ICANN 75
ANNUAL GENERAL
KUALA LUMPUR

SSAC Activities Update
September 2022

Agenda

- SSAC Overview
- Recent SSAC Publications
- Update on Name Collision Analysis Project
- Updates on SSAC Work Parties
- SSAC New Member Outreach
- Q&A

Security and Stability Advisory Committee (SSAC)

Who We Are

- **36** Members
- Appointed by the ICANN Board

What We Do

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

What is Our Expertise

- Addressing and Routing
- Domain Name System (DNS)
- DNS Security Extensions (DNSSEC)
- Domain Registry/Registrar Operations
- DNS Abuse & Cybercrime
- Internationalization (Domain Names and Data)
- Internet Service/Access Provider
- ICANN Policy and Operations

How We Advise

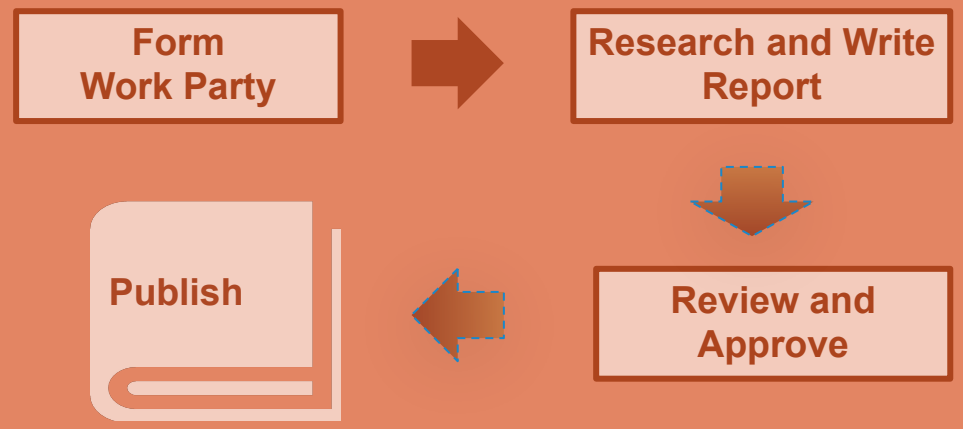
121 Publications since 2002

Security and Stability Advisory Committee (SSAC)

ICANN's Mission & Commitments

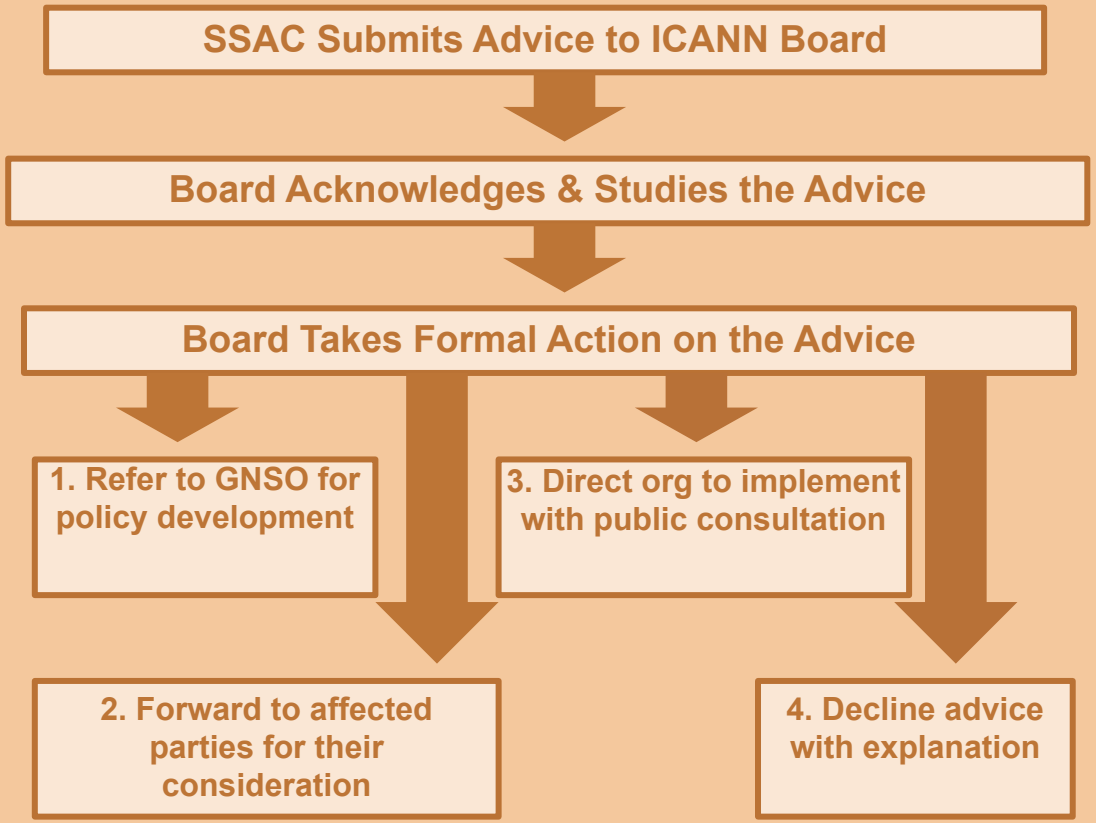
- Ensure the stable and secure operation of the Internet's unique identifier systems.
- Preserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet.

SSAC Publication Process



Consideration of SSAC Advice

(to the ICANN Board)



Security and Stability Advisory Committee (SSAC)

Recent Publications

[SAC121]: SSAC Briefing on Routing Security

[SAC120]: SSAC Input to GNSO IDN EPDP on Internationalized Domain Name Variants

Addendum to SAC114: Additional Context for Recommendation 1, Recommendation 3, Recommendation 7, and Additional References

ICANN | SSAC
Security and Stability Advisory Committee

Outreach

ssac.icann.org and SSAC Intro: www.icann.org/news/multimedia/621

www.facebook.com/pages/SSAC/432173130235645

SAC067 SSAC Advisory on Maintaining the Security and Stability of the IANA Functions Through the Stewardship Transition and SAC068 SSAC Report on the IANA Functions Contract: www.icann.org/news/multimedia/729

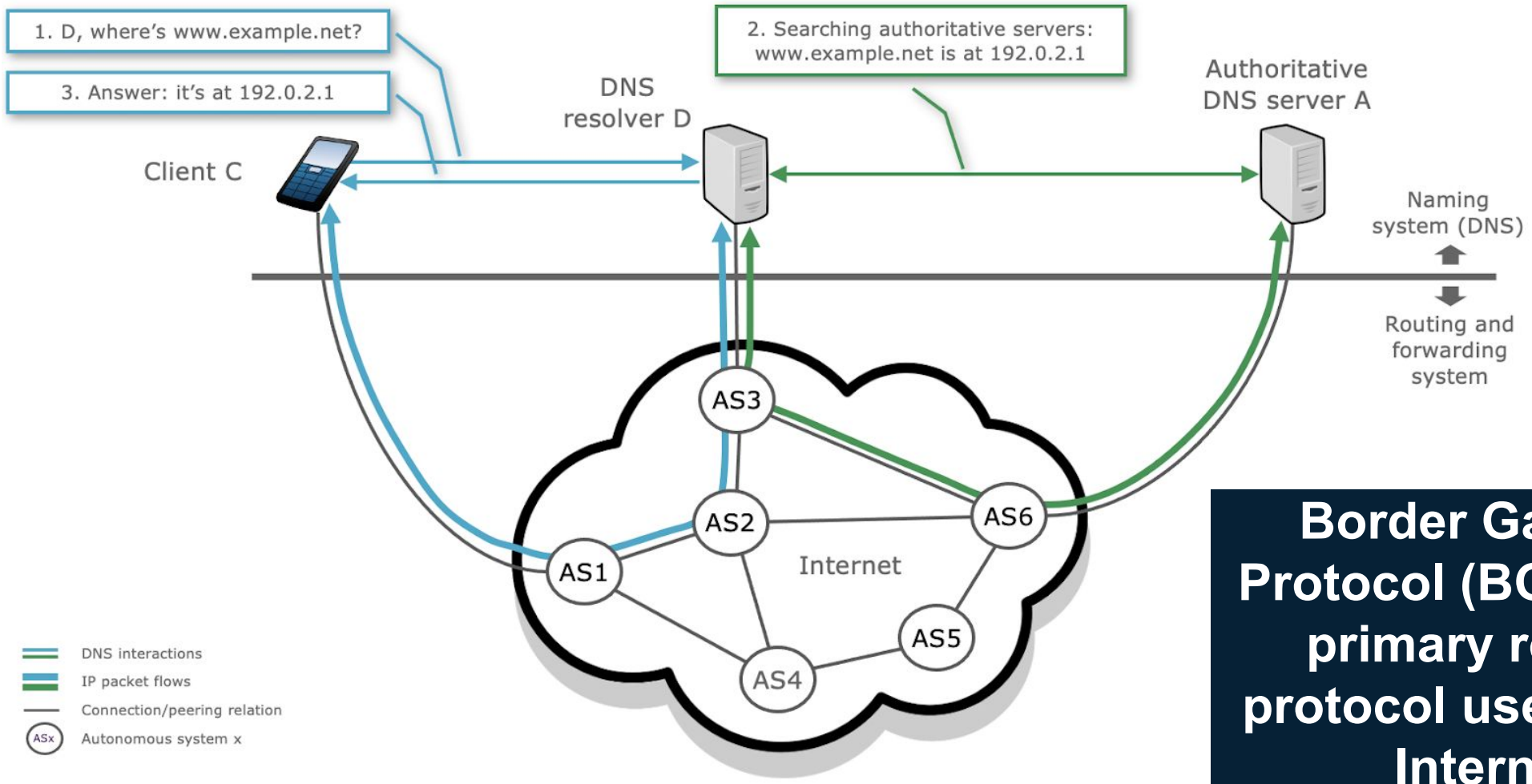
Recent SSAC Publications

SAC121: SSAC Briefing on Routing Security

SAC121: SSAC Briefing on Routing Security

- Background Technical Information
- Routing Security and the Domain Name System (DNS)
- Efforts to Enhance Routing Security
- Operating Secured Infrastructure
- Key Takeaways

Internet Routing for DNS Query



Border Gateway Protocol (BGP) is the primary routing protocol used on the Internet.

Figure 1: DNS traffic passing through multiple autonomous systems

Route Hijack for DNS Query

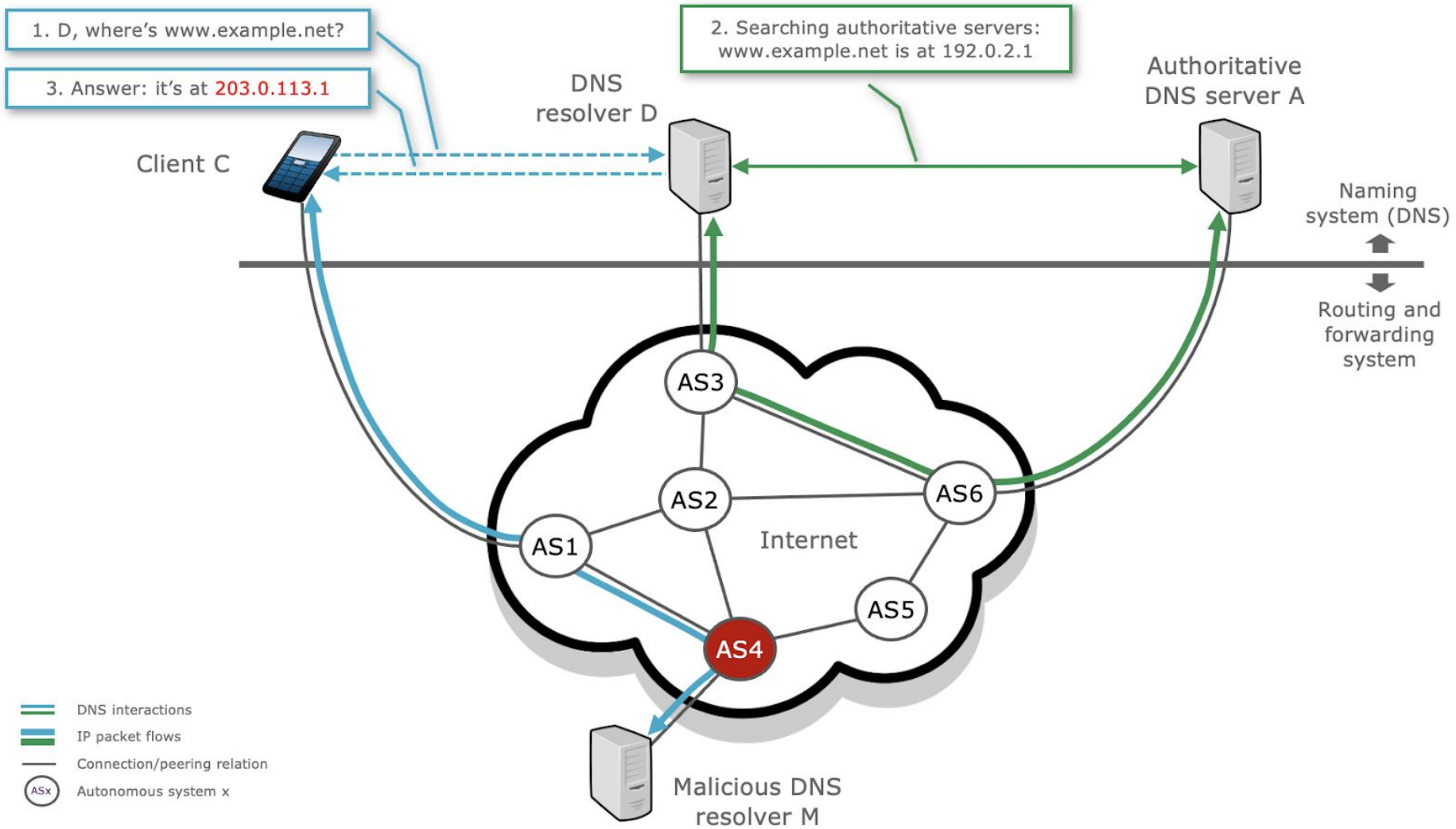


Figure 2: Hypothetical Route Hijack affecting the DNS

Routing Incident: MyEtherWallet / Route53

MyEtherWallet (myetherwallet.com) was attacked by unidentified criminals using a BGP hijacking attack

Attackers injected more specific routes for Amazon's Route53 DNS service

Attackers pretended to be the Route53 authoritative DNS servers

Their servers returned SERVFAIL for all queries, except those for MyEtherWallet

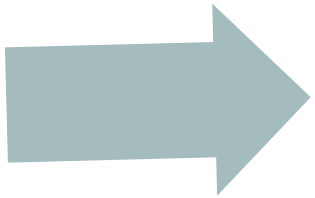
Attackers stole about $150,000 in Ethereum in ~2 hours

For ~2 hours all DNS zones hosted at Route53 were effectively broken

The Relevance of Routing Security for the DNS

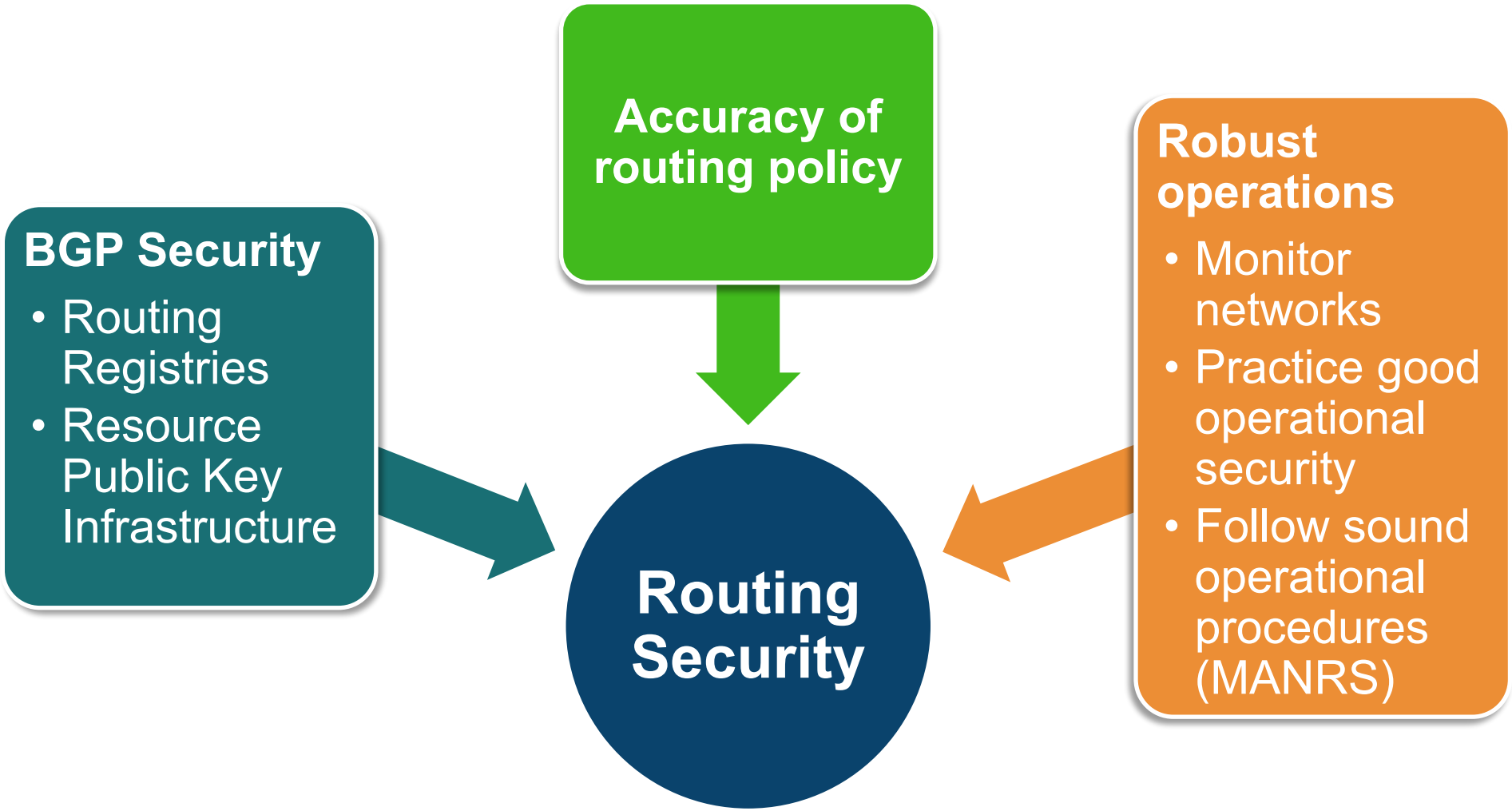
The DNS protocol and DNS resolution are susceptible to routing incidents

- Many authoritative DNS servers answer any query they receive
- Many DNS clients do not authenticate the identity of the server that provides the answer, and do not perform DNSSEC validation
- Stub resolvers have no visibility into which authoritative servers provide answers to queries
- Vast majority of DNS queries are in the clear and use UDP as the transport protocol



- A routing attack can substitute one DNS server for another without the awareness of the client
- Routing attacks can alter the network path of a query, allowing third parties to inspect DNS queries or otherwise eavesdrop on transactions.

Efforts to Enhance Routing Security



BGP Security: Routing Registries

Network operators can register their autonomous systems and the prefixes they originate in a routing registry.

Highlights

- Allows other operators to see what prefixes and routes a given AS should be announcing
- Most useful when carefully and continuously managed for consistency, coverage, and accuracy

Limitations

- When routing registries take on too broad of a scope or are not actively managed their consistency and utility falls.
- The contents of different routing registries may not be mutually consistent and there is no clear way to resolve conflicts between them.

BGP Security: Resource Public Key Infrastructure (RPKI)

Resource Public Key Infrastructure (RPKI) is a way for entities with functional control of IP Address prefixes to assert which autonomous systems are permitted to originate those prefixes.

Highlights

- Builds upon routing registries by designating the autonomous systems that are permitted to originate a routing announcement for a prefix
- Provides some protection from common sources of routing incidents
- Discussions on the efficacy of the RPKI are ongoing, but it may soon be required by some regulators

Limitations

- Not a complete solution to routing security
- All participants always need access to all the data
- No notification to relying parties when they need to update their data
- RPKI cannot secure the full path, only couples the origination of prefixes to ASes

Operating Secured Infrastructure

Organizations should practice good operational security and monitor their routes in order to detect anomalies and failures.

Endogenous Monitoring

- Monitoring from within the network being monitored
- Monitor ability to reach other networks
- Most important is connection to upstream provider

Exogenous Monitoring

- Monitoring from outside the network being monitored
- Monitor connectivity from external networks
- Important, but more expensive that endogenous
- Anycast adds additional complexity

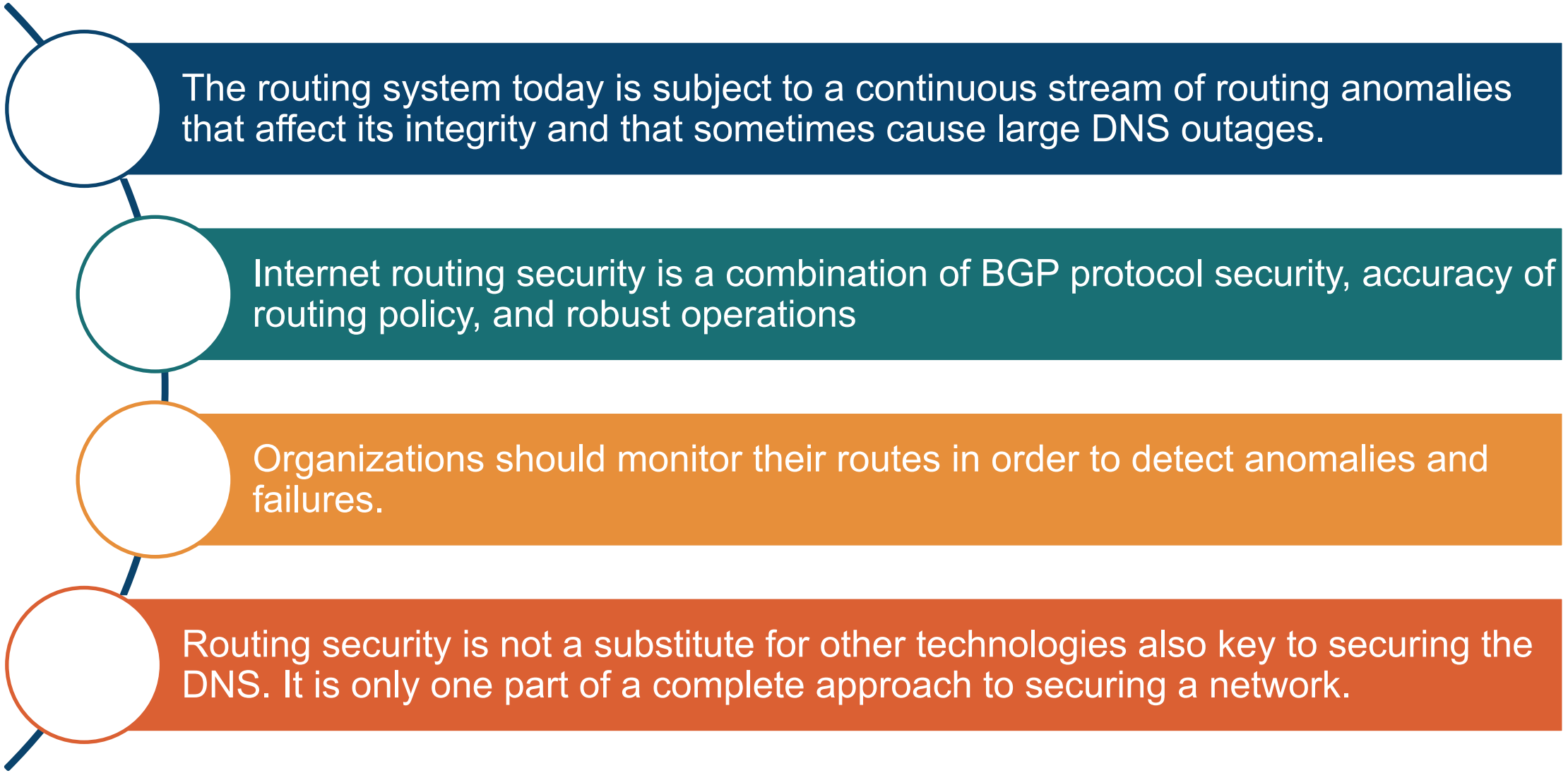
Operator Coordination

- Every org needs access to routing expertise to help remediate issues
- Network operator groups (NOGs) help facilitate relationship building & information sharing

MANRS for Network Operators

- Filtering
- Anti-spoofing
- Coordination
- Global Validation

Key Takeaways



Recent SSAC Publications

SAC120: SSAC Input to GNSO IDN EPDP on Internationalized Domain Name Variants

SAC120: Input to GNSO IDN EPDP on IDN Variants

- An IDN variant is an alternate code point (or sequence of code points) that could be substituted for a code point (or sequence of code points) in a candidate label to create a variant label that is considered the “same” in some measure by a given community of Internet users. There is no general agreement of what that sameness requires.
- In the DNS two variants are distinct domain names. It is users of specific communities that will recognize variants as equivalent.
- To ensure security and stability of IDNs with variants, an IDN and its variants must be treated as a single package from a domain provisioning and life cycle management perspective.
- This report includes an excerpt of relevant IDNs EPDP charter questions, questions asked by the EPDP team, and the SSAC’s response

SAC120: Input to GNSO IDN EPDP on IDN Variants

- A variant management mechanism serves two purposes:
  - Enhance security of IDNs that have variants
  - Promote an acceptable experience that meets the user expectations for those IDNs
- Balancing Security and Usability:
  - IDN and its variants must be treated as a single package from a domain provisioning and life cycle management perspective
  - Variants of an IDN that are in actual use can be delegated.

SAC120: Input to GNSO IDN EPDP on IDN Variants

- Important Limitations:
  - There is no protocol solution in the DNS or other protocols (e.g., HTTP, SMTP, TLS) to enforce equivalence of variant domains.
  - Management of variant domains can introduce a combinatorial explosion for registries, registrars and registrants and need to managed carefully
- These limitations call for a conservative approach in the delegation and management of variant domain names.
- The Root Zone must use the ICANN Root Zone Label Generation Rule to determine variants for all current and future TLDs.

Name Collision Analysis Project

Jim Galvin and Matt Thomas (Co-Chairs)

NCAP Background

- ICANN Board tasked SSAC to conduct studies to present data, analysis and points of view, and provide advice to the Board on name collisions
  - Specific advice regarding .home/.corp/.mail
  - General advice regarding name collisions going forward
- Studies to be conducted in a thorough and inclusive manner that includes other technical experts
  - 25 discussion group members, including 14 SSAC work party members
  - 23 community observers
  - Chaired by James Galvin and Matt Thomas

NCAP - Recent Publications

- Case Study of Collision Strings
  - Studies of .corp, .home, .mail, .internal, .lan, and .local using DNS query data from A and J root servers.
  - Highlight changes over time of the properties of DNS queries and traffic alterations as a result of DNS evolution.
- A Perspective Study of DNS Queries for Nonexistent Top-Level Domains
  - Aims to understand the distribution of DNS name collision traffic throughout the DNS hierarchy
  - Provide insights into where and how DNS data can be collected and assessed.

NCAP - Key Findings so far

- Name collisions are and will continue to be an increasingly difficult problem; case study indicates impact has increased
  - DNS service discovery protocols and suffix search lists are a continuing problem
- Critical diagnostic measurements (CDMs) are defined as a way to measure name collisions by informing the assessment of the risk of delegation
- Any root server identifier is representative of the CDMs seen in the root server system (RSS)
- Mitigation and remediation is problematic, increasingly difficult as the volume and diversity of CDMs increases
- Existing measurement platforms could be extended to help inform applicants

NCAP - Critical Diagnostic Measurements

- Query Volume
- Query Origin Diversity
  - IP address distribution
  - ASN distribution
- Query TYPE Diversity
- Label Diversity
- Other characteristics
  - Open-Source Intelligence (OSINT)

- **Impact (or Harm) is determined by evaluating both Volume and Diversity across all CDMs**

NCAP - Work in Progress

- The NCAP discussion group is developing a framework to assess name collisions
  - How the Board is going to assess name collisions
  - Guidance on how to consider the risks of delegation given the existence of name collisions

- The initial framework, along with findings from other studies, will be published for public comment in 4Q2022

NCAP - How to Participate

- Review the report as soon as it is released for public comment
- Attend or review recording
  - NCAP Discussion Group (19 September 14:30 UTC)
  - NCAP Update (20 September 14:30 UTC)
- Join the discussion group

Updates on SSAC Work Parties

Current Work Parties

- Name Collision Analysis Project
- DS Automation
- Evolution of DNS Resolution
- DNSSEC and Security Workshops (Ongoing)
- Membership Committee (Ongoing)

DS Automation Work Party

- **Goal:** Develop recommendations for automated management of DS records for independent DNS operators
- **Scope:** Investigate the current state of DNSSEC DS RRSet management, including the methods available currently, and to possibly recommend specific methods that may more easily facilitate DS key updating that are not yet generally deployed
- **Deliverable:** An advisory that explains the issues, surveys the possible solutions, and provides recommendations to registries, registrars, and DNS service providers to facilitate the automatic initialization and updating of DS records
- **Intended Audience:** Registry, registrar, and DNS service provider industry

Evolution of DNS Resolution Work Party

- **Goal:** Discuss technologies that are changing the nature of DNS resolution and the implications of these changes on the DNS namespace, provisioners, and operators of DNS infrastructure
- **Scope:** Explore the current state and evolving nature of DNS resolution with a focus on SSR issues related to alternative naming technologies (e.g., blockchain)
- **Deliverable:** An SSAC report that analyzes the effects of relevant new technologies. The report may also suggest methods to measure the implications of these technologies, and possibly propose instrumentation to provide measurements where there may be instrumentation gaps.
- **Intended Audience:** The ICANN community as a whole, including network operators, DNS software implementers, policy makers, and concerned Internet users.

Topics of Interest/Possible New Work

- Examining datasets available from ICANN for use in the investigation of SSR-related issues that fall within SSAC's remit
- Examining practices that can potentially expose registrants to domain name hijacking via lame delegations
- Technical implications of forced removal or transfer of a TLD
- Long-term implications of namespace expansion

SSAC Skills and Potential New Member Outreach

Julie Hammer

SSAC Member Skills

- The skills of SSAC members span the following categories:

Domain Name System	IP Addressing/Routing
Security	Registration Services
Abuse	Internationalized Domain Names
Root Server System	Information Technology
Non-Technical (e.g., legal, risk management, business skills)	

- The SSAC Skills Survey is used to document the skills of all existing and potential SSAC Members

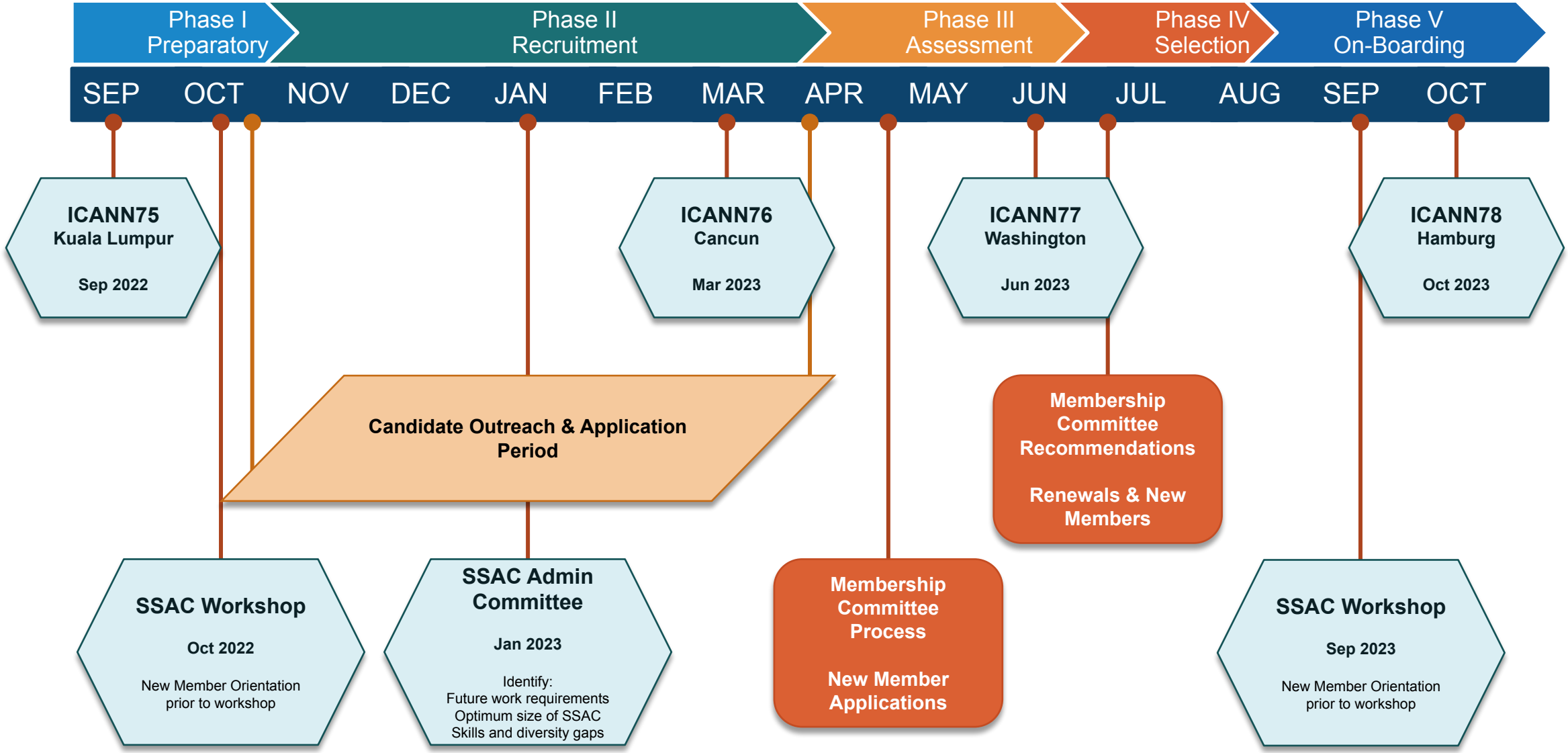
SSAC New Member Outreach

- SSAC is looking for motivated professionals who have skills in the SSAC skills categories and, in particular, expertise or background in:

ISP operations	Large-scale measurement
Large-scale Registrar Operations	Cloud/hosting experience
Browser Development/Testing	Mobile Apps Development/Testing
Low bandwidth resource-constrained Internet connectivity	Red Team experience

- The SSAC is interested in increasing membership from Africa, Latin America, and Asia-Pacific
- The SSAC is interested in increasing membership from an academic background

SSAC Membership Outreach – 2023 Timeline



SSAC Contact for Potential New Members

Individuals who are interested in enquiring about SSAC membership should:

- Contact Rod Rasmussen or Julie Hammer,
- Contact any member of SSAC Support Staff, or
- Send an email to ssac-staff@icann.org

Thank you