
ICANN
83
POLICY
FORUM
ICANN | GAC

GAC Session on Security and Stability

09:00-09:35 - GAC Meeting on DNS Blocking and OSS with the SSAC (35 mins)
09:35:10:15 - GAC Meeting on DNSSEC and Quantum with SIDNLabs (35 mins)

Wednesday 11 June 2025
09:00-10:15 CEST

ICANN | GAC

83 POLICY FORUM

Agenda

1. **GAC Meeting with the SSAC on DNS Blocking and Open-Source Software (OSS) (35 mins)**
   - Domain registration data access (5 mins)
   - Update on the SSAC Free and Open-Source Software Work Party (5 mins)
   - Briefing on SAC 127: DNS Blocking Revisited (25 mins)

2. **GAC Meeting with SIDNLabs on DNSSEC and Quantum (35 mins)**

83 POLICY FORUM

Domain Registration Data Access

Ram Mohan

Consistent Guidance to ICANN on Domain Registration Data Access

Collectively, the SSAC's recommendations from recent publications (SAC101v2, SAC118, SAC122) urge the creation of an access system with the following principles:

- ➜ **Structured & Expedited:** Formalize processes to ensure legitimate requests, especially urgent ones, are handled efficiently and predictably.
- ➜ **Policy-Driven:** Establish clear policies on response times and procedures, removing ambiguity for all parties.
- ➜ **Transparent & Data-Informed:** ICANN Org should compile and share metrics on data requests to guide the evolution of policy and ensure community oversight.
- ➜ **Foundational to Security:** Acknowledge that appropriate access to registration data is not an afterthought, but a foundational element of DNS security and stability, a principle established in our early work and reinforced in our feedback to the EPDP.

Our Overarching Goal: To ensure that any policy for gTLD registration data access is robust, well-defined, and serves the critical needs of the global Internet community in protecting against security threats.

Free and Open-Source Software (FOSS)

Maarten Aertsen

Recognizing Unique Characteristics of FOSS for Effective Policy

- DNS relies heavily on software created and maintained through Free and Open-Source Software development practices
- FOSS has unique development and governance characteristics compared to proprietary software
- **Growing Concern:** new software liability and security regulations are being developed without fully *understanding* and *considering* the FOSS model
  - Misunderstandings about FOSS can lead to policies/regulations that inadvertently weaken the DNS infrastructure
- **Objectives:**

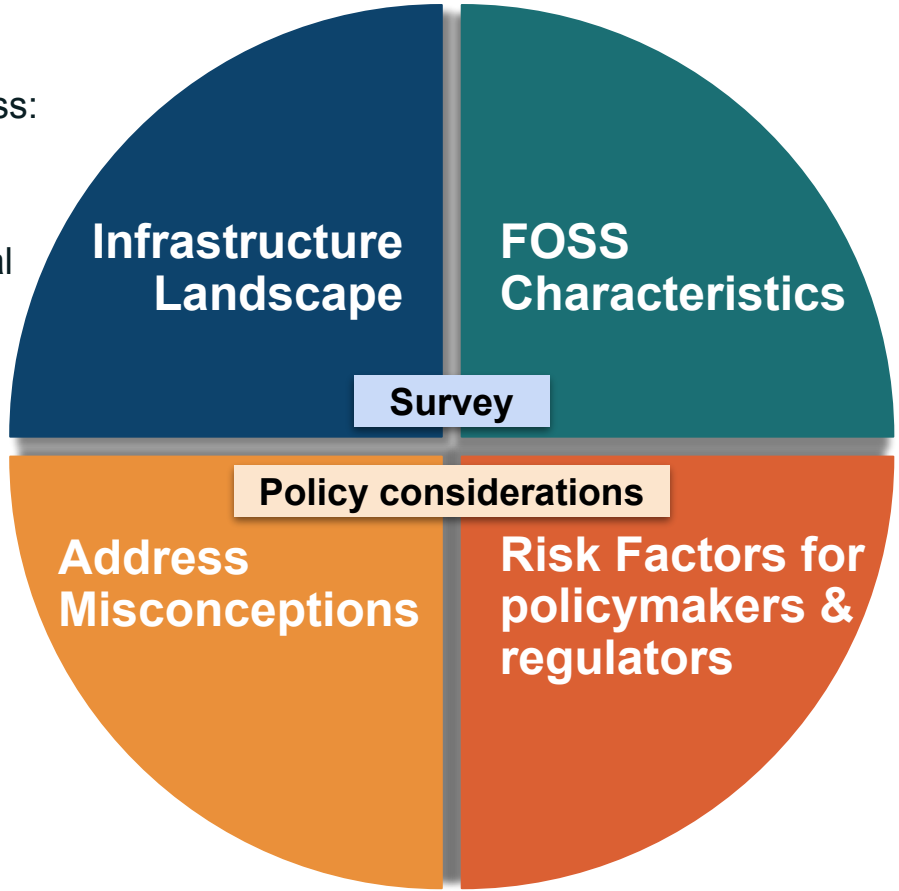
  (1) Make visible the critical reliance on FOSS in the DNS

  (2) Equip policymakers with the knowledge necessary to avoid policies/regulations that could unintentionally harm the FOSS ecosystem and, consequently, the DNS

Key Areas of Investigation

Map FOSS usage across:

- Domain registration (registries)
- Publication & Retrieval (DNS nameservers, DNS resolvers)



Analyze & contrast:

- FOSS & physical goods, proprietary software
- FOSS in general and FOSS popular in DNS

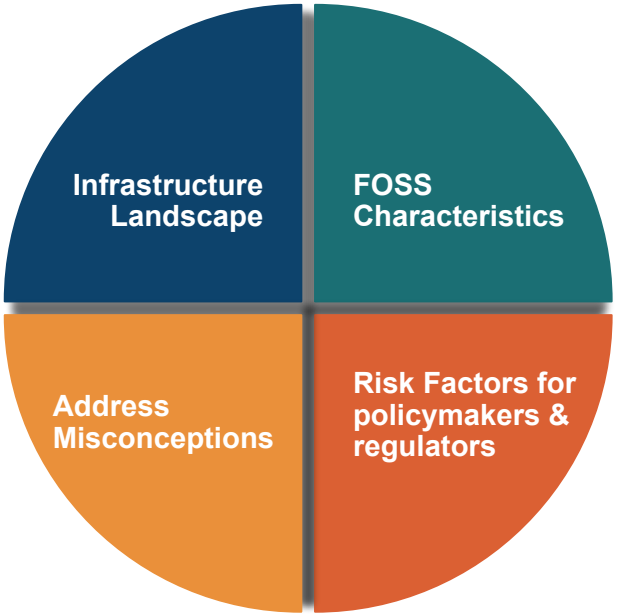
- Clarify assumptions both common and misplaced encountered in practice

Relevant risk factors for:

- Development of FOSS
- Operation of FOSS
- Regulatory approaches to FOSS

Timeline: aim for publication ahead of ICANN84 - Muscat

Continued use of FOSS in DNS and domain name registration is a strength, but there are key risks to consider.



ICANN 84 - Muscat:

SSAC to offer guidelines to policy makers and regulators concerning the use of FOSS

SAC127: DNS Blocking Revisited

Greg Aaron & Warren Kumari

ICANN83

11 June 2025

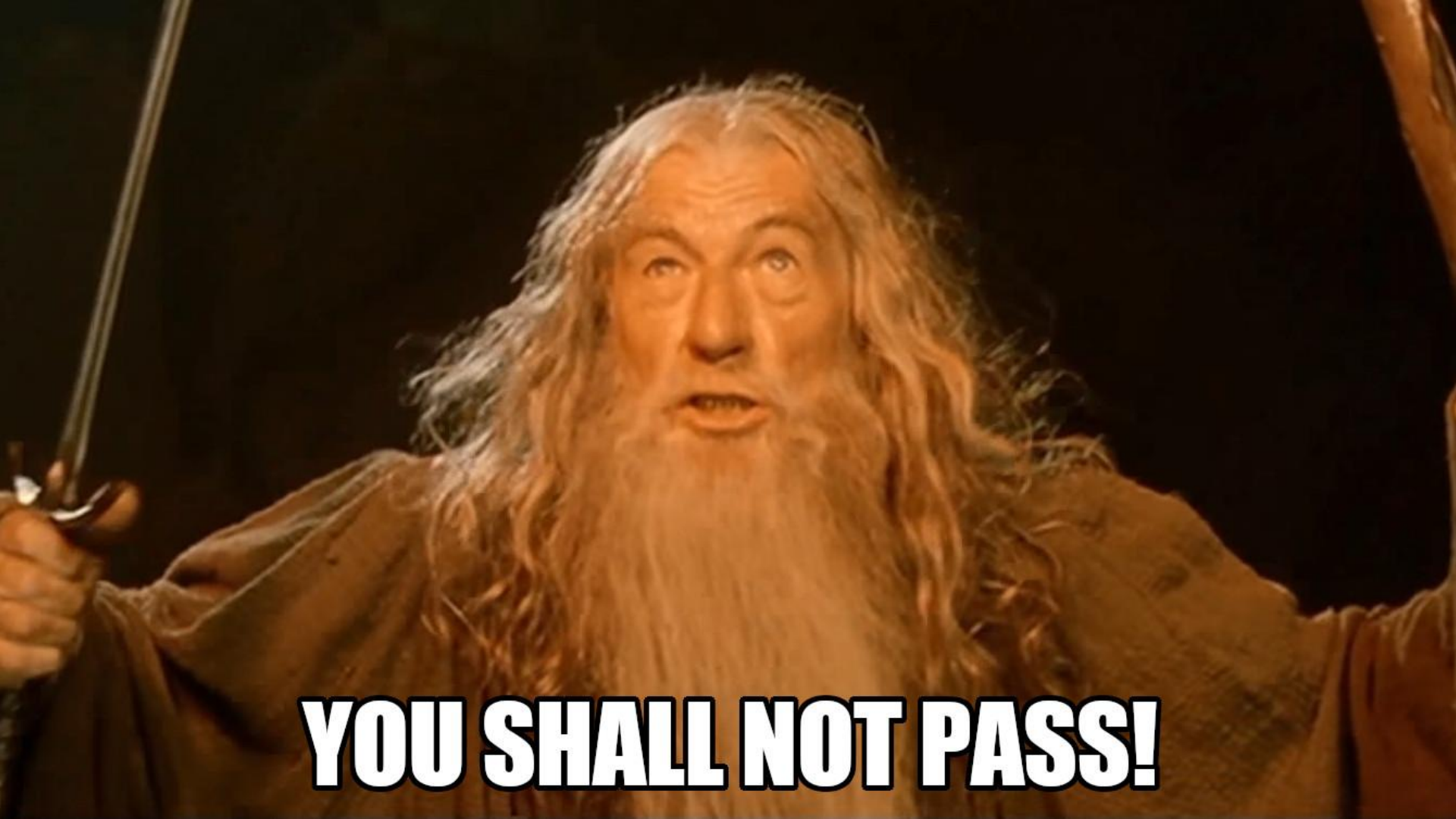
ICANN | SSAC

Security and Stability Advisory Committee

What is DNS blocking and why is it used?

What is DNS Blocking?

- DNS blocking is a technique that restricts access to domain names
- **Goal**: Prevent a set of users from accessing content and services that use a domain name.
- Accomplished by either blocking DNS queries or directing user to a different destination.
- Blocking affects all services that use DNS lookups, including Web, email, network management.


YOU SHALL NOT PASS!

Why is DNS Blocking Used?

Security

To protect users from online threats by blocking access to sites known for malware, phishing, and scams. This is a common security tool used by web browsers and email providers

Content Control

To enforce internal rules within an organization or household. This includes schools blocking gaming sites, companies blocking adult content, or parents enabling child-protection filters.

Legal & Political Reasons

Mandated by governments to block access to illegal activities, such as copyright infringement or incitement to violence. It is also used as a tool for censorship to control access to information.

Domain Suspension, Domain Seizure

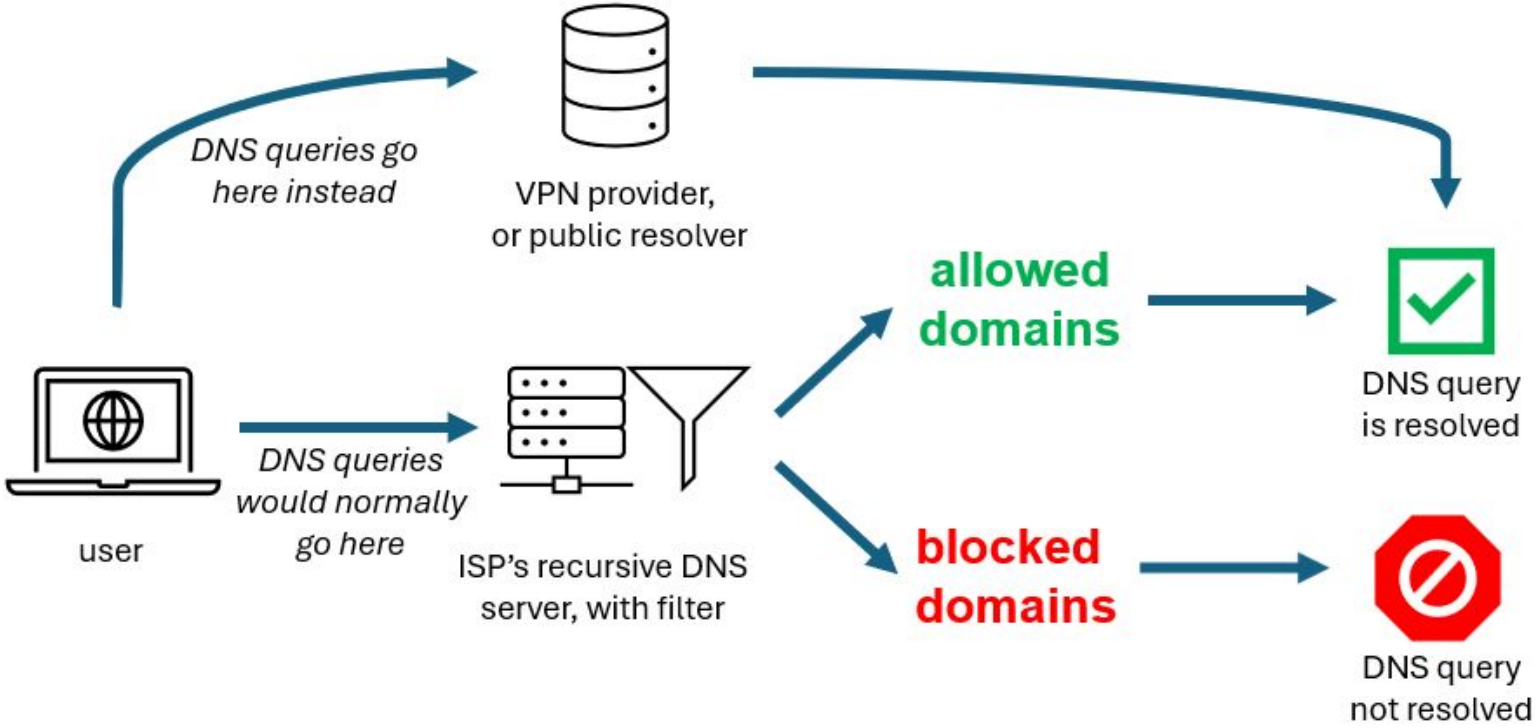
- Suspension is not “DNS blocking” but achieves a similar goal: prevents access to a domain and its content.
- Registrar or registry operator can suspend a domain.
- Removes domain from the DNS zone. Domain stops resolving for everyone.
- Domains can also be “seized”: domain taken away from control of the old registrant. The domain may redirect to different content.

A Note

“The SSAC notes that whether an action constitutes censorship, or the legality of any specific case of DNS blocking, will depend upon local laws (which vary widely across the globe), and can involve personal convictions, about which people may vary in good faith. For these reasons, the SSAC does not make statements in this report about the propriety of specific cases of DNS blocking – such discussions are more suited for political fora. The merits or advisability of governmental or other attempts to control access to resources on the Internet are beyond the scope of this report.”

Circumventing DNS Blocking

Circumvention: Go around the blocking

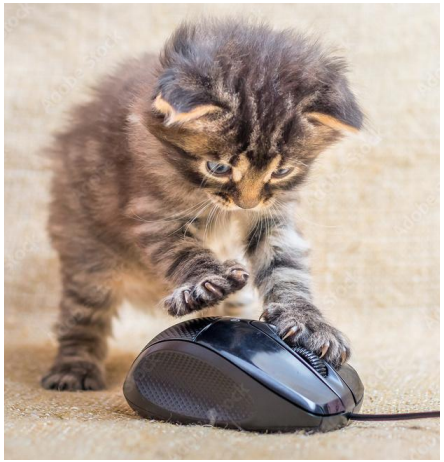


Circumvention by users: Alternative DNS Servers

- User changes DNS settings on their device, to use a resolver that doesn't enforce the same blocking restrictions.
- Public resolvers: offer reliability, security, lack of filtering.
  - Easy to implement, especially for non-technical users. ~21% of users worldwide use public resolvers.
  - Examples:
    - Google Public DNS (8.8.8.8)
    - Cloudflare's public resolver (1.1.1.1)
    - Quad9 (9.9.9.9)
- Government-sponsored resolvers such as DNS4EU

Circumvention by users: VPNs (Virtual Private Networks)

- Encrypt Internet traffic and route through alternative servers. Allows users to:
  - Bypass geographical restrictions (example: streaming)
  - Evade censorship
  - Enhance privacy and anonymization
  - Secure DNS resolution
- Use of VPNs is widespread
- Ongoing “cat and mouse” game



DNS Blocking: Considerations and Consequences

Issue #1: Collateral Damage & Over-Blocking

- **Over-blocking** occurs when a block is too broad and accidentally affects innocent content, services, or users.
- This often happens when an entire domain is blocked to address a problem that exists only on a small part of it.

Case Study: Italy's Piracy Shield

The Program: Italy's "Piracy Shield" requires internet providers to automatically block domains designated by the telecom regulator (AGCOM) as piracy sites.

The Block: In October 2024, the program erroneously added a critical Google domain to its blocklist.

The Domain's Purpose: This domain was part of a Content Delivery Network (CDN) essential for the functioning of Google Drive and was also used by YouTube.

The Impact: For several hours, users across Italy were unable to download files from Google Drive, and YouTube's accessibility was also affected.

Issue #2: It's Often Ineffective

The effectiveness or “success” of DNS blocking is often a matter of degree

Alternative DNS Resolvers:

- Users can switch to a public DNS provider (like Google's 8.8.8.8 or Cloudflare's 1.1.1.1) that doesn't have the block.
- This is now incredibly easy; some providers offer free apps that change DNS settings with a single tap.
- Over 20% of all internet users already use public resolvers.

Virtual Private Network (VPN):

- A VPN creates a private, encrypted tunnel for all of a user's traffic, bypassing local blocks entirely.
- Their popularity has surged not just for bypassing blocks, but also for general privacy and accessing geo-restricted content.

Issue #3: It Can Weaken Security

Isn't it ironic…don't you think?

While often used for security, DNS blocking can also introduce new security risks in two main ways:

Training Bad Habits

- Blocking can cause browser security warnings (certificate errors).
- By teaching users to click "Ignore" to get past the block, it trains them to ignore warnings that are meant to protect them from real attacks.

Reducing Network Visibility

- When users bypass local DNS, network operators lose the ability to see DNS-based threats on their own network.
- This makes it harder to detect malware-infected computers or fight large-scale cybercrime.

SSAC Recommendations

SAC127 Recommendations

Recommendation 1: SSAC recommends that any entity implementing or mandating DNS blocking understand the implications of the technology.

SAC127 Recommendations

Recommendation 2: SSAC recommends that DNS blocking implemented by any entity—by a government or any organization that has policy, legal, or operational control over a network or service—follow these guidelines:

A. The entity should determine whether DNS blocking will fulfill its objectives.

B. The entity should have a clear policy about what and how it will block, with well-defined review and decision-making processes that minimize risk.

C. The entity should implement the policy using a technique that minimizes overblocking or collateral damage that could affect its users.

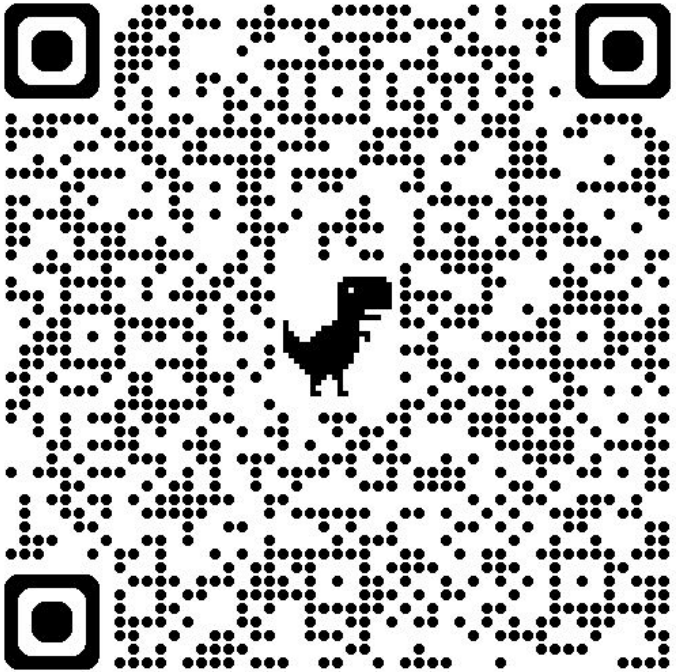
D. The entity should not affect networks or users outside its administrative control.

SAC127 Recommendations

Recommendation 3: SSAC recommends that operators of recursive servers use RFC8914 DNS Extended Error codes (see section 6.6 Extended DNS Error) to indicate to end users and troubleshooters that DNS blocking is taking place.

SAC127: DNS Blocking Revisited

Visit bit.ly/4kw1X3R or scan the QR code for **SAC127: DNS Blocking Revisited**



Discussion

waiting on finalization of shorter deck:
https://docs.google.com/presentation/d/1OhKnLng6HmKygdNjTwW2cWPJXfKItfQzRkVZgm4tTdU/edit?slide=id.g336bbdf72c7_0_0#slide=id.g336bbdf72c7_0_0

Thank you

GAC Meeting with SIDN Labs on DNSSEC and Quantum

Cristian Hesselman, SIDN Labs

Q&A