ICANN 81 | ANNUAL GENERAL MEETING

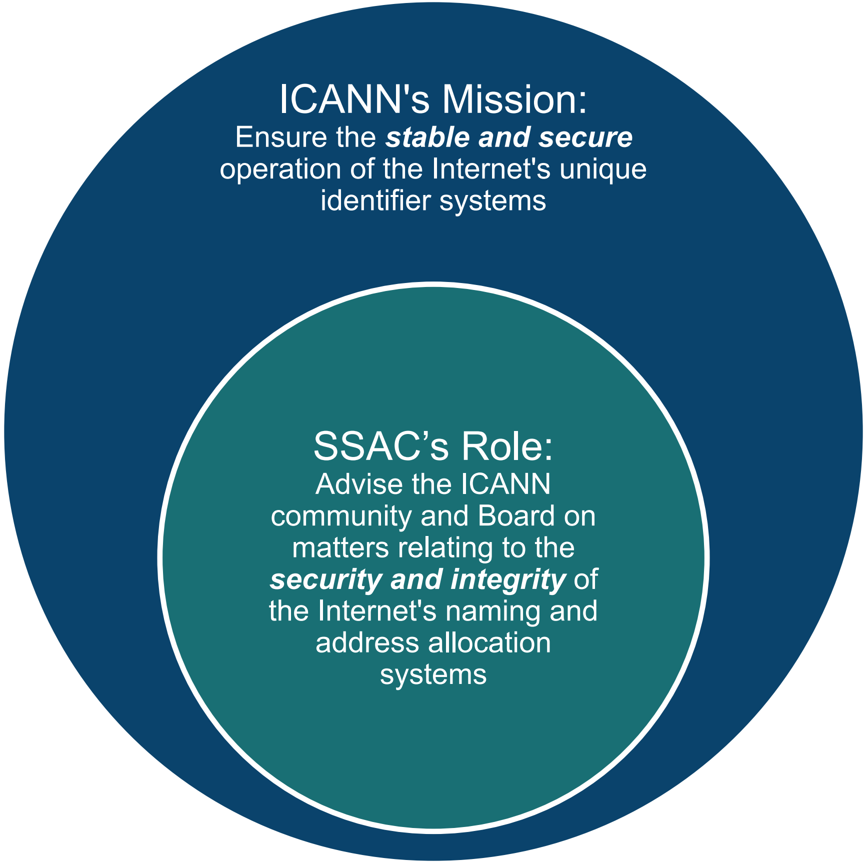
Joint Meeting
SSAC - GAC

Security and Stability Advisory Committee and ICANN

ICANN 81 AGM – Istanbul
10 November 2024

Agenda

- Introduction to SSAC
- SSAC’s Five Steady-State Topics
- DNS Abuse and AI
- Blockchain and the DNS
- SSAC and the GAC



ICANN's Mission:

Ensure the ***stable and secure*** operation of the Internet's unique identifier systems

SSAC’s Role:

Advise the ICANN community and Board on matters relating to the ***security and integrity*** of the Internet's naming and address allocation systems

Who We Are

Europe: 13

North America: 25

Asia/ Australia/ Pacific: 6

Latin America/ Caribbean islands: 0

Africa: 2

The SSAC Leadership Team (2024-2026)

Ram Mohan
Chair

Tara Whalen
Vice-Chair

James Galvin
ICANN Board Liaison

Danielle Rutherford
Policy Support Staff

John Emery
Policy Support Staff

Kathy Schnitt
Policy Support Staff

Jeff Bedser
Leadership Team

Barry Leiba
Leadership Team

Skills collectively include: Registry, DNS Operations, Privacy, Human Computer Interaction, Technical Standards, Risk Management, DNSSEC, Cryptography, DNS Abuse, Threat Intelligence, Internet messaging, Cybersecurity, Executive Leadership, Strategy, Public Policy, Data Analysis

5 Topics: The SSAC As An Authority

Intent

SSAC as an authority on key topics in ICANN

1	DNS Abuse	The most significant security issue facing our community.
2	New gTLDs	One of the largest strategic and tactical priorities for our community.
3	DNSSEC	A significant technology that improves DNS security. Still evolving.
4	Alternative Namespaces	New namespaces should want to integrate with the existing one. What are the issues?
5	Internet Governance & SSR	Add technical heft and provide meaningful advice for policy makers worldwide.

AI and DNS Abuse*

Jeff Bedser

* Credit to Laurin Weissinger, SSAC Member for key content

What is Machine Learning (ML) and Artificial Intelligence (AI) (AI)

AI Generated image

- **ML** is a subset of AI where algorithms learn from data to make predictions or decisions.
- **AI** encompasses broader techniques enabling machines to mimic human intelligence, including reasoning, learning, and problem-solving.
- **ML** is a key method within **AI**.

DNS Abuse - AI application?

AI Generated image

- Creating new text, images, videos, or other artifacts
  - Logo files of banks, ecommerce etc. for targets of phishing/pharming
- Generating ‘appearing as a human’ text to lure victims into the fraud
- Utilizing multi language support to craft directly targeted text in the regional language of the victim

Generative AI Technologies: Randomization is the New Threat

AI Generated image

Until now: Fighting DNS Abuse at scale has used pattern matching and recognition

1. Look for underlying infrastructure (NS records, hosts, IP addresses, Ry/Rr patterns.
2. HTML templates, file Hash values
3. Time and date correlation of domain name registration and delegation

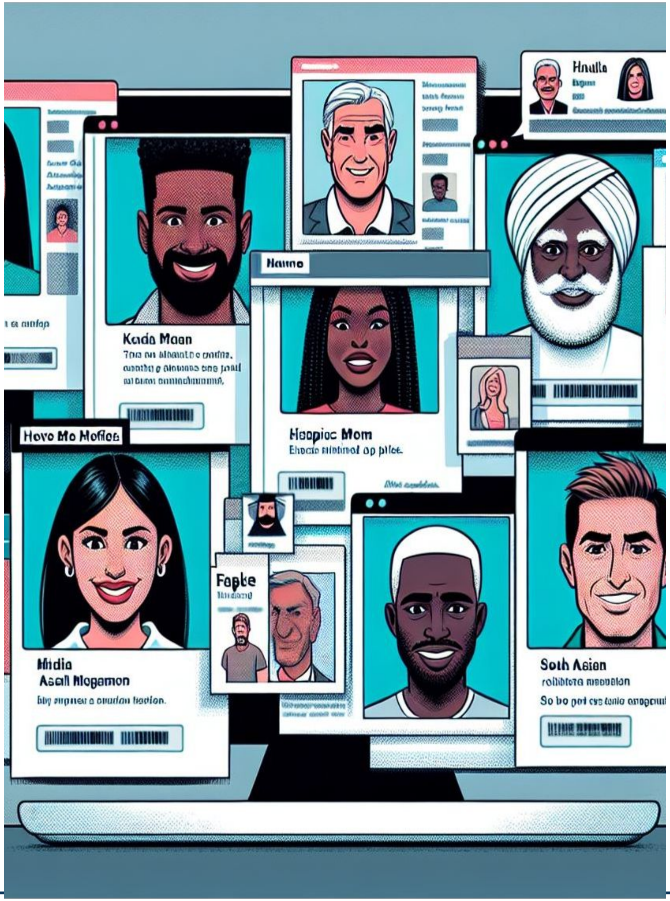
With generative AI, each specific domain or URL can be randomized.

Current methodologies of pattern matching become stressed.

What Are Other Uses of AI for Abuse?

Common New AI-based Attacks

- **Sockpuppeting** — Creation and use of fake identities, accounts, reviews, etc. (for use with Registration of domains and hosting accounts)
- **Non-consensual intimate imagery** (NCII); **Child sexual abuse material** (CSAM)
- **Falsification** — Fabrication of information / data, e.g. documents, pictures, (for use with registration of domains, accounts etc)



AI Generated image

Generative AI Misuse

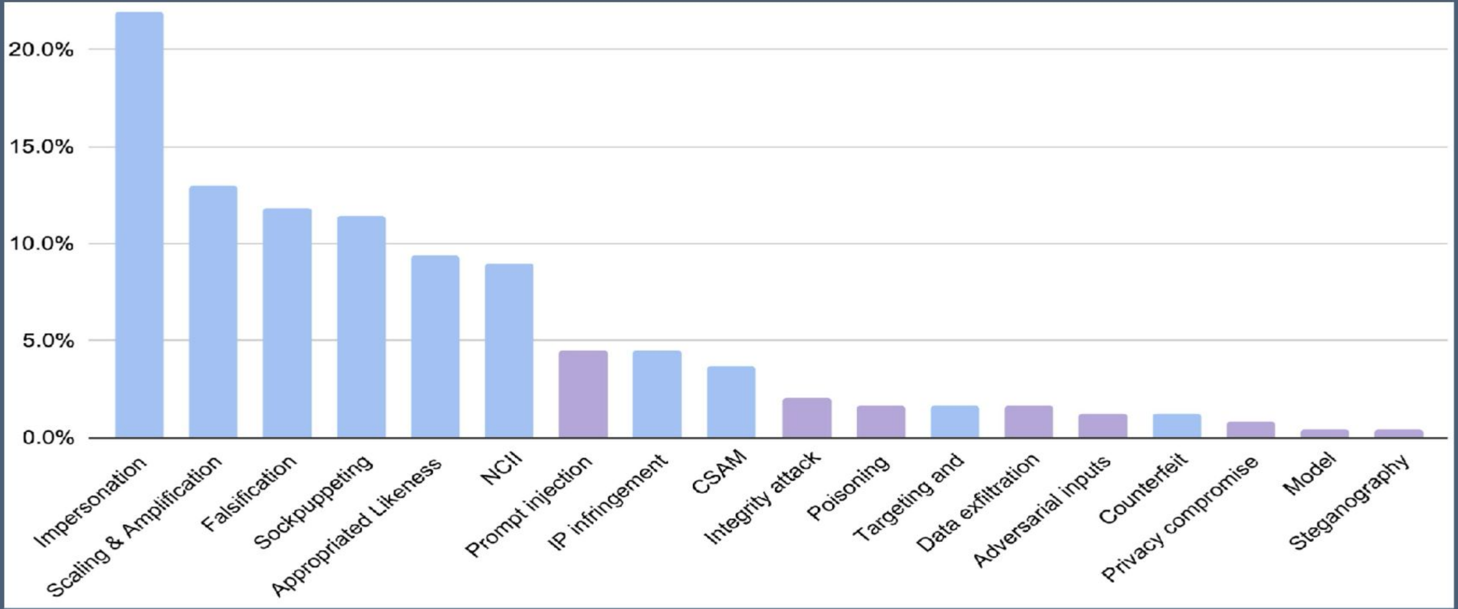


Figure 1 | Frequency of tactics across categories from: Generative AI Misuse: A Taxonomy of Tactics and Insights from Real-World Data — Marchal, Xu, Elasmar, Gabriel, Goldberg and Isaac (2024) — Note: Each bar represents the frequency with which a tactic was identified within our dataset. Each case of misuse could involve more than one tactic.

Crime: Increasing Scale and Reach

AI Generated image

- Even though the capabilities of AI-enhanced technology might not always lead to more sophisticated attacks, they certainly have the potential to increase **scale and reach**.
- Cybercriminals will progressively integrate AI techniques and the use of AI systems in their plans

Blauth, Gstrein, Zwitter (2022) Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI

Good News! It’s Not All Bad News!

AI Generated image

ML Identifies AI-Generated Phishing Emails With High Accuracy

AI Generated image

- AI can be as effective at detecting phishing emails as it is in generating them.
- AI-generated phishing emails are different from regular emails, and also from manually-generated phishing scam emails
- Natural Language Processing (NLP) enables Generative AI tools to understand, process, and manufacture texts that read and sound human and authentic.

Eze & Shamir (2024) Analysis and Prevention of AI-Based Phishing Email Attacks

AI must evolve to manage these threats

Attack vectors and strategies that use AI for abusive purposes

- Political disinformation
- Profit oriented abuse
- Scaling and speeding up criminal enterprises

Cyber crime = Money. Bad actors change strategies when necessary to ensure profits.

This is a continuation of the same threatscape where deployment of the newest technologies must match the pace of the bad actors.

Blockchain and the DNS

- SAC123: SSAC Report on the Evolution of Internet Name Resolution
- 2024 SSAC Workshop Panel: Blockchain and DNS
- Connect with the SSAC as you are building your policy papers on Blockchain and DNS

SSAC and the GAC

Capacity Building

How can we work with you to build capacity on key security and stability issues?

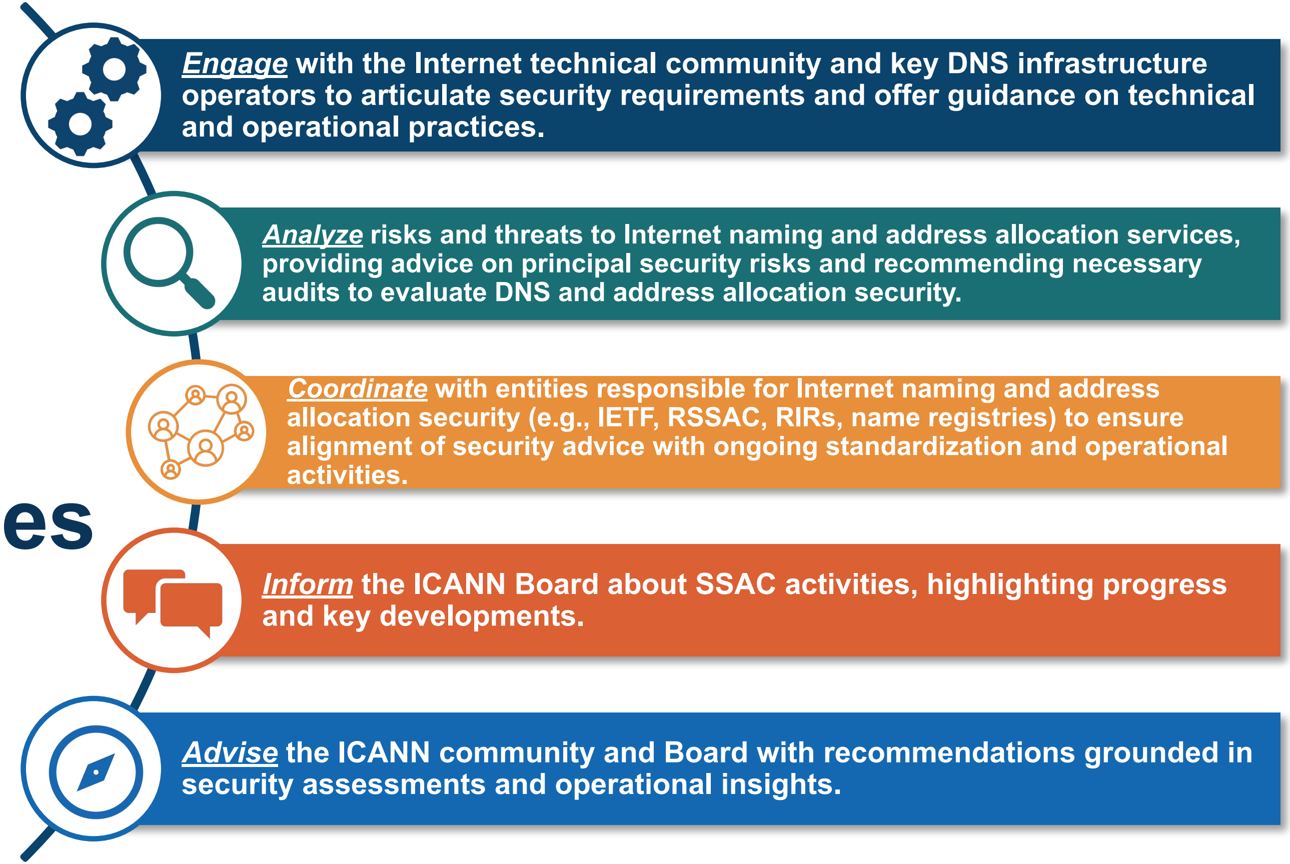
Security Briefing Papers

What are the most important security topics that we can provide briefing papers on?

Working with you and your Government

We can help you prepare for important meetings in your Government on SSR issues

SSAC's Responsibilities



Engage with the Internet technical community and key DNS infrastructure operators to articulate security requirements and offer guidance on technical and operational practices.

Analyze risks and threats to Internet naming and address allocation services, providing advice on principal security risks and recommending necessary audits to evaluate DNS and address allocation security.

Coordinate with entities responsible for Internet naming and address allocation security (e.g., IETF, RSSAC, RIRs, name registries) to ensure alignment of security advice with ongoing standardization and operational activities.

Inform the ICANN Board about SSAC activities, highlighting progress and key developments.

Advise the ICANN community and Board with recommendations grounded in security assessments and operational insights.

Questions for the SSAC?