

CDAR

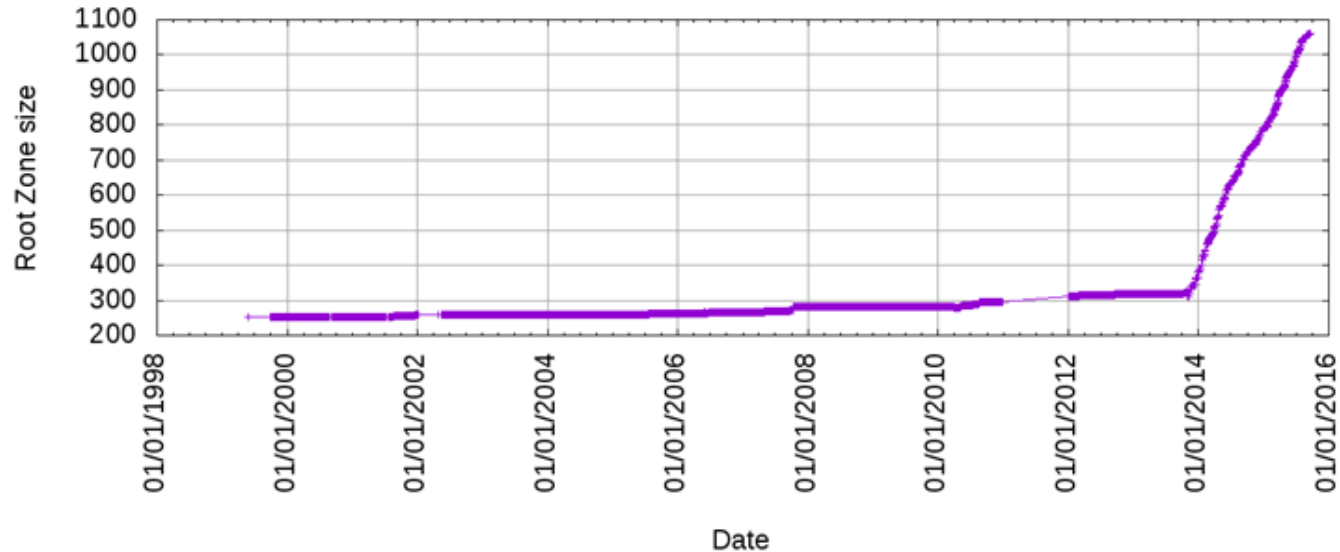
Continuous Data-driven Analysis of Root Stability

15 March 2017
ICANN58 – SSR review team

Bart Gijsen (TNO)

CDAR Study

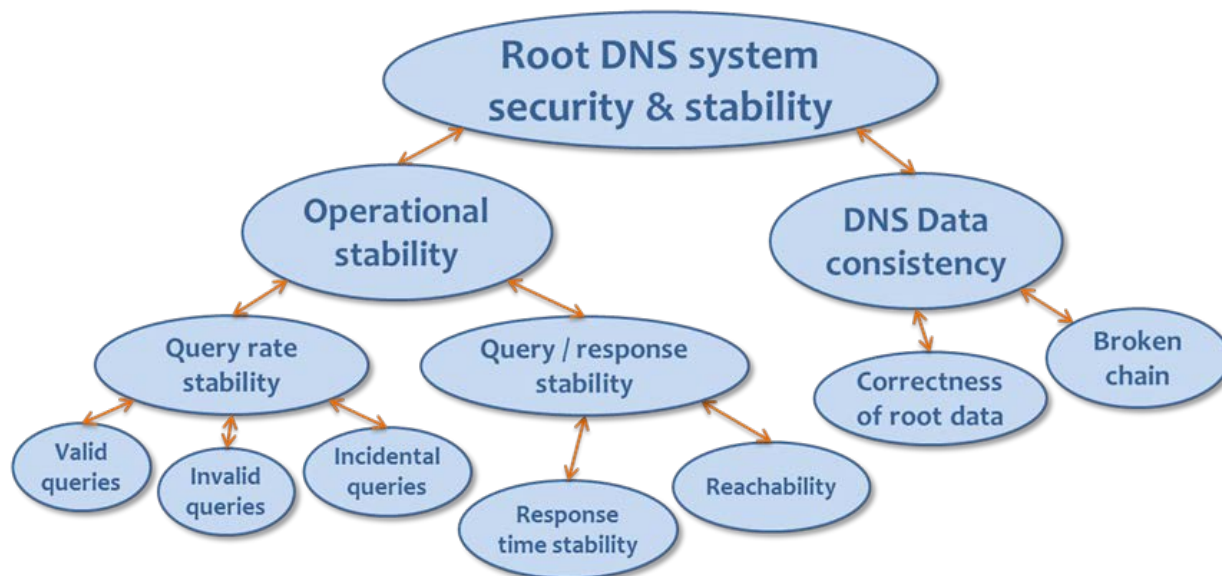
- Context:



- Question: *did delegation of new gTLDs degrade the stability or security of the root DNS system?*
 - Secondary: can we expect a degradation in the near future?

Analyses

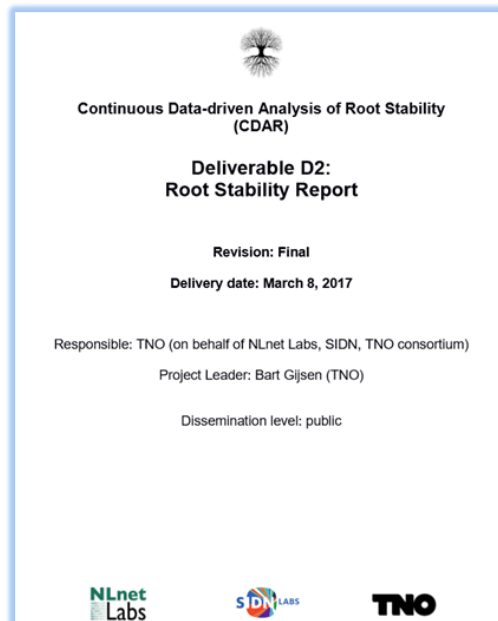
- Large amount of historical data sets analyzed:
 - RSSAC002 (since October 2013)
 - DITL (yearly 2-day data collections from 2012 thru 2016)
 - RIPE Atlas (selected intervals in period of new gTLD delegations)
 - Other: ZFR, Registry reports, 'Renumbering', DNSSEC validator
- Analyzed metrics:



Primary Conclusion

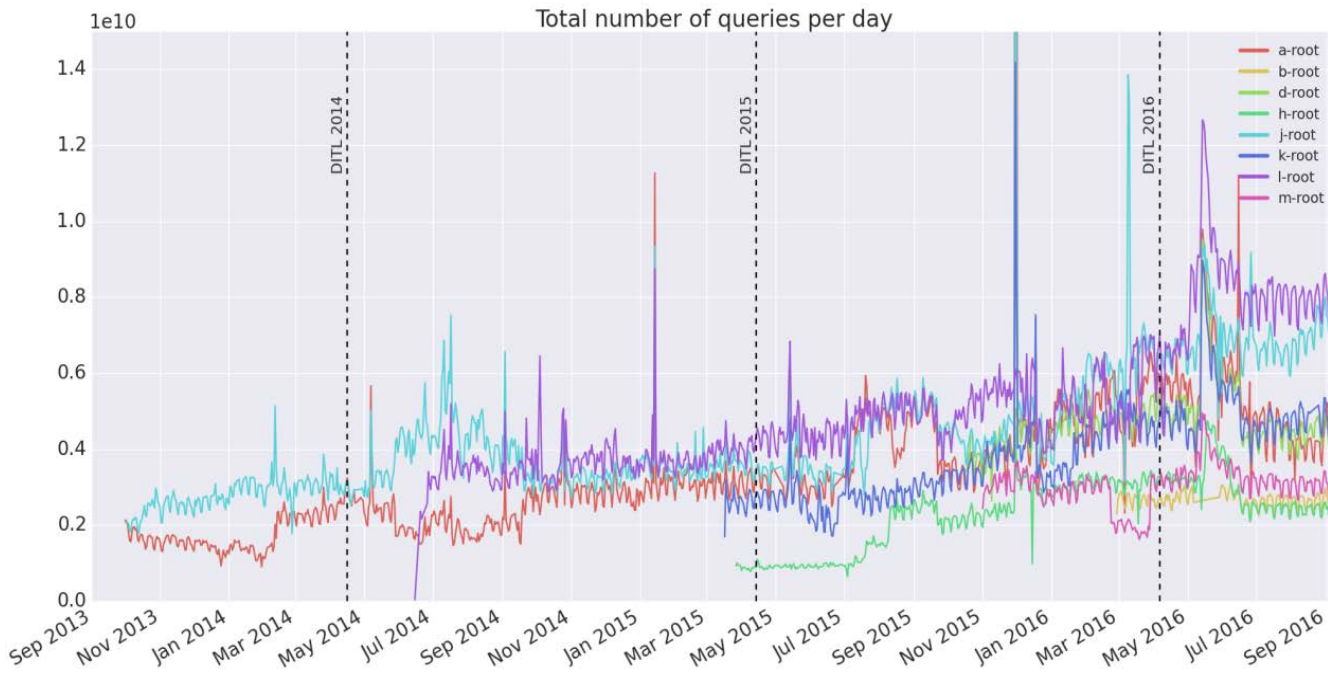
- Has the delegation of new gTLDs degraded the stability or security of the root DNS system?

Investigated data sets show no degradation of the stability or security of the root DNS system that can be attributed to delegation of new gTLDs



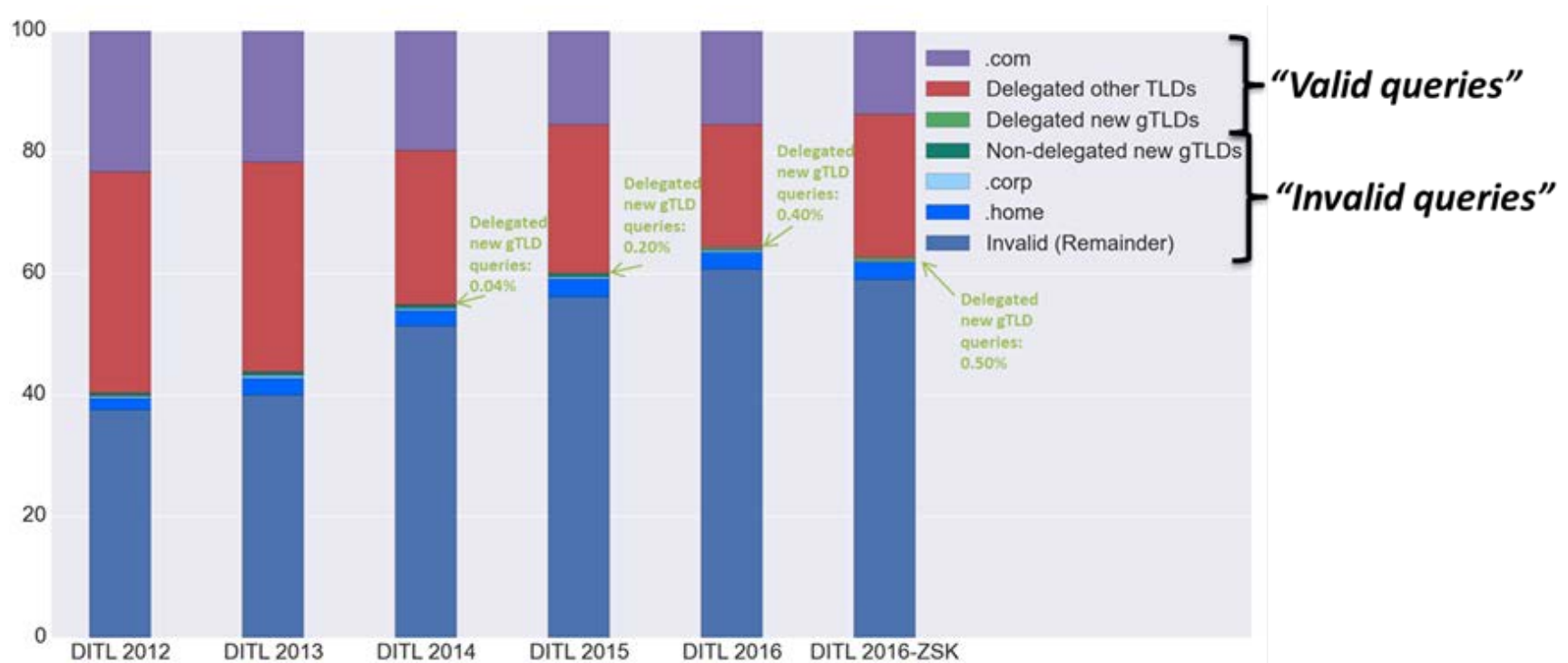
www.icann.org/en/system/files/files/cdar-root-stability-final-08mar17-en.pdf

Finding: Traffic is Increasing



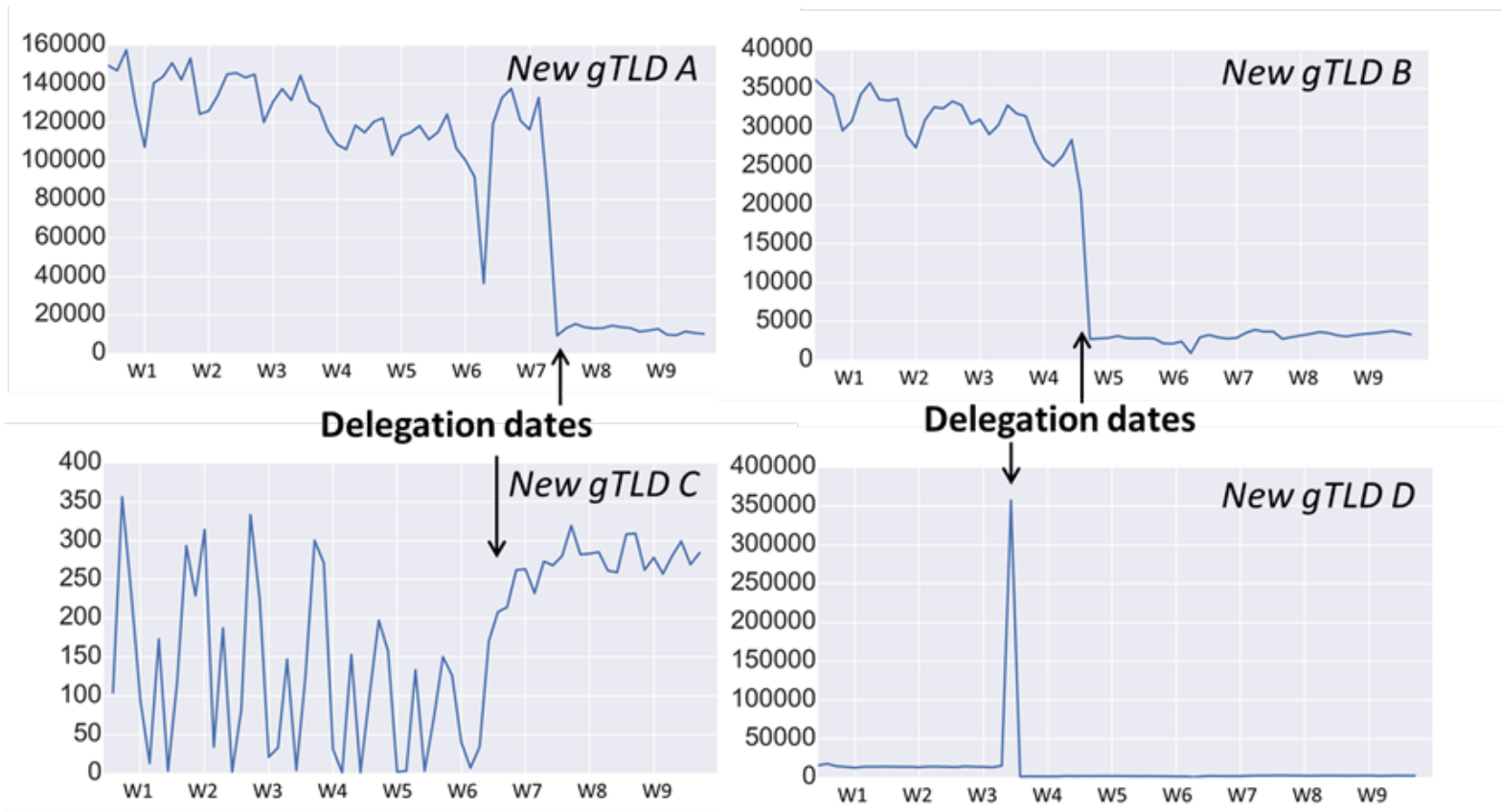
- Both query rate to the root DNS system as well as the size of the root DNS system is growing
 - Apparently, root DNS system has been able to grow along with the increase in root server traffic over the past years
- Total query volume consists of:
 - queries for valid and invalid TLDs +
 - incidental peaks of query volumes during rare events (e.g. November 30, 2015 and June 25, 2016)

Finding: Fraction of Valid / Invalid



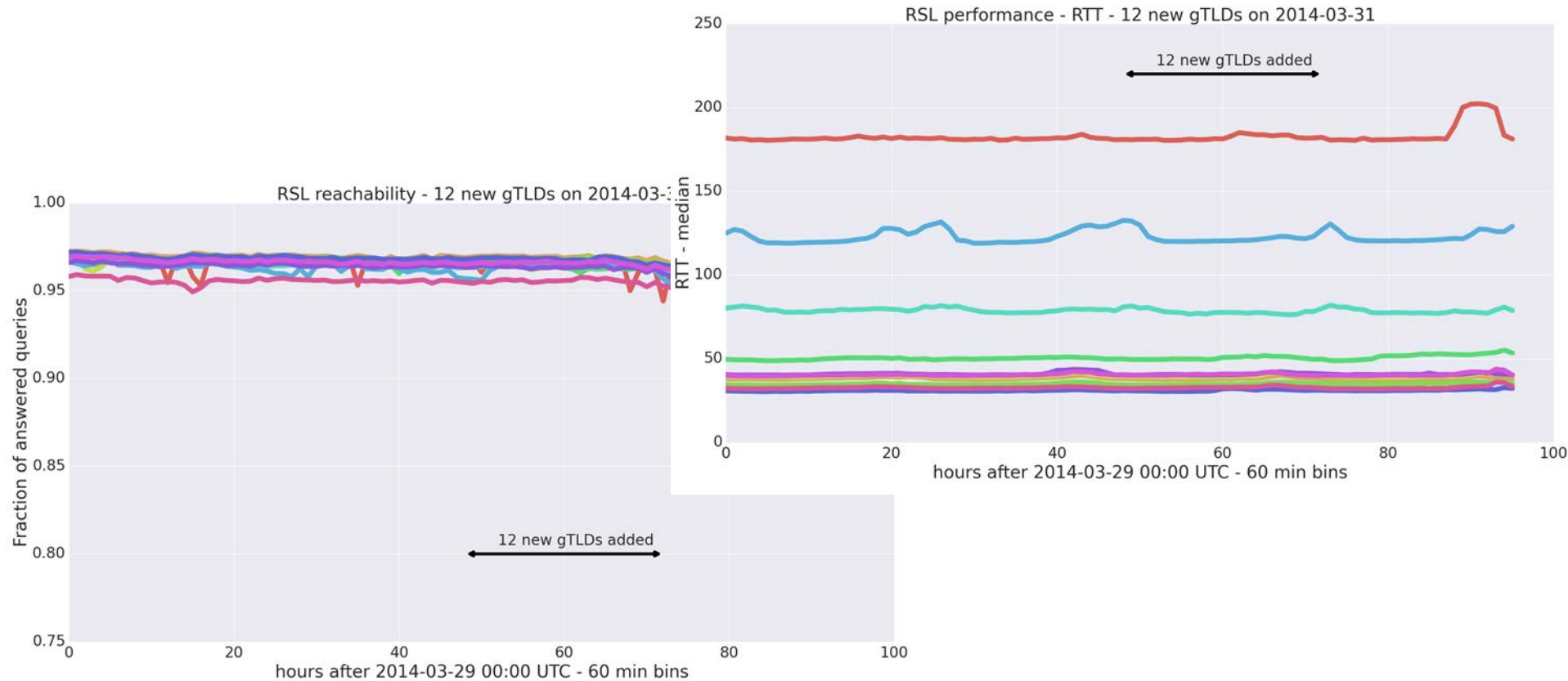
- Fraction of queries for invalid TLD names increases over time
 - No indication that the delegation of new gTLDs has contributed to this trend
- New gTLD queries do contribute to the valid query volume although this contribution is very small
 - During DITL 2016: only 1.1% of the total valid query volume (only 0.4% of the total valid+invalid query volume)
 - Slightly increasing fraction, but insignificant so far

Finding: Microscopic Effects



- Fluctuations in query rates visible around initial new gTLD delegation
 - But at low volume and converges to new steady state fast

Finding: No Visible Impact From the Outside



- RIPE Atlas measurements: fluctuations have no visible impact on RTT performance or reachability of root DNS system

Finding: DNS Data Consistency

- Scan for data errors that might be introduced:

(Different) errors as a result of changes in the root zone file due to delegations of new gTLDs?

– *No errors slip through the zone file verification steps*

DNSSEC validation errors due to non-matching cryptographic data?

– *No significant errors observed for delegated new gTLDs*

Conclusion of CDAR Data Analysis

- We did not observe a degradation of the stability or security of the root DNS system due to new gTLDs
- We recognize that this conclusion is ...
 - Confined by the imperfections of the available measurement data and
 - Limited to the results of the analyses that we designed and executed
 - Interactions with technical DNS community revealed no additional, possible negative effects

Future Impact?

- What impact can we expect in the near future?
 - Presuming that:
 - Evolution of new gTLD delegations continues current pattern and
 - Observed time-invariant correlations remain invariant
 - Then, we see no signs that more new gTLD delegations will degrade the stability or security of the root DNS system in the near future
- Risk factors (disruptive new gTLD developments)
 - Non-exhaustive list ...
 - Possible impact of future new gTLD delegations:
 - Fast popularity increase of new gTLDs (.com-like)
 - Unbounded growth of the number of new gTLDs
 - Leaking queries, due to removal new gTLDs from root zone
 - Possible impact that is not new gTLD related
 - Increase in the amount of processing on root name servers due to other (use of) DNS protocols
 - Unusual large query volume events (DDoS)

Recommendations

- Remain enforcement of current measures to preserve current evolution pattern, in particular:
 - Controlled rate of delegating new gTLDs
 - Monitor impact of new gTLD delegations ⇔ more frequently
- Monitor risk factors
 - Detect disruptive growth of heavy queried new gTLDs
 - (Detect changes in use of DNS protocols that may increase traffic / processing)

Acknowledgement

- Providers of relevant data sets
 - DNS-OARC, RIPE NCC, amongst others
- Community interactions

Questions and Discussion

Acknowledgements

DNS-OARC, RSSAC002 data providers, RIPE NCC, ICANN

CDAR Project Team

Bart Gijsen (TNO)

Benno Overeinder (NLnet Labs)

Cristian Hesselman (SIDN)

Daniël Worm (TNO)

Giovane Moura (SIDN)

Jaap Akkerhuis (NLnet Labs)

Coordinator

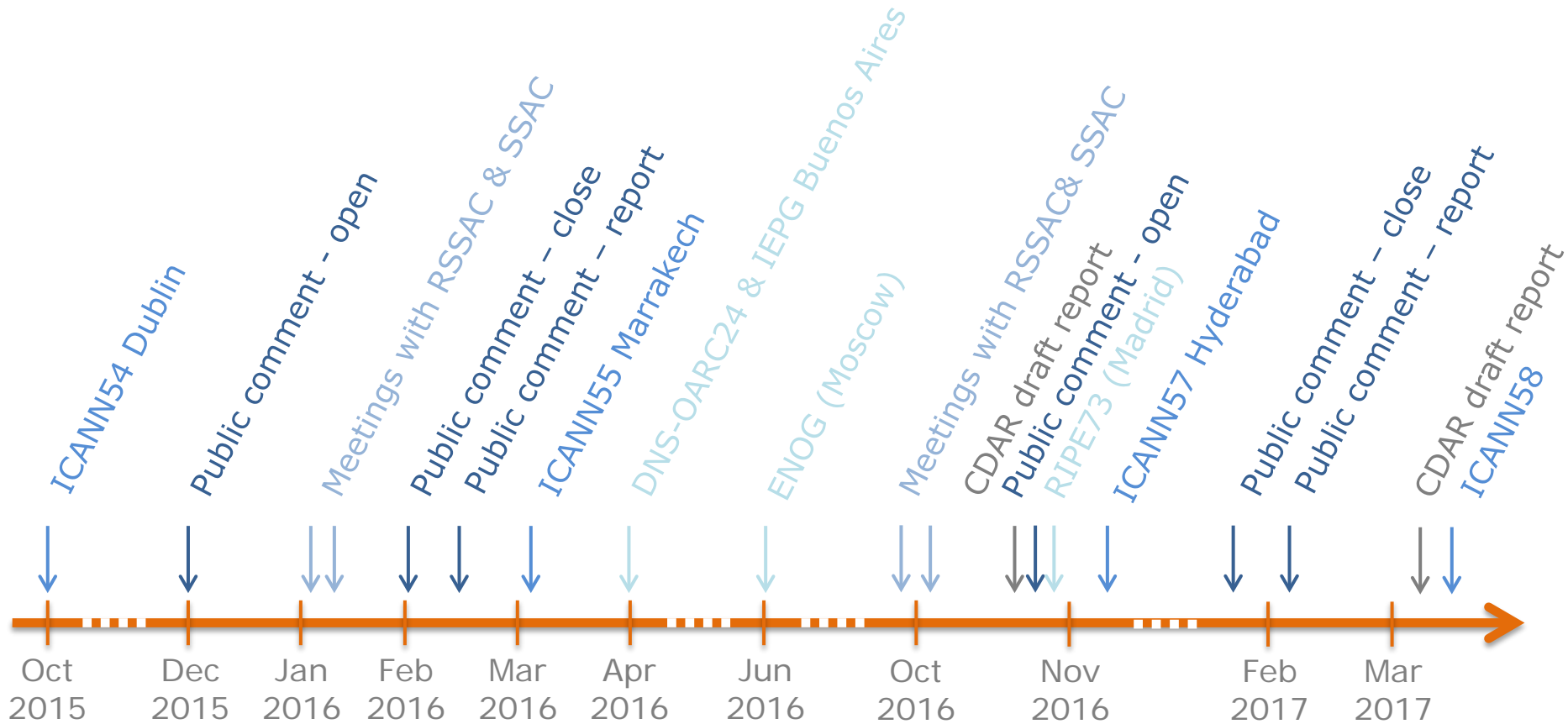
Bart Gijsen (Msc.)

+31 6 53 72 52 18

bart.gijsen@tno.nl

CDAR Home: <http://www.cdar.nl>

Community Interaction



Public Comments

- Feedback from 7 commenters

Main comments	CDAR / ICANN response
RSSAC: questions for clarifications, interpretation of findings and suggestions for refining recommendations related to monitoring the root DNS' security and stability.	CDAR: Reformulations made throughout the final report: "continuous monitoring" ⇔ "more frequent monitoring" Individual questions are responded in ICANN public comment staff report.
"Gradual rate of new gTLD delegation": what should be the threshold?	CDAR: "Controlled" delegation should be based on monitoring identified parameters; not on a threshold.
Report includes fact-based (data-driven) and "speculative" results: distinguish them.	CDAR: reformulations made throughout the final report.
Follow-up with CDAR recommendations: <ul style="list-style-type: none"> • Continue monitoring • Publicly available root DNS data 	ICANN: <ul style="list-style-type: none"> • CTO intends to perform & publish regular analysis of root-server traffic • Launches an Open Data Initiative
New areas of research	ICANN: possible subjects for future research are being considered.