# DNS Abuse Mitigation

GAC Topic Leads:
Susan Chalmers (United States)
Janos Drienyovszki (European Commission)
Tomonori Miyamoto (Japan)

Guest Speakers:
Martin Kunc, CZ.NIC, National CSIRT of the Czech Republic
Karen Rose and Greg Aaron, Interisle Consulting Group
Graeme Bunton, NetBeacon Institute

10 June 2025 - ICANN83

ICANN | **GAC**
Governmental Advisory Committee

# Agenda

1. **Introduction**

2. **Updates on DNS Abuse Landscape and Mitigation**

   - CZ.NIC: Presentation on a Phishing Campaign

   - Interisle: Scope and Distribution of Phishing

3. **Next Steps: Policy Development and Other Avenues for Progress**

   - NetBeacon: Proposed Topics for PDPs on DNS Abuse

   - GAC Proposals for PDPs

   - Procedural Avenues for Additional DNS Abuse Efforts

4. **GAC Prague Communiqué Consideration**

# 1. Introduction

- DNS Abuse mitigation is a priority issue for the GAC

- gTLD Registries and Registrars are contractually required to respond to reports of DNS Abuse

- ICANN contracts define DNS Abuse as the use of domain names, or the DNS system, to perpetuate *malware, botnets, phishing, pharming, and spam* (when used as a delivery mechanism)

- GAC Topic Leads (EC, JP, US) program covers:
  - Ongoing work taking place within ICANN
  - Reviewing and analyzing evidence and data
  - Sharing good practices about efforts outside of ICANN

# Introduction
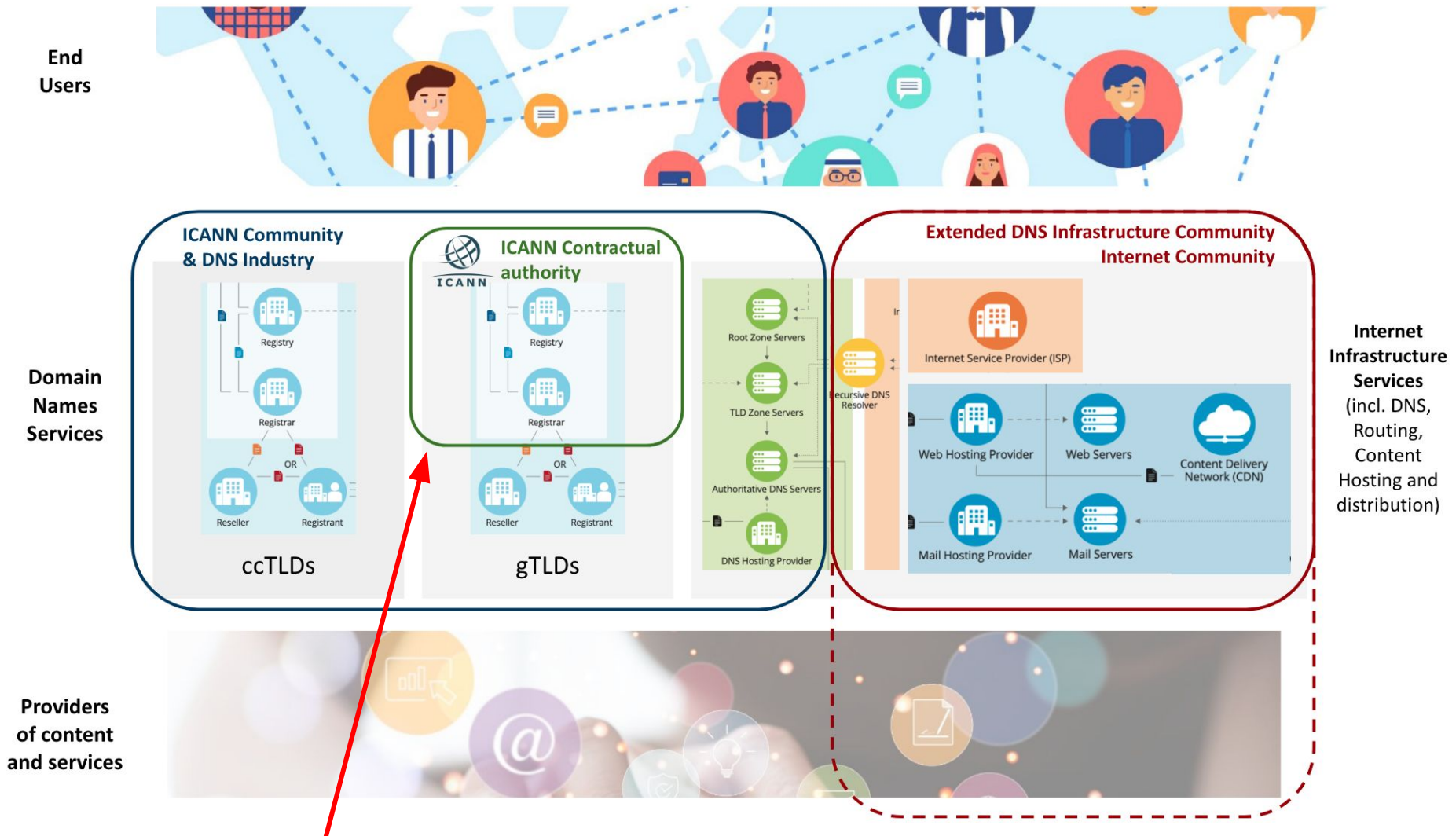


The scope of ICANN contractual authority is limited. The community of relevant actors is broader, within ICANN and outside ICANN. A lot is being done and can be done beyond the remit of ICANN's contracts.

# 1. Introduction

- Discussions in ICANN81: "What can be done within ICANN?"
  - Briefing from ICANN about RA/RAA compliance
  - Discussion with stakeholders about the effect of the RA/RAA amendments
  - GAC discussion about effects of the amendments and relevant experiences

- Discussions in ICANN82: Reviewing evidence and looking forward
  - Discussion of results from a GAC Survey on DNS Abuse (Jan-Feb 2025)
  - ICANN Compliance Update
  - Presentation & Discussion: INFERMAL Report, Domain Metrica

- Pre-ICANN83 Webinar on DNS Abuse Mitigation
  - Proposal for PDPs on DNS Abuse by the NetBeacon Institute
  - Contracted Parties Perspectives
  - Objective, Timeline, and Progress of the GNSO DNS Abuse Team

- **Discussion in ICANN83:**
  - **Emerging Topics for Policy Development on DNS Abuse**
  - **Timeline and Next Steps for GNSO on DNS Abuse**
  - **["What can be done within the broader ecosystem?" / Trusted Notifiers]**

# 1. Introduction

Registration → Abuse → Mitigation

**Countermeasure at registration (Proactive/Preventative measures)**

Reaction to the INFERMAL

- Restricting bulk API registration?
- Verification before activation / Shorter verification time

**Countermeasure at taking down (Abuse handling)**

Compliance enforcement activity

- Reporting for more transparency?

Shortening the reaction time

- Reducing burden of staff
- Trusted notifiers?

# Agenda

1.  **Introduction**

2.  **Updates on DNS Abuse Landscape and Mitigation**

    ○   CZ.NIC: Presentation on a Phishing Campaign

    ○   Interisle: Scope and Distribution of Phishing

3.  **Next Steps: Policy Development and Other Avenues for Progress**

    ○   NetBeacon: Proposed Topics for PDPs on DNS Abuse

    ○   GAC Proposals for PDPs

    ○   Procedural Avenues for Additional DNS Abuse Efforts

4.  **GAC Prague Communiqué Consideration**

# 2. DNS Abuse Landscape and Mitigation: CZ.NIC

Presentation by:     **Martin Kunc**

CZ.NIC, National CSIRT of the Czech Republic

# 2. DNS Abuse Landscape and Mitigation: Interisle

Presentation by: **Karen Rose** and **Greg Aaron**

Interisle Consulting Group

# Agenda

1. **Introduction**

2. **Updates on DNS Abuse Landscape and Mitigation**

   ○ CZ.NIC: Presentation on a Phishing Campaign

   ○ Interisle: Scope and Distribution of Phishing

3. **Next Steps: Policy Development and Other Avenues for Progress**

   ○ NetBeacon: Proposed Topics for PDPs on DNS Abuse

   ○ GAC Proposals for PDPs

   ○ Procedural Avenues for Additional DNS Abuse Efforts

4. **GAC Prague Communiqué Consideration**

# 3. Next steps / Topics for PDPs: NetBeacon Proposals

Presentation by:    **Graeme Bunton**

Executive Director, NetBeacon Institute

# 3. Next steps / Topics for PDPs: GAC Areas of Interest

- **Bulk Registration of Domain Names**
Seattle Communiqué (17 March 2025): *"the GAC considers it important to look further into the topic of bulk registrations of domain names as one of the most correlated drivers to DNS Abuse, according to the INFERMAL report."*

- **Proactive measures**
Hamburg Communiqué (30 Oct. 2023): *"the GAC reiterates the importance of considering proactive monitoring and transparency of reporting"*
  - Monitoring of registration behaviors
  - Greater identity verification requirements

- **Reporting Obligations**
  - ICANN Compliance, measurement programs, and cybersecurity research provide insights; CPH reporting obligations could complete the picture.

# 3. Next Steps / Avenues for Policy Action

- GNSO Small Team on DNS Abuse
  - To evaluate DNS Abuse mitigation efforts to date and determine whether further policy work is needed
  - Draft Findings and recommendation by Sep. 2025
  - Final Report to GNSO Council by Oct. 2025.

- GAC/Board Bilateral

- Policy Development Processes

- Contract Amendments

- GAC Advice

# Agenda

1. **Introduction**

2. **Updates on DNS Abuse Landscape and Mitigation**

   ○  CZ.NIC: Presentation on a Phishing Campaign

   ○  Interisle: Scope and Distribution of Phishing

3. **Next Steps: Policy Development and Other Avenues for Progress**

   ○  NetBeacon: Proposed Topics for PDPs on DNS Abuse

   ○  GAC Proposals for PDPs

   ○  Procedural Avenues for Additional DNS Abuse Efforts

4. **GAC Prague Communiqué Consideration**

# 4. Communiqué Consideration

- ## Issues of Importance

  - **Reviewing the landscape of DNS Abuse and mitigation**
  - **Topics for Targeted Policy Development on DNS Abuse**
  - **Next Steps for DNS Abuse prevention and mitigation before further delegation of New gTLDs**

- ## Advice

  - **Encouraging targeted, narrowly-scoped PDPs that deliver consensus outcomes on a much faster timeline?**

# New Agenda - Plenary Session (75 min)

1. **Introduction (incl. Overview of challenges/opportunities for action on DNS Abuse) [5 min] - Tomo**

2. **Updates on DNS Abuse Landscape and Mitigation - Moderation: Tomo**

   a. **Host Country Presentation on a Phishing Campaign incl. Q&A [15+5 min > 25 min]**

   b. **Interisle Report on Phishing (magnitude of the problem) [5-10 min > 35 min]**

3. **Discussion of next steps / procedural avenues for progress and possible topics for "micro-PDPs" [35 min > 65 min]  Moderation: Janos / Susan**

   a. **Overview of NetBeacon Proposals [5 min]**

   b. **Discussion of additional potential PDP ideas  [10 min]**

      – **Bulk Registration + Proactive measures (risk-based approaches, registration behaviors monitoring, verifications at time of registration before delegation) - Janos**

      – **Reporting Obligations - Susan**

   c. **Presentation of procedural avenues for additional DNS Abuse efforts (incl. reference to what's understood of the DNS Abuse Small Team's plans) - Susan [5 min]**

   d. **GAC Discussion [10 min]**

4. **GAC Discussion on Next Steps / Communiqué Consideration [5 min > 75 min]**