Overview on
DNS Abuse Mitigation
- A Starting Landscape

At-Large Capacity Development Webinar & Discussion

Justine Chew
ALAC Co-Vice Chair
ALAC Liaison to GNSO

Natálie Terčová
ALAC Leadership Team Member

Matthias Hudobnik
ALAC Liaison to SSAC

Laura Margolis
ALAC Liaison to ccNSO

14 April 2026

ICANN
AT-LARGE

Purpose of this Call

Following…

1. Deep Dive on DNS Abuse – CPWG, 15 Jan 2025
2. DNS Abuse Strategy introduction – CPWG, 25 Jun 2025 …

Let's examine the current landscape of stakeholders / activities around DNS abuse mitigation, to figure out ….

- Where At-Large could play a role;
- What role(s) At-Large should play and how;
- How should/could At-Large mobilize to undertake those roles;
- What else should At-Large pay attention to; …

…. to develop OUR strategy for combating DNS abuse

Flashback: At-Large DNS Abuse High-Level Strategy Development

Note: Strategy should consider preventive, in addition to curative measures

A Starting Landscape

- Key Stakeholders

- Role, Limits
- Relationships
- Impact

ICANN OCTO – Security, Stability & Resiliency Dept.

26 February 2026- At-Large held a webinar with ICANN OCTO (SSR team)

- Focus: **understanding DNS Abuse and available mitigation tools**
- Followed by a **joint ALAC–OCTO session at ICANN85 (11 March 2026)**
- Objective: strengthen shared understanding of **data-driven and preventive approaches to DNS Abuse mitigation**

Context and Challenges

Domains used for: phishing, malware distribution, botnet command-and-control

The DNS ecosystem creates **opportunities for malicious actors**, especially at scale

Key structural challenge:

- Security outcomes are often shaped by **misaligned incentives**
- Actors responsible for prevention do not always bear the consequences of abuse

Implication:

- Effective mitigation depends on **robust, well-designed metrics** to guide decisions and resource allocation

Resources:
[1] 26 February 2026 At-Large Meets OCTO-SSR Webinar: ICANN83 ALAC-OCTO Joint Session Recap on an introduction to OCTO-SSR and its work
[2] 11 March 2026 ALAC-OCTO Session at ICANN85, Mumbai to further understand the work of OCTO-SSR, including some new initiatives

Key Implications for At-Large

Malicious actors often register **large volumes of domains in short timeframes**, forming coordinated abuse campaigns

OCTO-SSR approach:

Combines: registration data + DNS data + reputation data (RBLs)

Identifies **"associated domains"** → detects entire abuse campaigns, not just single domains

Key findings:

- Methods can identify **>50% of known abusive domains** and uncover new ones
- **Data delays limit proactive detection** → timeliness is critical

Why this matters for At-Large:

- Enables shift to **preventive (proactive) user protection**
- Highlights need for:
  - **better access to high-quality data**
  - balanced approaches (false positives vs. missed abuse)
- Supports informed input into **policy discussions on DNS Abuse mitigation**

Reputation Data: Role and Limitations

Reputation data identifies potentially malicious domains, IPs, or URLs based on observed behavior

Commonly used in **Reputation Block Lists (RBLs)** to support detection and mitigation

Key limitations:

- No single dataset provides complete or consistent coverage
- Data sources differ in:
  - collection methods
  - scope and focus
  - update frequency

Critical evaluation factors:

- Degree of **overlap vs. unique data** across sources
- **Timeliness** (how quickly threats are detected and updated)
- Risk of **false positives and blind spots**

= Effective use requires **combining multiple data sources** and continuous validation

SSAC – Security and Stability Advisory Committee

- SAC115 – Definition of DNS Abuse

  "DNS Abuse"[1] means

  1. malware,
  2. botnets,
  3. phishing,
  4. pharming, and
  5. spam (when spam serves as a delivery mechanism for the other 4 forms of DNS Abuse)

- Other SSAC efforts / engagements in this area

Resources:
[1] Definition of DNS Abuse, Section 2.1 of SAC115 (https://www.icann.org/en/system/files/files/sac-115en.pdf)

ccNSO – Country Code Names Supporting Org.

- DASC – ccNSO DNS Abuse Standing Committee
- Other ccNSO efforts / engagements in this area

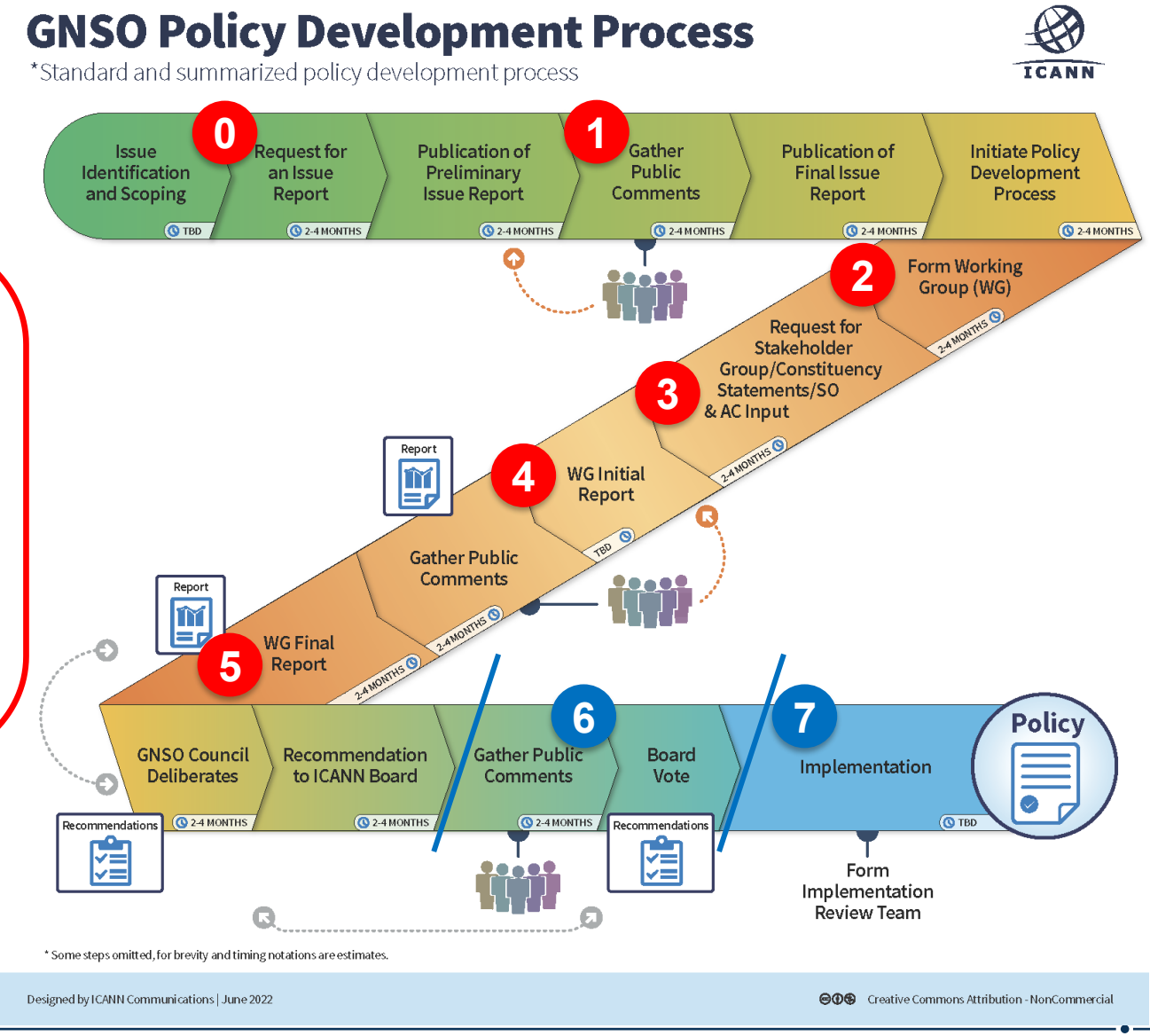
GNSO – Generic Names Supporting Org.

- Key gTLD DNS Abuse mitigation contractual obligations
  - Registrar Accreditation Agreement (RAA) sec 3.18
  - Registry Agreement (RA) Spec. 6 sec 4; Spec. 11 sec 3(b)

- Avenues -> obligations
  - Direct CPH-ICANN negotiations – eg. 2024 Global Amendments to the 2013 RAA & Base RA
  - **Consensus Policy**
    - Generally results out of PDPs
    - Implemented by Contracted Parties
      – https://www.icann.org/en/contracted-parties/consensus-policies
    - Implemented by ICANN Org

ALAC/At-Large Participation in gTLD PDPs

- 0 Can initiate Issue Report
- 1 Submit ALAC comments
- 2 Participate in PDP Working Group
- 3 Provide ALAC early input
- ⊙ Discuss issues arising from PDP WG Charter/Charter Questions & deliberations with CPWG applying the Funnel
- ⊙ Establish ALAC positions, advocate positions in PDP WG deliberations
- 4 5 6 Submit ALAC comments (or Advice)
- 7 Participate in IRT



Source: https://gnso.icann.org/en/basics/consensus-policy/pdp

Flashback: GNSO DNS Abuse Mitigation Gaps (1st Look)

High Priority

6. Introduce friction in access to "bulk/batch" registrations	G2 Withhold unrestricted API access for new customers [5]
	G9 Lack of syntactic & operational registrant data validation [2]
	G12 Lack of proactive/timely verification at registration [2]
	G25 Lack of data on bulk registration abuse [1]
1. Associated domain check	G1 Investigate associated domains [4]
	G10 Broaden use of abuse data for preventive action [2]
12. Proactive vs reactive	G11 Minimal deterrent effect of reactive measures [2]
	G23 Challenges in real-time detection of short-lived abuse [4]
	G26 Underuse of predictive algorithms for early detection [1]
2. Complainant reports	G17 25% unactionable complaints [3]
	G27 Awareness on reporting abuse [1]
5. Enforcement challenges	G13 Disparate registrar abuse mitigation responses [3]
	G15 No sanctions/deterrents for recurring non-compliance by CPs [3]
	G20 Delayed ICANN enforcement actions [4]
	G29 Ambiguity in RAA, RA language ('reasonable', 'prompt') [3]
10. Mitigation info from CPs	G18 Measurement challenges due to 'uncharacterized' domains [4]
	G22 Limited transparency in mitigation actions taken reducing accountability & oversight [4]

← Preventive

Curative →

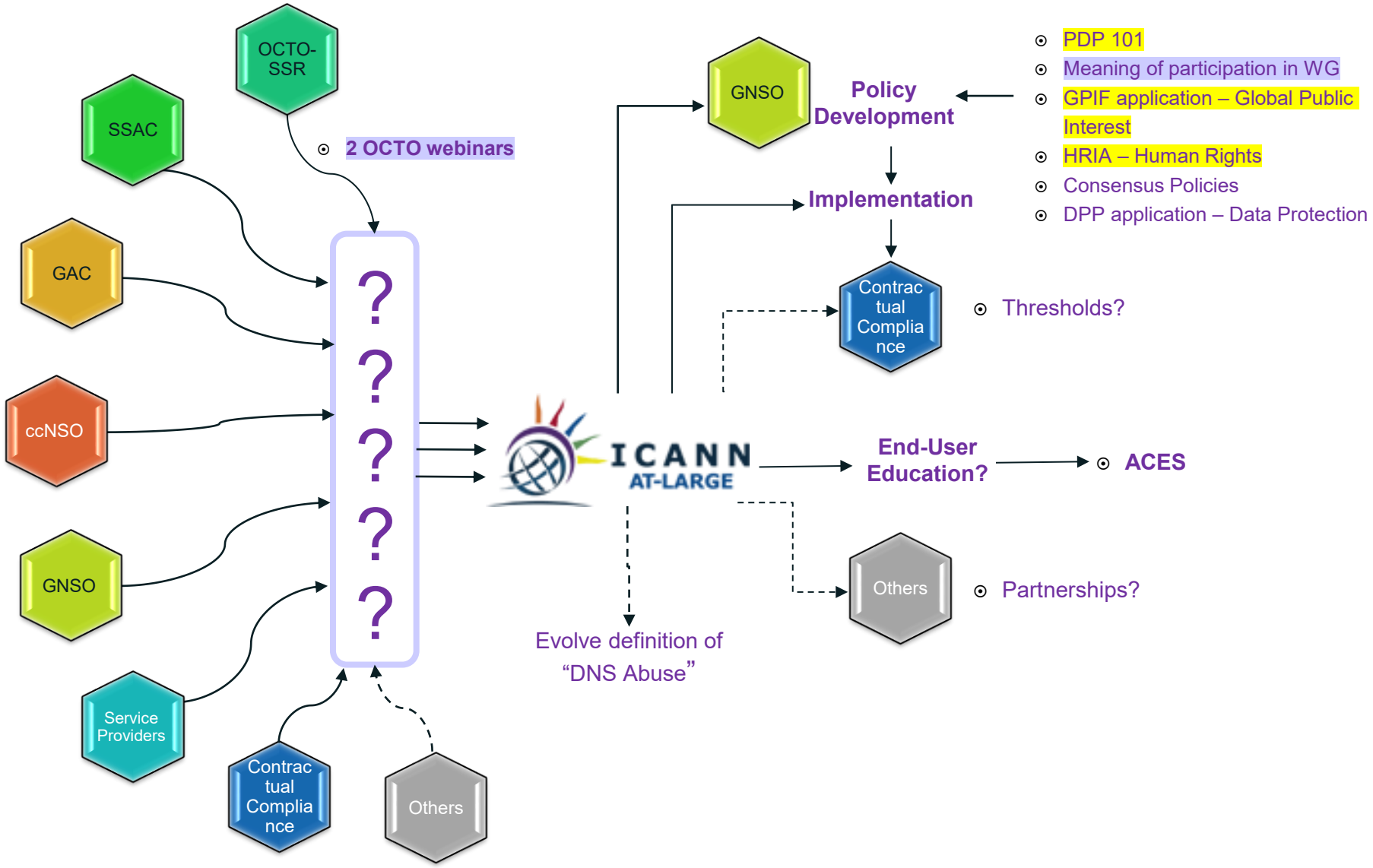
7. Forbid incentives promoting abuse	G21 Inconsistent registrar credential performance [4]
	G6 'Discounts' more prone to DNS abuse [2]
	G7 Free services more likely to be abused by threat actors [2]
11. Subdomains	G3 Unregulated subdomain abuse [5]
3. Compromised vs Malicious	G19 Attention to hijack legitimate domains [4]
	G24 Lack of definition [1]
4. Dispute Resolution	G4 Recourse mechanism for legitimately aggrieved registrants [5]
8. Industry coordination	G5 Inefficient coordination on DGA-based abuse to support LEA [5]
9. Lack of research/data	G8 Lack of empirical research on abuse factors [2]
	G14 No ICANN overview of mitigation actions outside of contract enforcement [3]

Low Priority

Source:

[1] GNSO Council DNS Abuse Small Team Report (Oct 2022)
[2] INFERMAL Report – Inferential analysis of maliciously registered domains (Nov 2024)
[3] ICANN Org Report on DNS Abuse mitigation requirements (Nov 2024)
[4] NetBeacon Blog – Analysis of Impact of ICANN Contract Amendments (Dec 2024)
[5] NetBeacon PDP Whitepaper (May 2025)

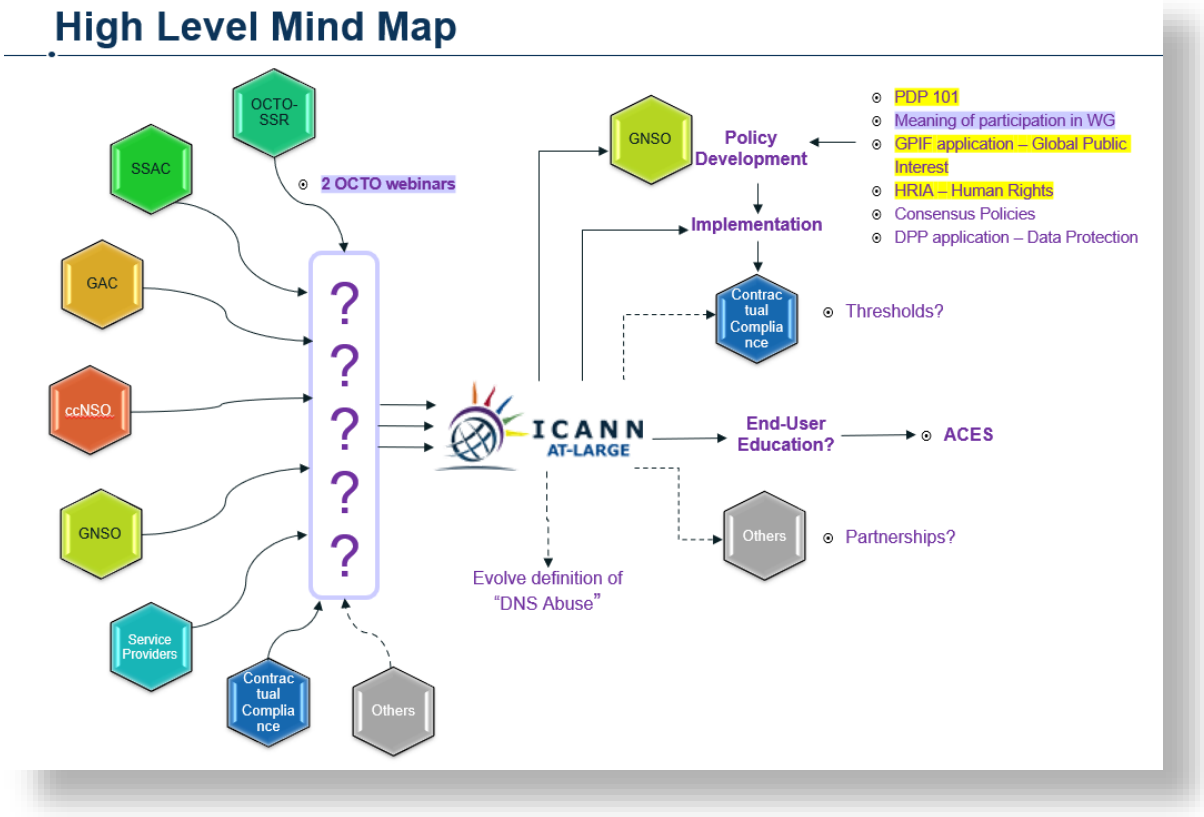
High Level Mind Map



Discussion & Feedback

Some prompts

- Our role in GNSO policy development processes
- Our role in awareness/education campaigns (via ACES?)
- Involvement with/of other stakeholders, partnerships



GOOGLEDOC FOR INPUT

Close

THANK YOU FOR YOUR PARTICIPATION

We will be back for more!