ccNSO DNS Abuse Standing Committee

ICANN78 DASC update to GAC, 25 October 2023

ICANN | ccNSO

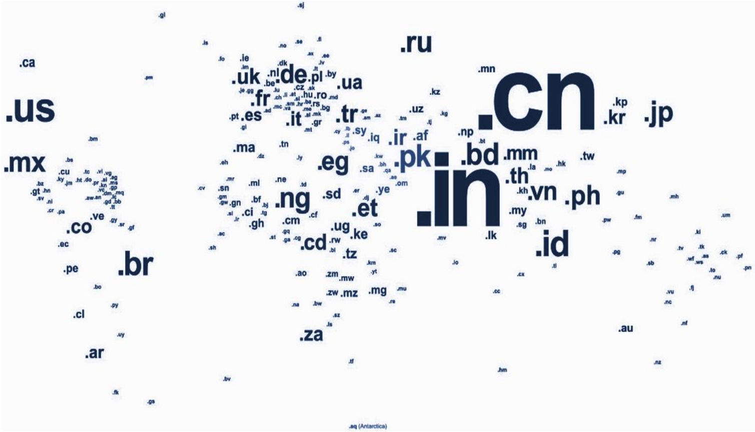
Country Code Names Supporting Organization

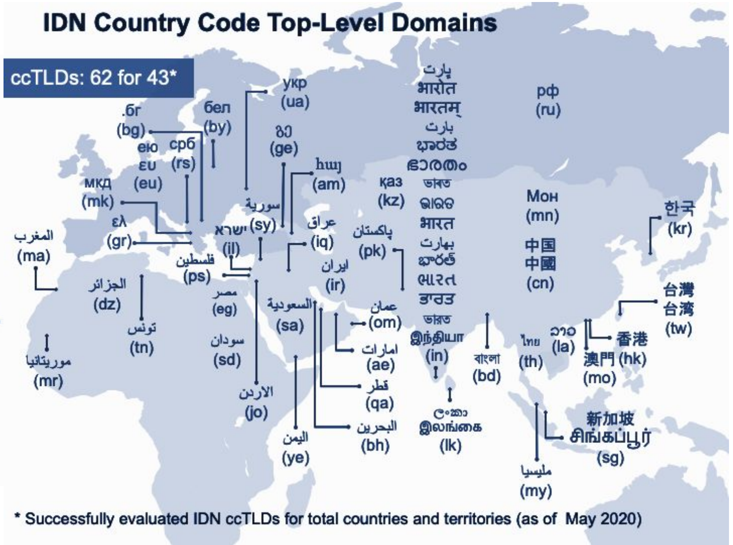
Agenda

- About DASC
- Useful tools for ccTLDs, provided by DASC:
    - Repository
    - Dedicated e-mail list
- DASC 2022 survey
- Join the DASC session on tools and measurements at ICANN78
- What happens post ICANN78?

What does ccNSO stand for?

- **ccNSO**: Country Code Names Supporting Organization (within ICANN)
  - Created for and by ccTLD managers
- **ccTLD manager:** organization or entity responsible for managing a ccTLD
- **ccTLD:** country code top-level domain





IDN Country Code Top-Level Domains

ccTLDs: 62 for 43*

* Successfully evaluated IDN ccTLDs for total countries and territories (as of May 2020)

POPULAR STANDARDS

ISO 3166 COUNTRY CODES

About the ccNSO DNS Abuse Standing Committee (DASC)

1. Share information, insights and practices

2. Raise understanding and awareness

3. Promote open and constructive dialogue

4. Assist ccTLD managers in their efforts to mitigate the impact of DNS Abuse

DASC does not formulate any policy or standards: out of scope of the ccNSO policy remit

About the DASC repository

A vetted list of resources, news articles, and other information related to DNS abuse, that could help ccTLDs address DNS abuse that they might encounter.

David McAuley, DASC Repository sub group Chair: "*We encourage members of the community: If you see something that might be helpful to ccTLDs, please let us know!*".

- Consult the Repository: https://community.icann.org/x/Ege7Cg
- Contribute to the Repository here: https://community.icann.org/x/DoWZDg

https://youtu.be/-5h6VsCXzyY

Heads up: DASC launches a dedicated e-mail list

Useful tool to ccTLDs, to better understand and mitigate DNS Abuse:

- Modelled after TLD Ops and other ccNSO lists
- The list will be closed, but not confidential
- Monthly contact list summary

Learn more:

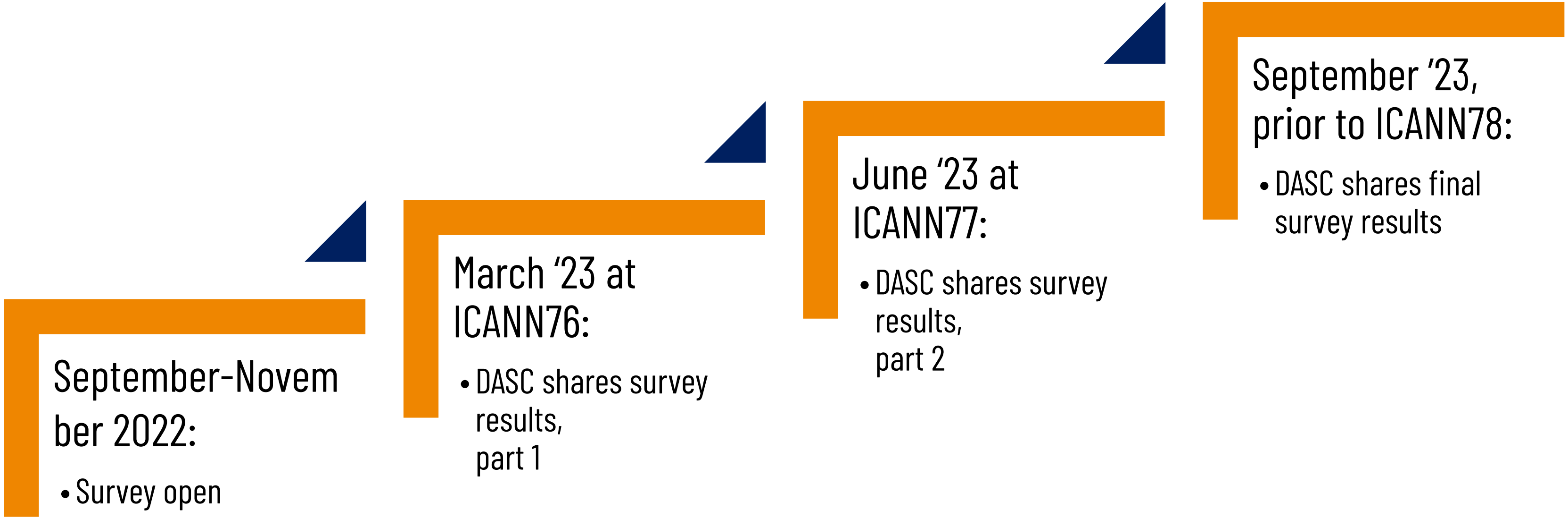
- DASC session on tools and measurements at ICANN78
- ccNSO mailing lists and newsletters

About the DASC survey

Results (session recordings): https://ccnso.icann.org/en/workinggroups/dasc.htm

- Open: September '22 - end November '22
- All ccTLDs were invited to respond, regardless of ccNSO membership
- 57 unique responses. Estimate: representing approx. 100 ccTLDs
  - 316 delegated ccTLDs in total (ASCII & 61 IDN alike)
  - Some ccTLD managers provide services for multiple ccTLDs, but responded for 1 TLD only
  - Some ccTLD managers informed DASC they could not respond, for various reasons
  - Some ccTLDs responded multiple times: latest submission as final one
  - Some responses were incomplete
- About half of the respondents did not want their ccTLD mentioned

Timeline



September-November 2022:

- Survey open

March '23 at ICANN76:

- DASC shares survey results, part 1

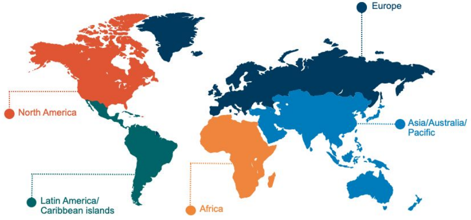
June '23 at ICANN77:

- DASC shares survey results, part 2

September '23, prior to ICANN78:

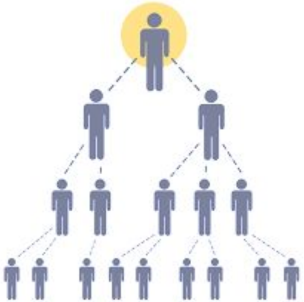
- DASC shares final survey results

What makes ccTLDs different?



Region

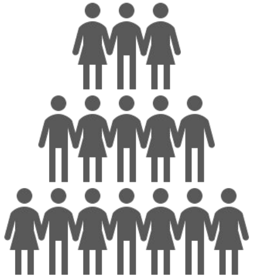
Governance model



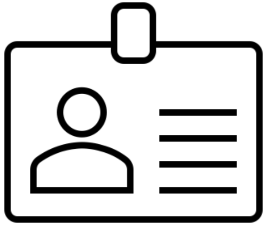
Registry model

% domains exposed to DNS Abuse

Number of domains



Number of employees



ccTLD has Abuse Officer

ccTLD is affected by DPL

What was shared previously?

ICANN76

- Where and when do respondents take action?
- What are the DNS Abuse mitigation trends?
  - Mitigation methods, outreach & education to registrars
  - Trusted notifier arrangements, type of action when abuse is detected, reporting mechanisms for the public
- Tools & feeds
- Combined results: mitigation methods vs region, registry model, size

ICANN77

- Pre-registration
  - Which information is being collected?
  - Do respondents perform pre-registration verifications?
  - Do respondents perform checks at time of registration, and if so, for which data?
- Post-registration
  - Methods: manual vs automated
  - When do post-registration verifications happen?
- Mid-cycle
  - Type of action when abuse is detected, based on: Feed, LEA request, due diligence verifications
  - Measures to keep registration data accurate over time
- Renewal
  - Do respondents perform verifications?

What was shared previously?

ICANN76

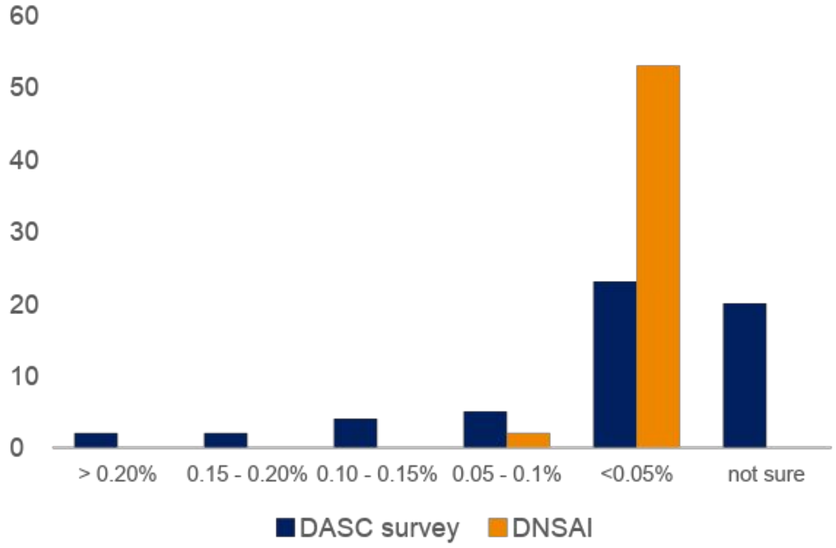
- Where and when do respondents take action?
- What are the DNS Abuse mitigation trends?
  - Mitigation methods, outreach & education to registrars
  - Trusted notifier arrangements, type of action when abuse is detected, reporting mechanisms for the public
- Tools & feeds
- Combined results: mitigation methods vs region, registry model, size

ICANN77

- Pre-registration
  - Which information is being collected?
  - Do respondents perform pre-registration verifications?
  - Do respondents perform checks at time of registration, and if so, for which data?
- Post-registration
  - Methods: manual vs automated
  - When do post-registration verifications happen?
- Mid-cycle
  - Type of action when abuse is detected, based on: Feed, LEA request, due diligence verifications
  - Measures to keep registration data accurate over time
- Renewal
  - Do respondents perform verifications?

What stood out?

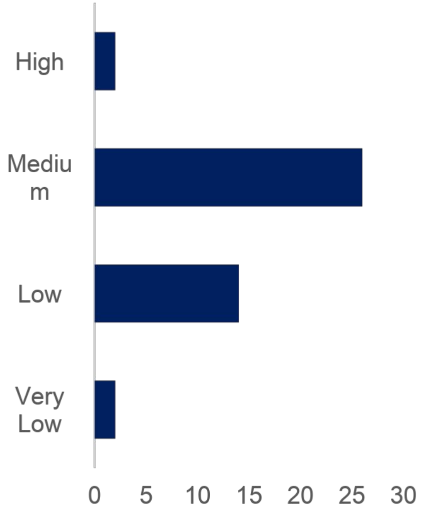
Comparison: survey responses vs DNSAI data



- Many respondents unsure about level of Abuse in their TLD. Hence, comparison with DNS Abuse Institute (DNSAI) data.
- DNSAI Compass data refers to phishing and malware only.
- Vast majority: less than 0.05% of abusive domains, less than 20 names reported as DNS Abuse.
- DNS Abuse rate of 0.05% means: only noticeable number (e.g. >100) for ccTLDs with large domain portfolio. This may explain why respondents were unsure about levels of abuse in their ccTLDs

What stood out?

Pricing variation across ccTLDs

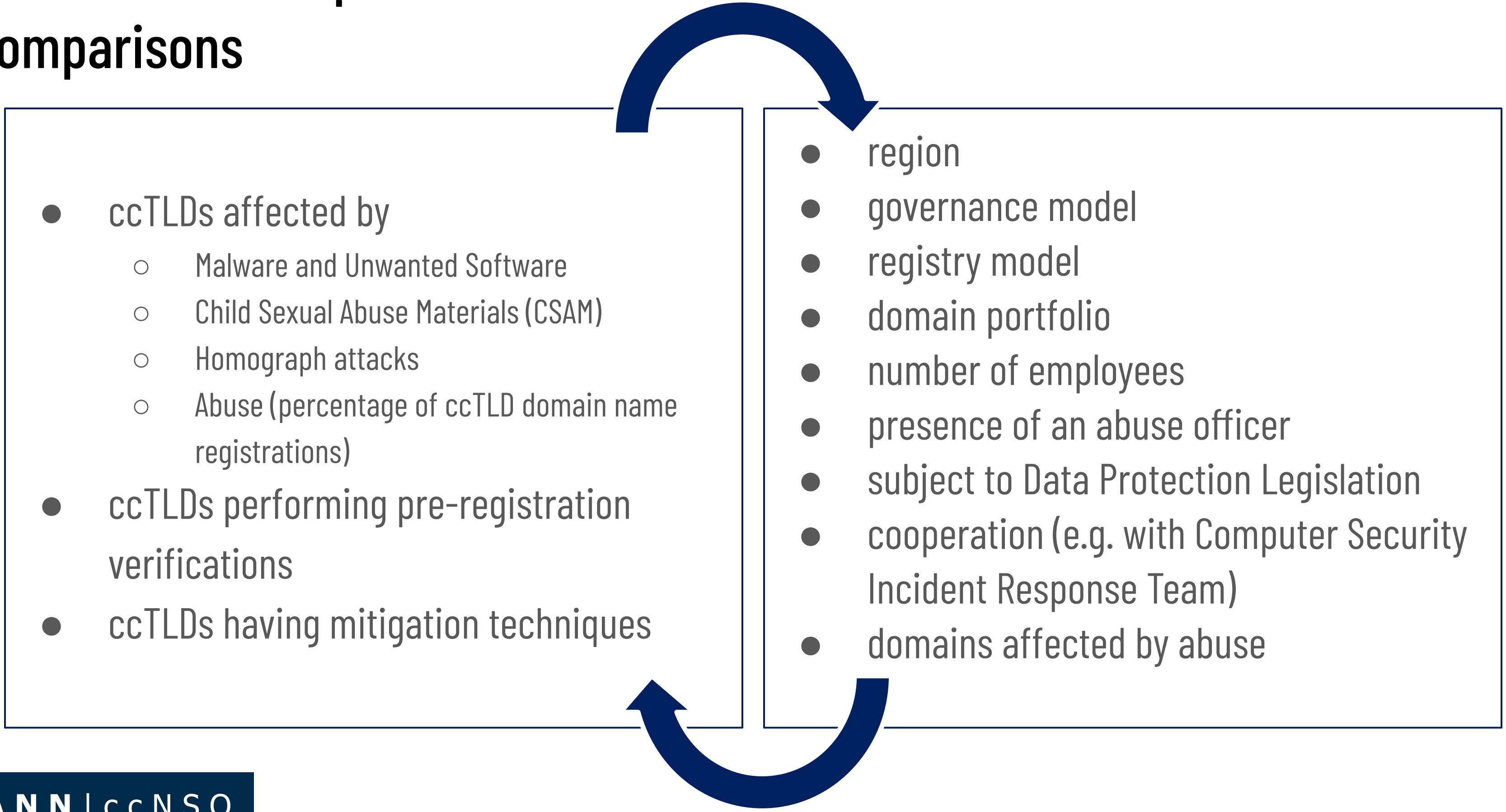


Legend
At retail level

High: > 100 USD
Medium: 21-99 USD
Low: 6-20 USD
Very Low: < 5 USD

- Largest ccTLDs in terms of volume of names generally in the low price range
- No discernible correlation of price with the level of DNS Abuse
- Data based on registrar and ccTLD registry pricing, where publicly available (44 ccTLDs)

Webinar on 28 September: comparisons



- ccTLDs affected by
  - Malware and Unwanted Software
  - Child Sexual Abuse Materials (CSAM)
  - Homograph attacks
  - Abuse (percentage of ccTLD domain name registrations)
- ccTLDs performing pre-registration verifications
- ccTLDs having mitigation techniques

- region
- governance model
- registry model
- domain portfolio
- number of employees
- presence of an abuse officer
- subject to Data Protection Legislation
- cooperation (e.g. with Computer Security Incident Response Team)
- domains affected by abuse

DASC survey: Main Findings

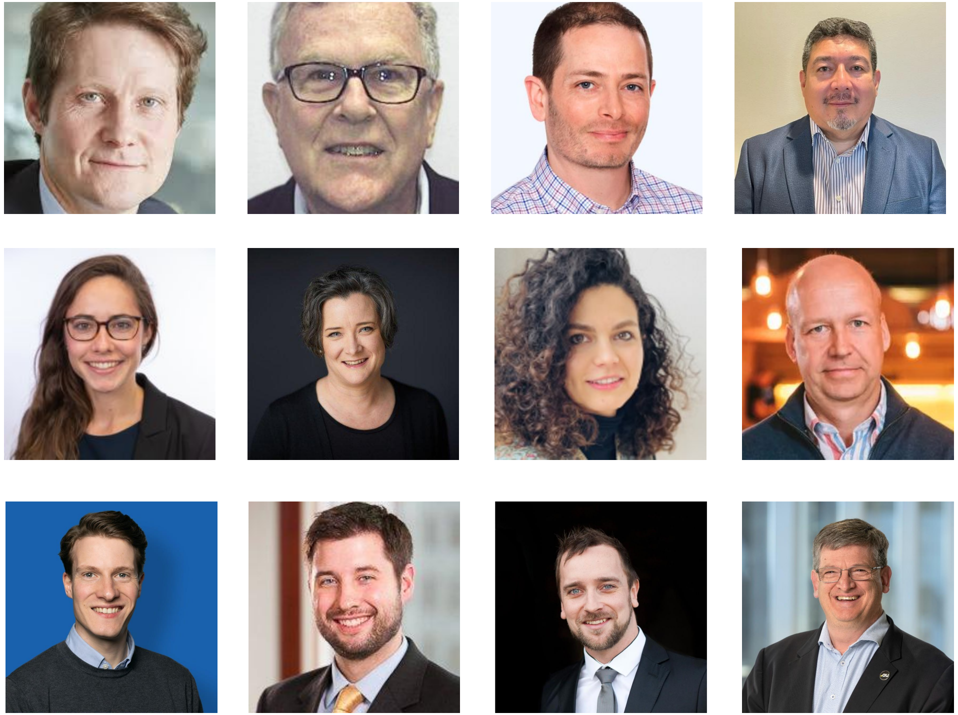
- Overall, relatively low levels of abuse for ccTLDs
    - Many ccTLDs do take action, despite respondents saying they have limited resources, and do not have access to tools
    - Different types of ccTLDs do perform checks, regardless of their region, governance model, registration model, domain portfolio size, number of staff
- Checks could happen prior to registration, but are more often done shortly after registration, or when abuse is being detected

ICANN78: Tools & Measurements | Wed., 25 October (11:15-15:15 UTC)

Learn more about different perspectives on tools and measurements of DNS Abuse. DASC reminds the ccTLD community about its repository and invites ccTLDs globally to contribute. Finally, DASC is proud to launch a dedicated email list at ICANN78, as a useful resource for ccTLDs.

Session chair: Nick Wenban-Smith (.uk)

1. Welcome & introductions
2. DASC resources for ccTLDs: DASC repository, e-mail list
3. Tools & Measurements: different perspectives
4. Dialogue between GNSO and ccNSO DNS Abuse Working Groups on similarities and differences
5. Wrap-up & Closure



What happens post ICANN78?

Suggestions from ICANN77:

- Do data validation and registration policies for ccTLDs relate to DNS abuse, if so how?
- How can ccTLDs effectively work with registrars to mitigate DNS abuse?
- What are the tools and measurements ccTLDs can use to mitigate DNS abuse?
- Do ccTLD governance models and regulatory frameworks impact DNS abuse?

Thank you!

ccnsosecretariat@icann.org

ICANN | ccNSO