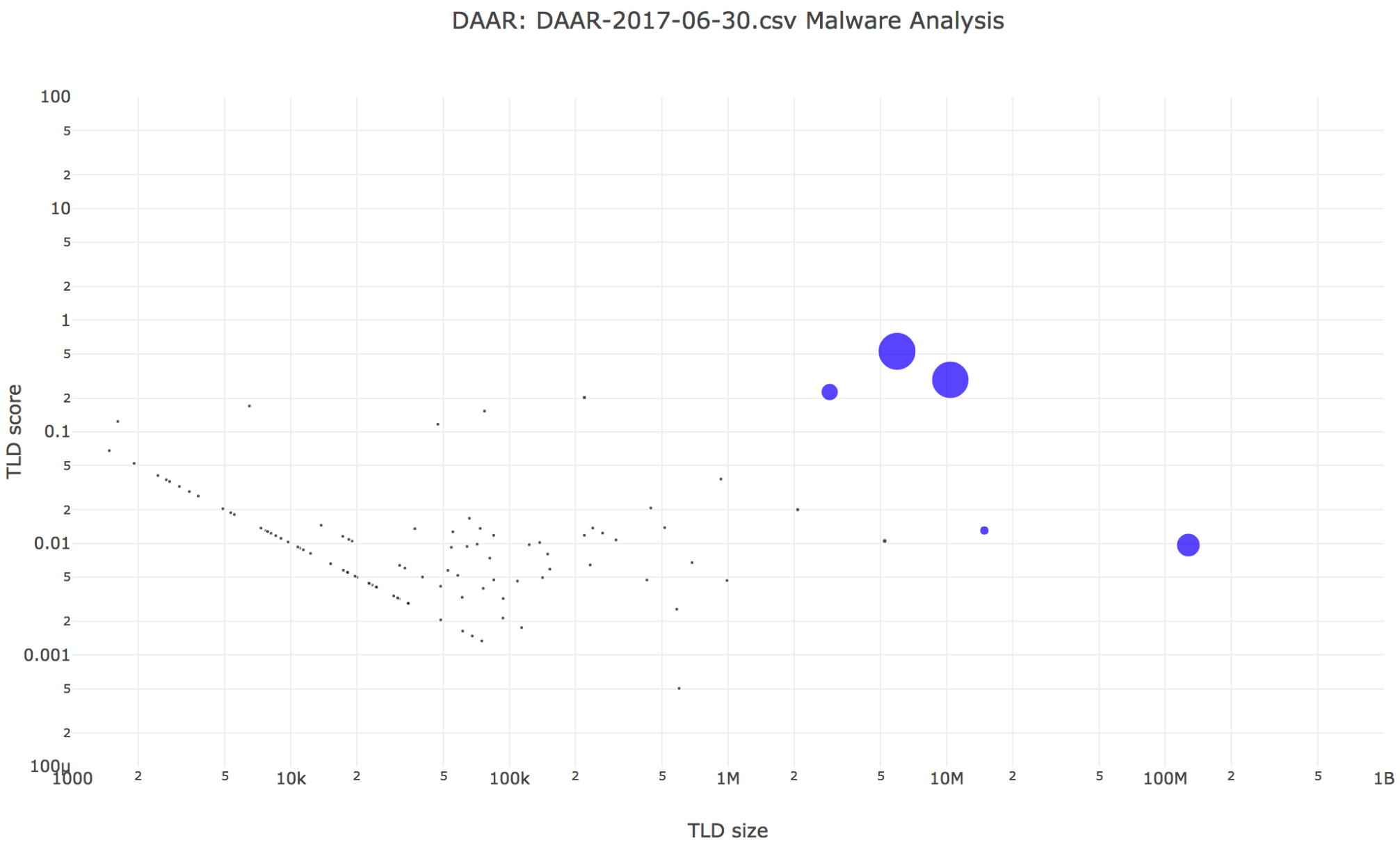
Example: M2.1 Spam (Work in Progress)



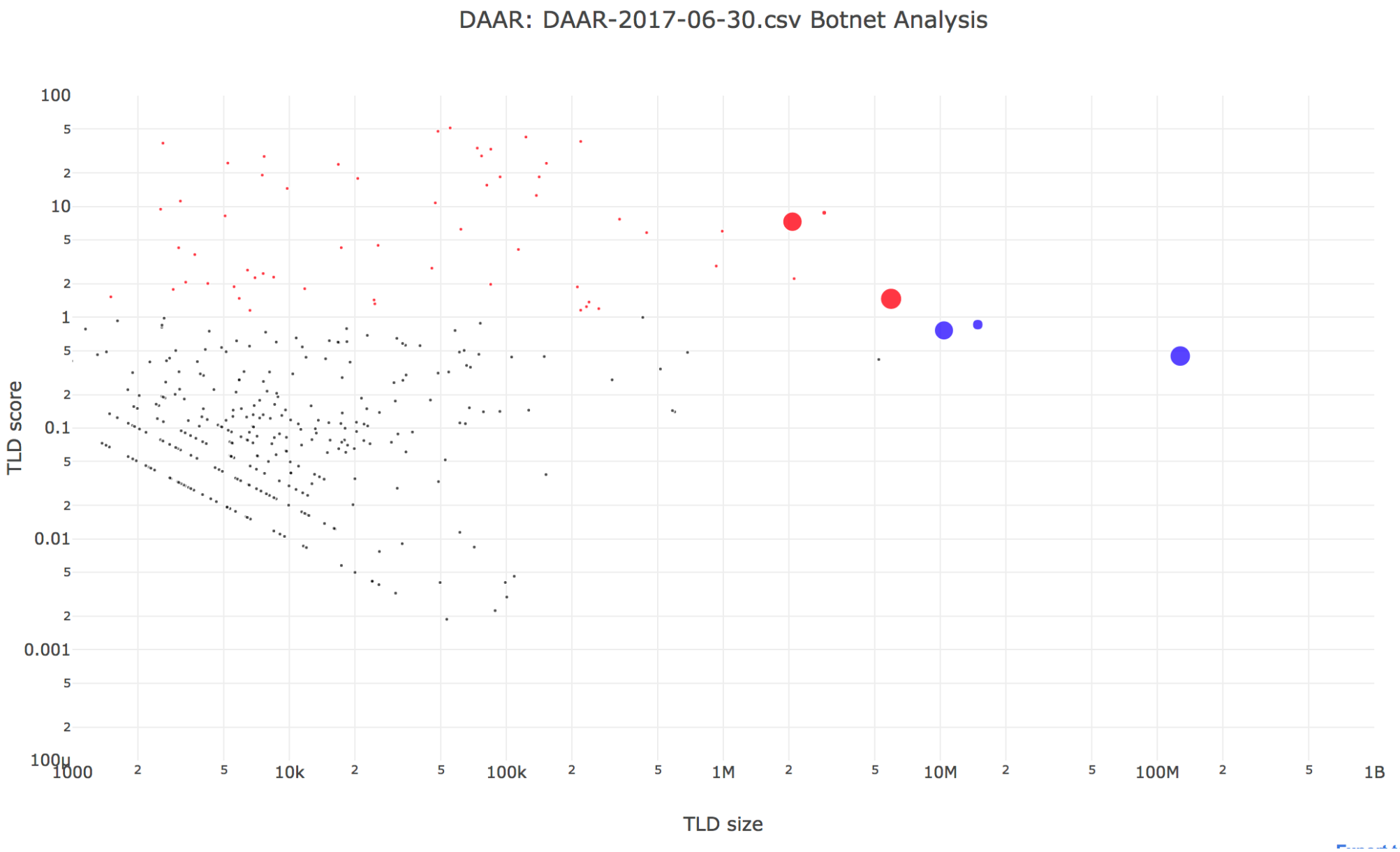
Example: M2.2 Phishing (Work in Progress)



Example: M2.2 Malware (Work in Progress)



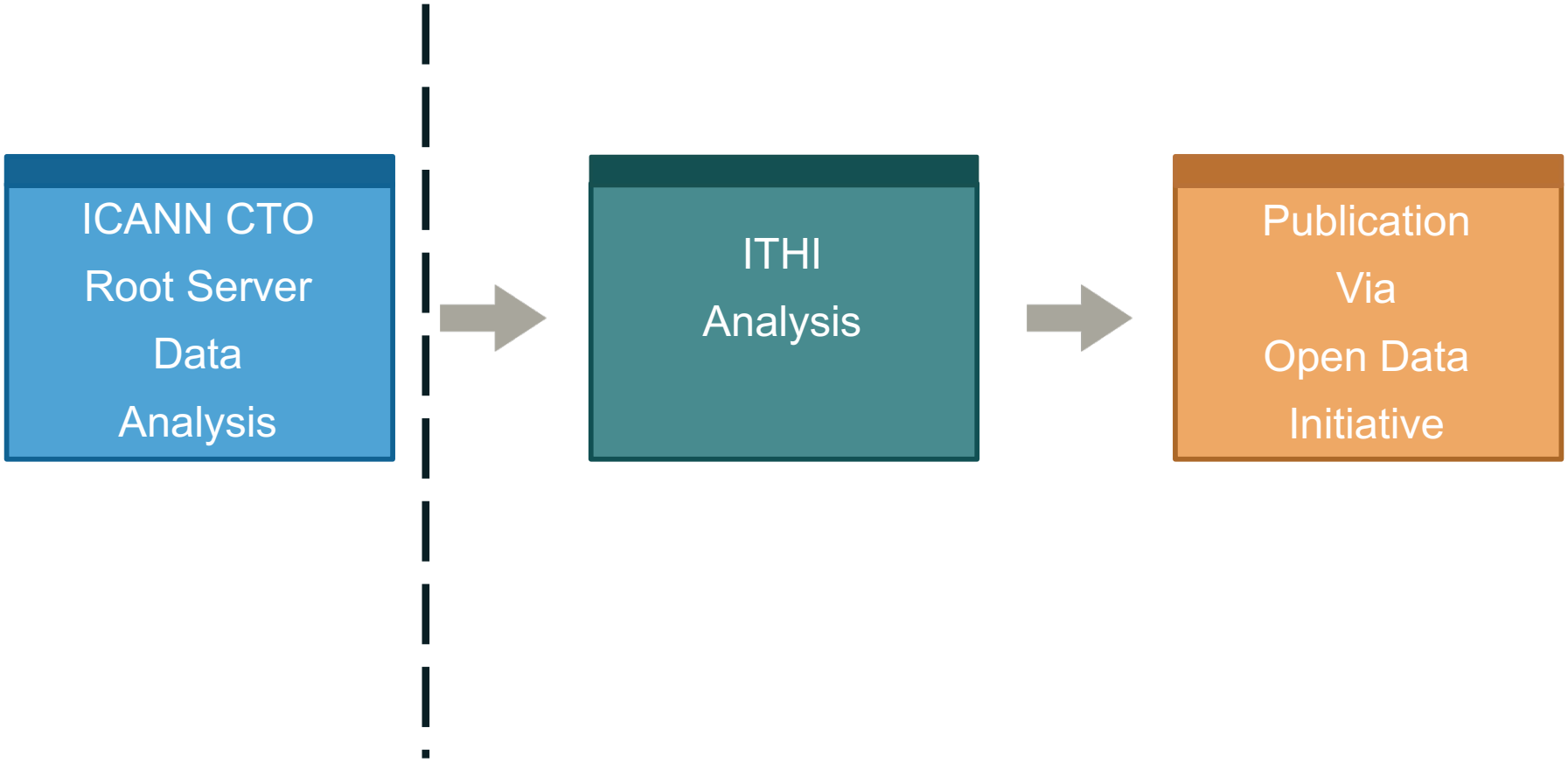
Example: M2.2 Botnet (Work in Progress)



ITHI Names

Overhead in Root Traffic

ITHI Names: Excessive Root Traffic



ITHI Cooperation with OCTO/Root Server Analysis

We worked in conjunction with the OCTO/Research project analyzing traffic at a collection of root servers.

Measure the overhead to the minimum traffic that would be required in a “best case” scenario where DNS resolvers were only asking for TLDs that exists and would respect the associated TTLs.

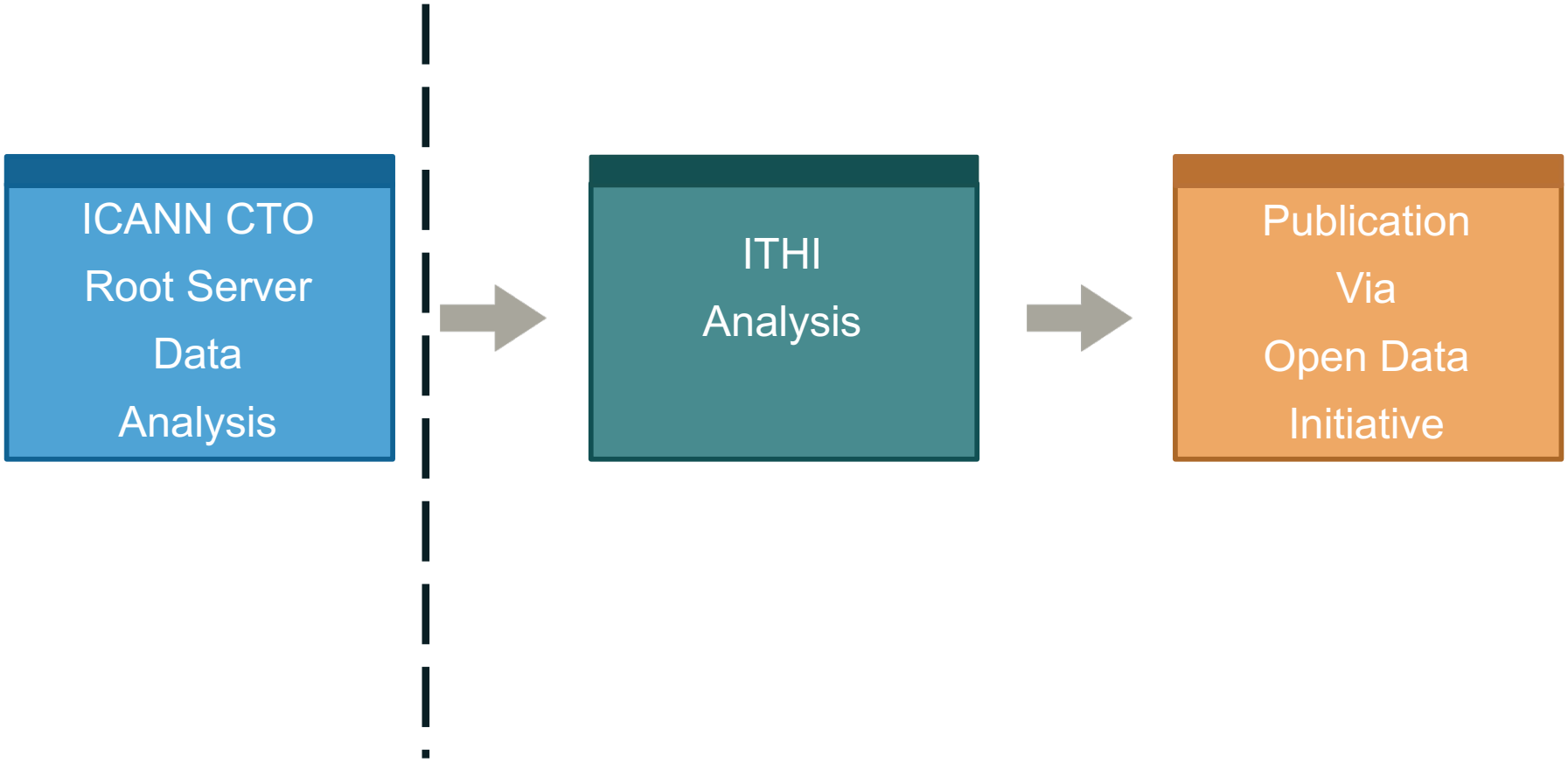
Candidate Metric Related to Overhead in Root Traffic

M3	The overhead to the minimum traffic that would be required in a “best case” scenario where all DNS resolvers were only asking for TLDs that exists and would respect the associated TTLs.
M3 encompass 2 sub-metrics	
M3.1 M3.2	% of NX domain % of queries that should never have been sent (TTL)

ITHI Names

Leakage

ITHI Names: Leakage



ITHI Cooperation with OCTO/Root Server Analysis

We worked in conjunction with the OCTO/Research project analyzing traffic at a collection of root servers.

Candidate Metric Related to Leakage

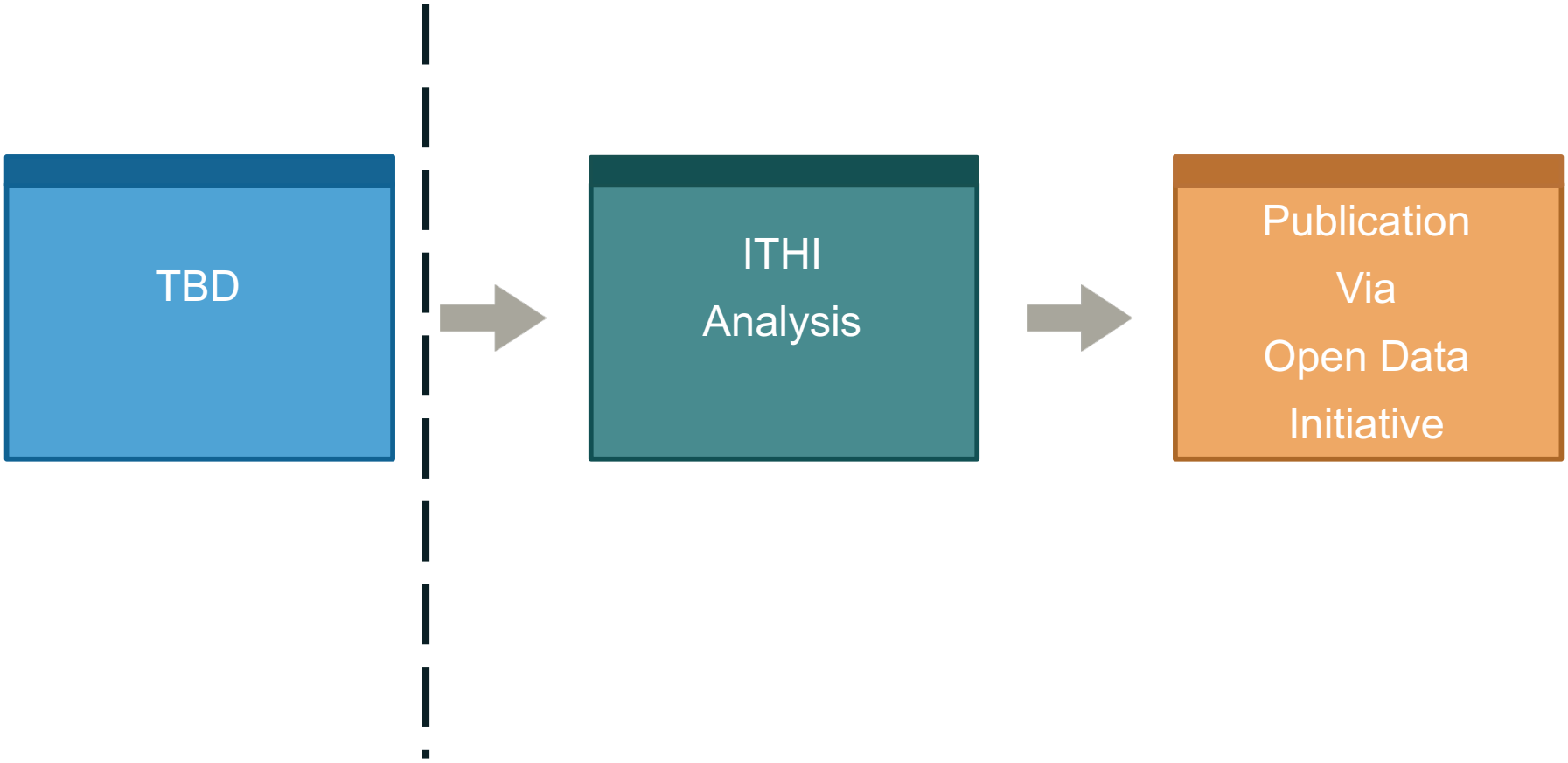
M4	Leakage

M4 encompass a list of
“Top-N” strings seen at the root
that have not been delegated by ICANN
or put on the RFC6761 ”Special Use Names”

ITHI Names

Lies

ITHI Names: Lies



ITHI Cooperation with TBD

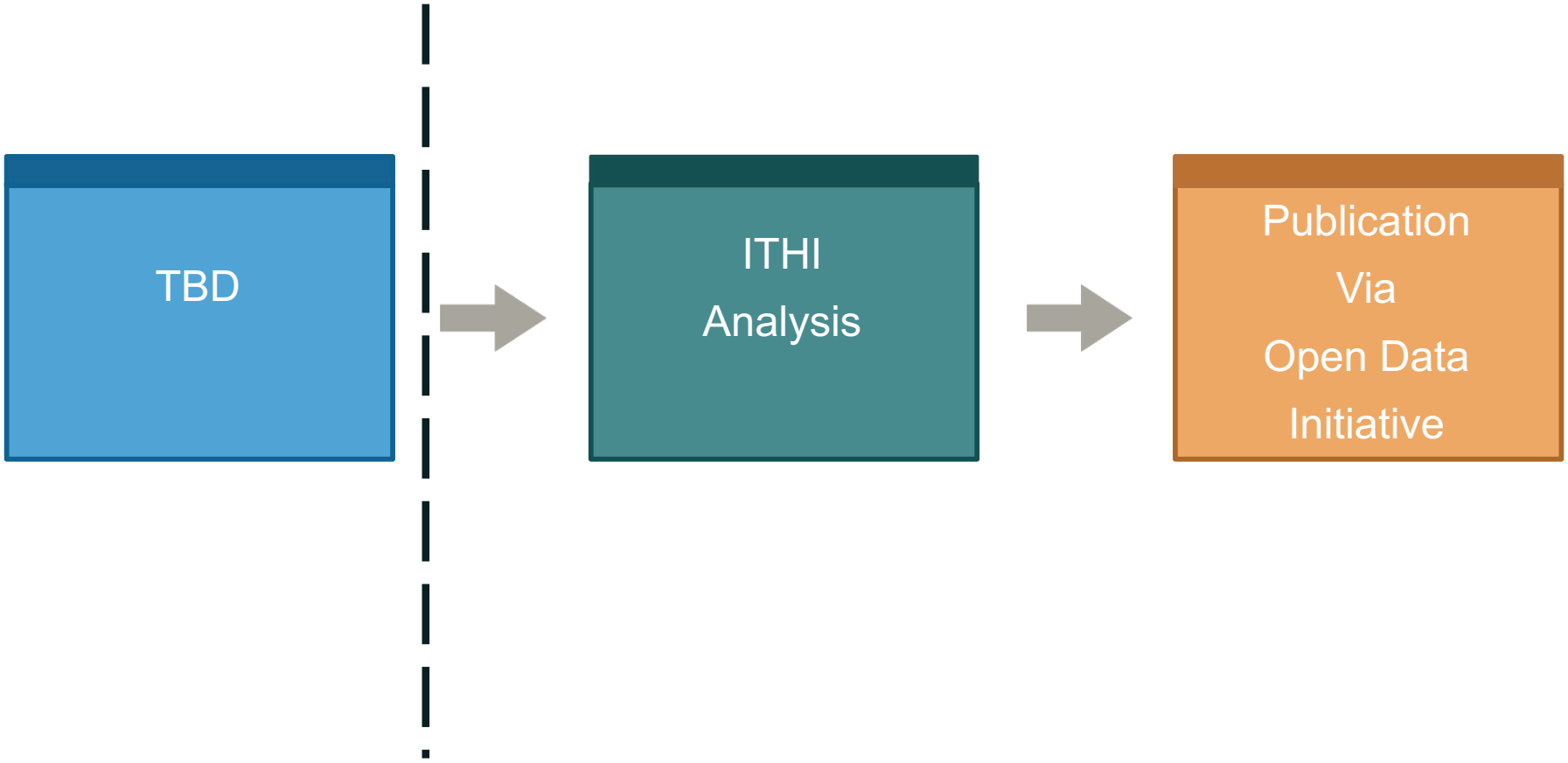
Candidate Metric Related to Excessive Root Traffic

M5	Lies
% of DNS resolvers lying to their clients (out of the top 10,000 resolvers)	

ITHI Protocol Parameters

Scoped to DNS Releted Registries

ITHI Protocol Parameters



ITHI Protocol Parameters

We will limit the study to the IANA Protocol Parameter Registries related to the DNS

The idea is to observe traffic both at Root Servers and Recursive Resolvers and look at:

- Frequency of each registered parameter
- Presence (and Frequency) of unregistered parameters

Candidate Metric Related to DNS Protocolk Parameter Usage

M6	DNS Protocol Parameter Usage

M6 encompass the list of parameters and their frequencies plus a list of unregistered parameters (and their frequencies)

ITHI Numbers

NRO-Driven Process

Number Community Participation

- The RIR community is driving their own evaluation of ITHI metrics.

- The RIR registry services have proposed a set of metrics focused on data accuracy. Those metrics need to be reviewed by the RIR community.

- It is expected that this branch of the project will be merged with the overall ITHI initiative at a later point in time.