



Enhancing DNS Security in Asia: Strengthening Resilience for the Digital Future

ICANN APAC, Istanbul - November 2024

Carrisa Tehputri, BA, MIA
ICANN NextGen

📍 Bali, Indonesia

Background

- AI Consulting, 10a Labs
- Trust and Safety Associate, SAP
- Cybersecurity Consultant, NextPeak

Education

- Master of International Security Policy, SIPA, Columbia University (2023)
- Bachelors of Arts in Public Policy, New York University (2018)

Interest

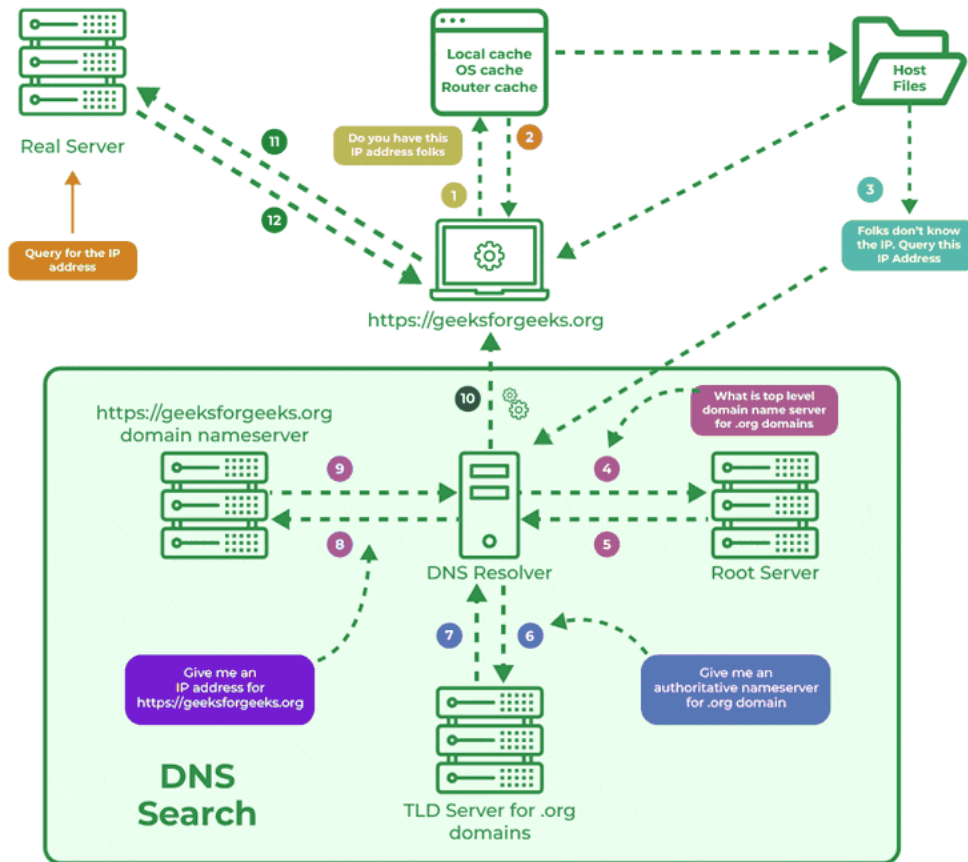
Internet governance, artificial intelligence, technology policy, cybersecurity, public policy, counterterrorism, international law, military AI



Carrisa Tehputri, BA, MIA

Introduction to DNS and DNS Security

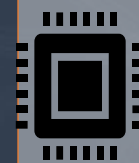
How Does DNS Works



What is DNS? DNS translates domain names into IP addresses to enable internet connectivity.



What is DNS Security? DNS Security ensures the integrity, confidentiality, and availability of DNS data.



Why it Matters: Critical for the functioning of the internet, handling trillions of queries daily.

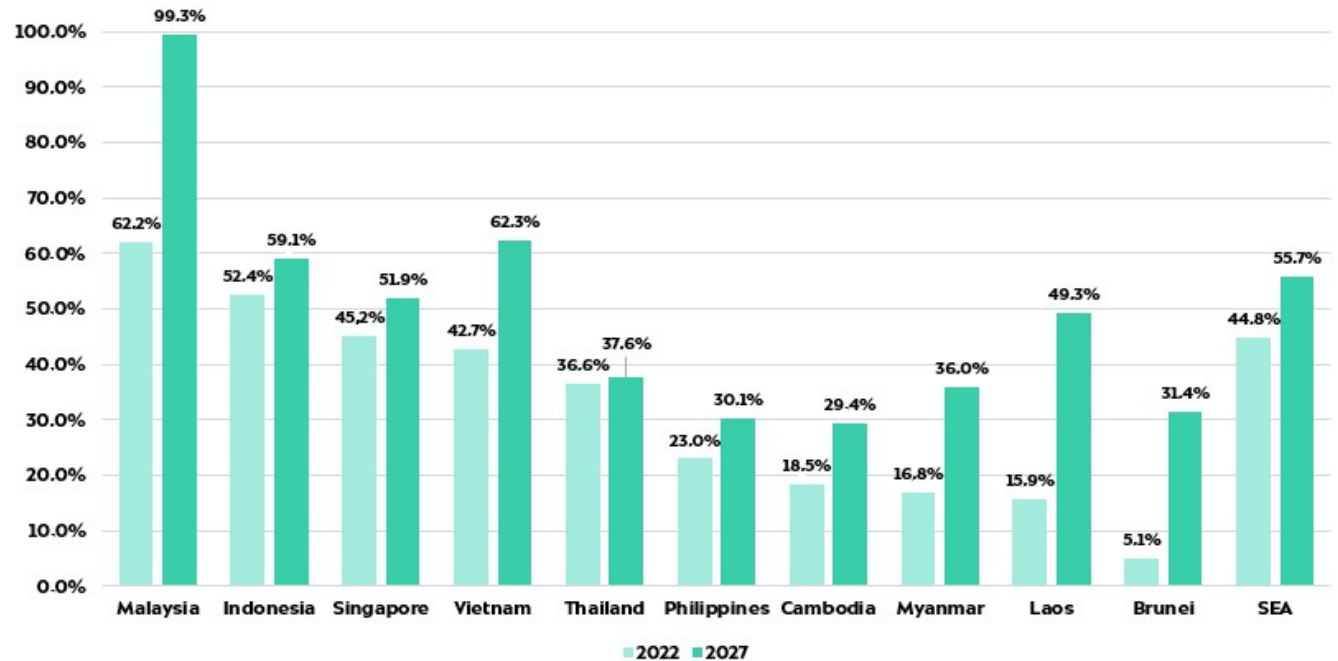
Status Quo of DNS Security in Asia

Current Landscape:

- DNS security adoption varies significantly across the region
- Japan and South Korea lead with modernized infrastructure.
- Countries like Indonesia and Myanmar face vulnerabilities.

SEA Digital Economy as the share of GDP

UNA
FINANCIAL



Growth:

Internet usage and the digital economy are booming in Asia, raising the stakes for securing DNS.

Importance of DNS Security for Asia's Digital Ecosystem

- **Asia is Home to Over 50% of Global Internet Users**
- **DNS-Based Attacks Lead to Major Disruptions:** In 2020, a DNS attack in Malaysia caused significant e-commerce downtime.
- **Uninterrupted Access:** DNS security is vital for ensuring trust and preventing financial losses.

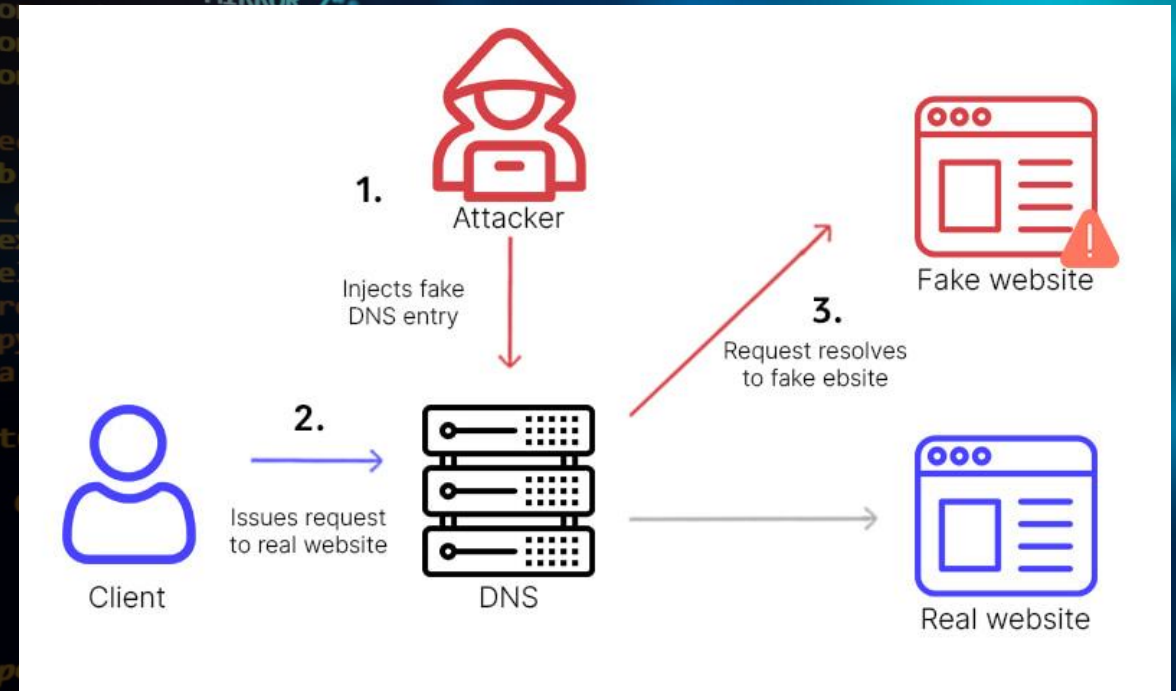
Asia Has the Largest Percentage of Internet

Asia has the largest percentage of Internet users by continent/region.



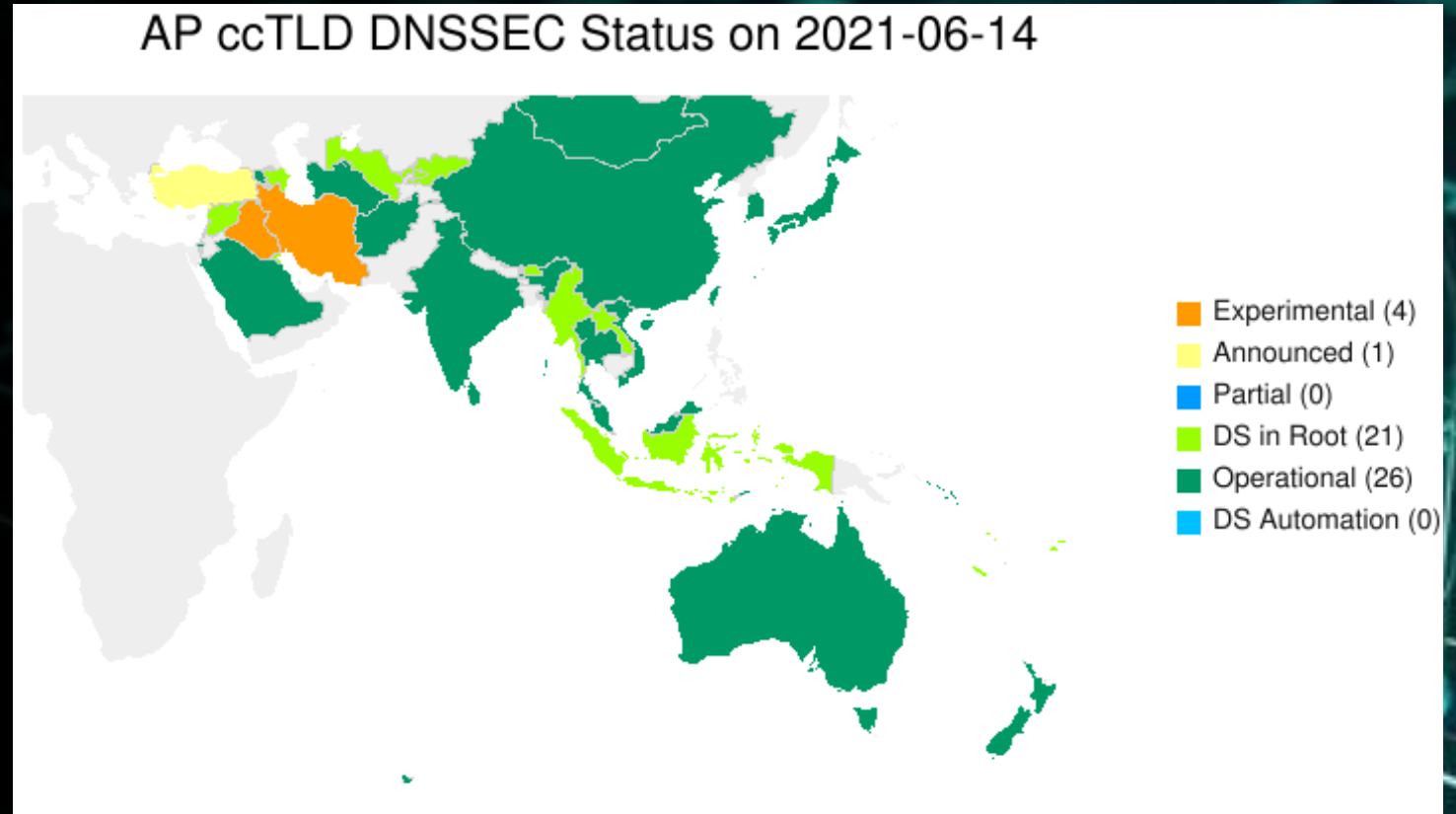
Major DNS Security Challenges

- **DNS Spoofing/Cache Poisoning:** Attackers redirect traffic to malicious websites.
- **DDoS (Distributed Denial of Service):** Overloading DNS servers disrupts internet services.
- **Lack of DNSSEC Adoption:** DNSSEC is not widely implemented, leaving vulnerabilities.
- **Inconsistent Regulations:** Differing levels of regulatory oversight in countries.



Why DNSSEC is Crucial

- **DNSSEC (DNS Security Extensions)**
- **Current Adoption in Asia is Low:** Barriers include awareness, cost concerns, and perceived complexity.
- **Benefits:** Would significantly reduce DNS-based attacks.



ICANN's Role in Enhancing DNS Security

ICANN's Role in Enhancing DNS Security

- ICANN has been actively building DNS security capacity in Asia through workshops, consultations, and partnerships with governments and organizations (e.g., APTLD, DAAR).
- However, more targeted efforts are needed to meet growing digital demands and mitigate evolving threats.



Recommendations for ICANN to Enhance DNS Security in Asia



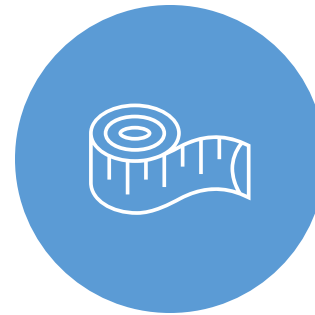
**Expand DNSSEC
Adoption Programs**



**Localized Threat
Intelligence Sharing**



**Collaborate on
Regulatory
Harmonization**



**Scale Capacity-
Building Efforts**

Conclusion

Reinforce	Reinforce the importance of DNS security: It's essential for protecting Asia's digital economy and infrastructure.
Highlight	Highlight DNSSEC adoption as a key solution: It mitigates the risks of DNS-based attacks and provides a foundation for stronger security.
Emphasize	Emphasize the role of ICANN: Through its workshops, partnerships, and technical support, ICANN is pivotal in driving change across the region.
Call	Call to action: Encourage all stakeholders—governments, businesses, and ISPs—to collaborate and take decisive action to strengthen DNS security.