NEXTGEN@ICANN84 PRESENTATION

ICANN'S DNS ABUSE DEFINITION: A CRITICAL REVIEW

AHMAD UMAIR SUHAIDI | 29 OCTOBER 2025 | DUBLIN, IRELAND

ICANN One World, One Internet

UNIVERSITI TENAGA NASIONAL

OBJECTIVES

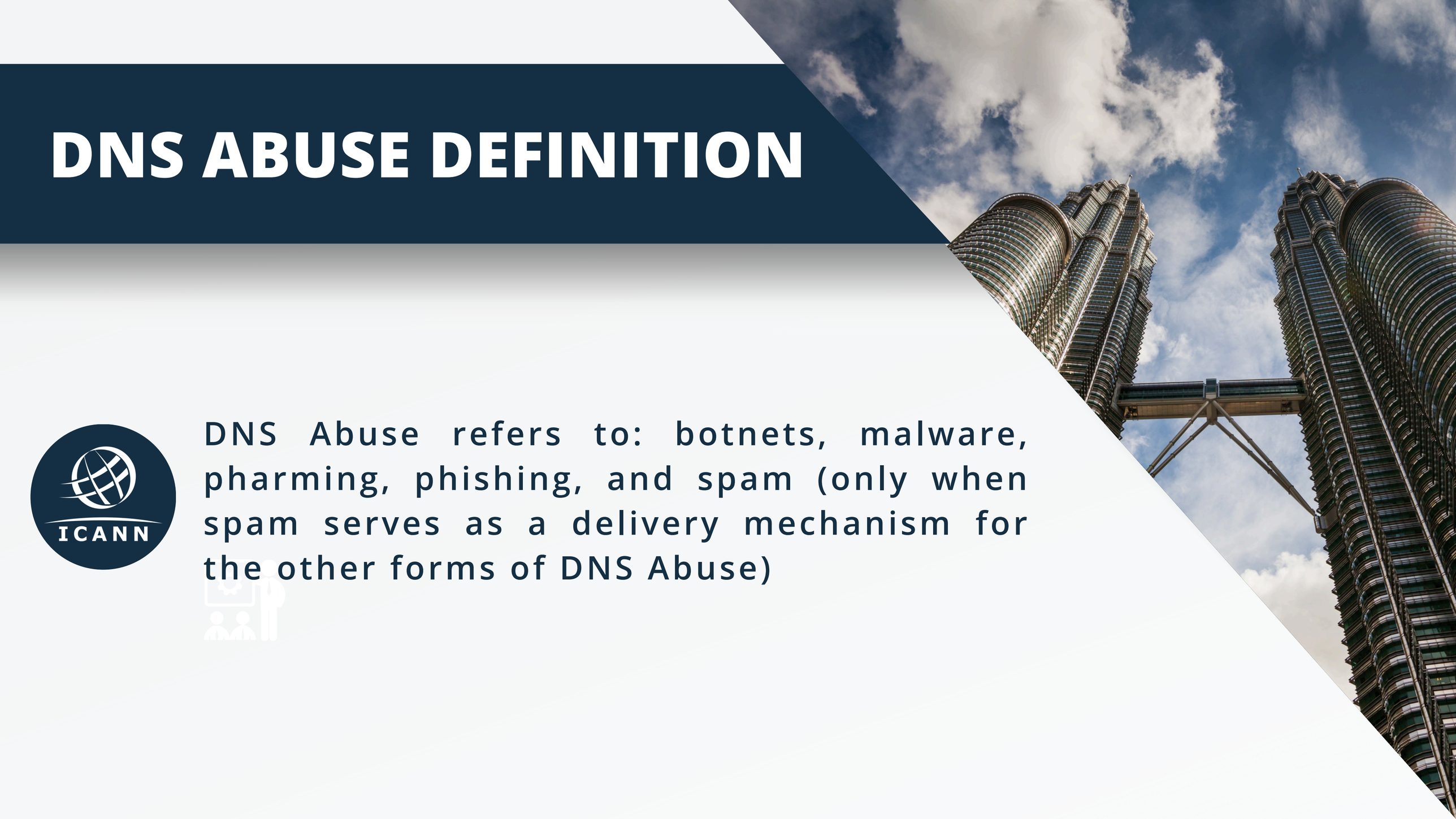
01 Explain and Compare ICANN’S Current DNS Abuse Definition

02 Highlight Key Criticisms to Some of the Elements in ICANN’s Definition

03 Examine Enforcement Realities.

04 Way Forward

DNS ABUSE DEFINITION



DNS Abuse refers to: botnets, malware, pharming, phishing, and spam (only when spam serves as a delivery mechanism for the other forms of DNS Abuse)

OTHER DEFINITIONS

ICANN

Narrow and technical. Focuses only on 5 categories: malware, botnets, phishing, pharming, and spam (only when delivering the others). Excludes content abuse.

MYNIC

Broader.
Defines domain name abuse as any illegal, malicious, or deceptive act tied to domains.
It still includes ICANN's Big-5 but expands into areas that overlap with content-related misuse

INTA

Very broad.
Any use of domains or DNS protocol for deceptive, malicious, or illegal activity.
Explicitly covers content-related abuse.

THE BOUNDARY THAT MATTERS

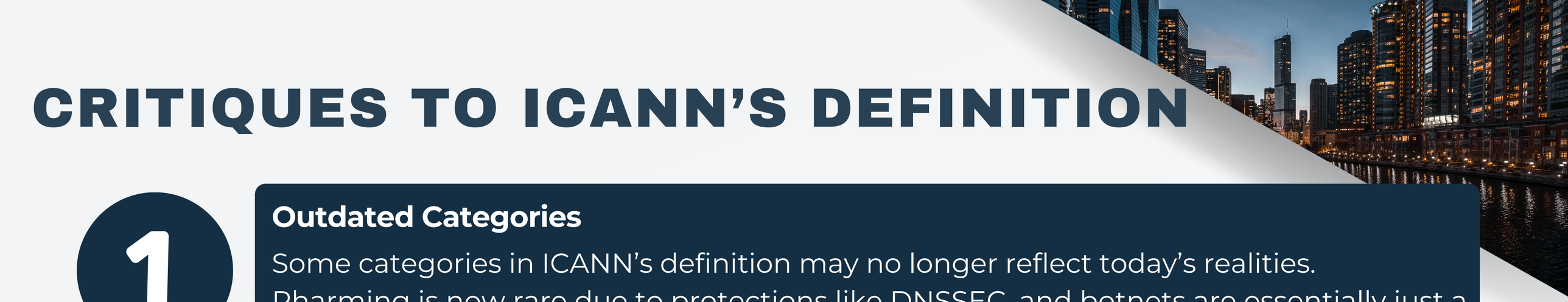
Abuse of the DNS (Technical Abuse)

Direct misuse of the DNS itself, such as phishing domains, malware sites, or botnet. This is within ICANN’s remit.

Abuse by the Means of the DNS (Content Abuse)

Harmful or illegal content hosted on domains, like scams or counterfeit goods. This is outside ICANN’s remit, since ICANN does not regulate content.

CRITIQUES TO ICANN'S DEFINITION



1

Outdated Categories

Some categories in ICANN's definition may no longer reflect today's realities. Pharming is now rare due to protections like DNSSEC, and botnets are essentially just a part of malware. This makes both feel outdated or redundant.

2

Malware and Compromised Sites

Not all malware domains are the same. Some are created by bad actors, but others are normal websites that have been hacked.
Treating both as the same kind of abuse can unfairly punish innocent website owners.

3

Spam and ICANN's Remit

Spam is tricky. ICANN only counts spam as abuse if it delivers other harms like phishing or malware. But deciding this often requires looking at the content of emails, which steps outside ICANN's technical role since ICANN does not regulate content.

ENFORCEMENT REALITIES

Blunt Tools

Registrars can usually only suspend or delete an entire domain. They cannot just remove one harmful page. This creates a risk of collateral damage, especially on shared platforms.

Messy Practice

Enforcement is inconsistent across registrars. Some act quickly, others delay, so abuse often just migrates to “weaker” providers. On top of that, global jurisdiction issues and evasion tactics like fast-flux make enforcement messy.

WAY FORWARD

The path forward is to refine ICANN's DNS Abuse approach while staying true to its technical mission. This means:

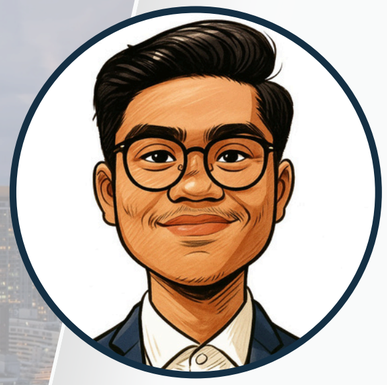
Stay Remit-True

Review Regularly

Differentiate Cases

Trusted Notifier

THANK YOU



Ahmad Umair Suhaidi

UNITEN | ISOC My | Netmission.Asia

linkedin.com/in/umairsuhaidi/

umairsuhaidi@gmail.com

ICANN One World, One Internet

UNIVERSITI TENAGA NASIONAL

REFERENCES

- ICANN. (n.d.). DNS Abuse. Internet Corporation for Assigned Names and Numbers. Retrieved September 28, 2025, from https://www.icann.org/dnsabuse
- MYNIC. (2025, May). Acceptable use & abuse policy. MYNIC Berhad. Retrieved September 28, 2025, from https://mynic.my/storage/pdf/MYNIC_Acceptable_Use_%26_Abuse_Policy.pdf
- International Trademark Association. (2023, May 24). International Trademark Association announces three board resolutions during 2023 Annual Meeting Live in Singapore [Press release]. INTA. Retrieved September 28, 2025, from https://www.inta.org/news-and-press/press-releases/international-trademark-association-announces-three-board-resolutions-during-2023-annual-meeting-live-in-singapore
- Dreyfus, C. (2023, October 17). Domain name abuse: INTA's new definition. Dreyfus Law Firm. Retrieved September 28, 2025, from https://www.dreyfus.fr/en/2023/10/17/domain-name-abuse-intas-new-definition
- Bunton, G. (2021, June 10). A thought experiment: Defining DNS abuse. DNS Abuse Institute (now NetBeacon Institute). Retrieved September 28, 2025, from https://dnsabuseinstitute.org
- Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG). (2023, April). M3AAWG comments on ICANN proposed DNS abuse amendments. Retrieved September 28, 2025, from https://www.m3aawg.org
- Spamhaus. (2022, October 25). DNS abuse: ICANN call for action. The Spamhaus Project. Retrieved September 28, 2025, from https://www.spamhaus.org
- CENTR. (2020, October 27). CENTR report on ICANN 69: DNS abuse discussions. Council of European National Top-Level Domain Registries. Retrieved September 28, 2025, from https://centr.org
- ICANN. (2022, May 17). ICANN org publishes DNS abuse trends: January 2021 – January 2022. Internet Corporation for Assigned Names and Numbers. Retrieved September 28, 2025, from https://www.icann.org/resources/press-material/release-2022-05-17-en
- Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG). (2019, February). M3AAWG best practices for mitigating abuse of compromised websites. Retrieved September 28, 2025, from https://www.m3aawg.org
- Anti-Phishing Working Group (APWG). (2023). Phishing activity trends report 1st quarter 2023. APWG. Retrieved September 28, 2025, from Add a little bit of body text

SPECIAL THANKS

1. Paulo Marcos Drewiacki (NIC.br)
2. Fernanda Iunes (ICANN)
3. Mastura Mukhtar (MYNIC)
4. Dr. Suhaidi Hassan (UUM)
5. Dr. Rohaini Ramli (UNITEN)
6. Mohamad Afiq Ammar Tulos (MCMC)
7. Alban Kwan (CSC)