Security Update

Presenter

Yurie Ito – Director Global Security Programs

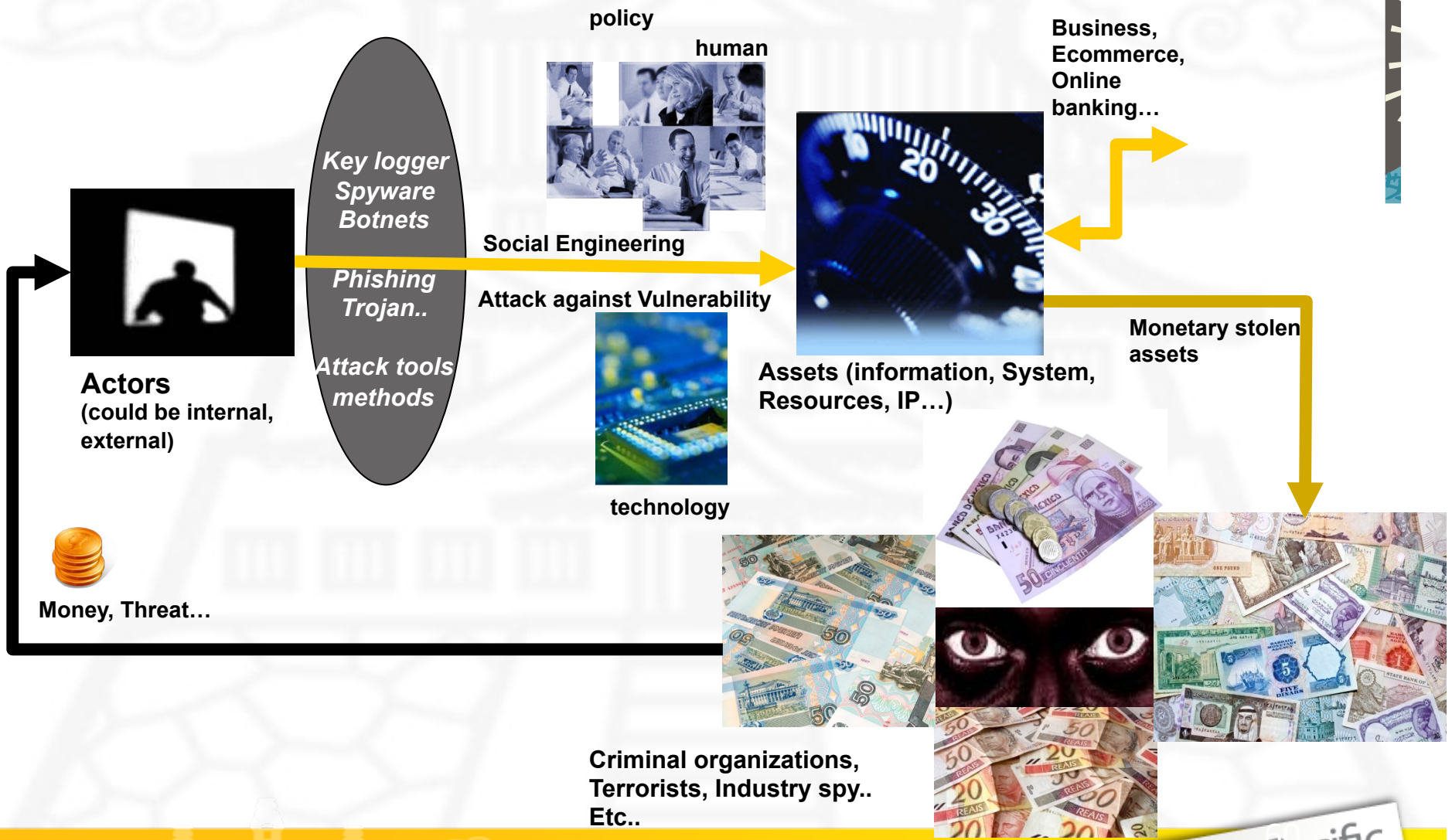
Making the Internet DNS More Secure and Resilient: An ICANN Perspective

ICANN TOKYO | 26-27 AUGUST 2010

The Internet as an Ecosystem

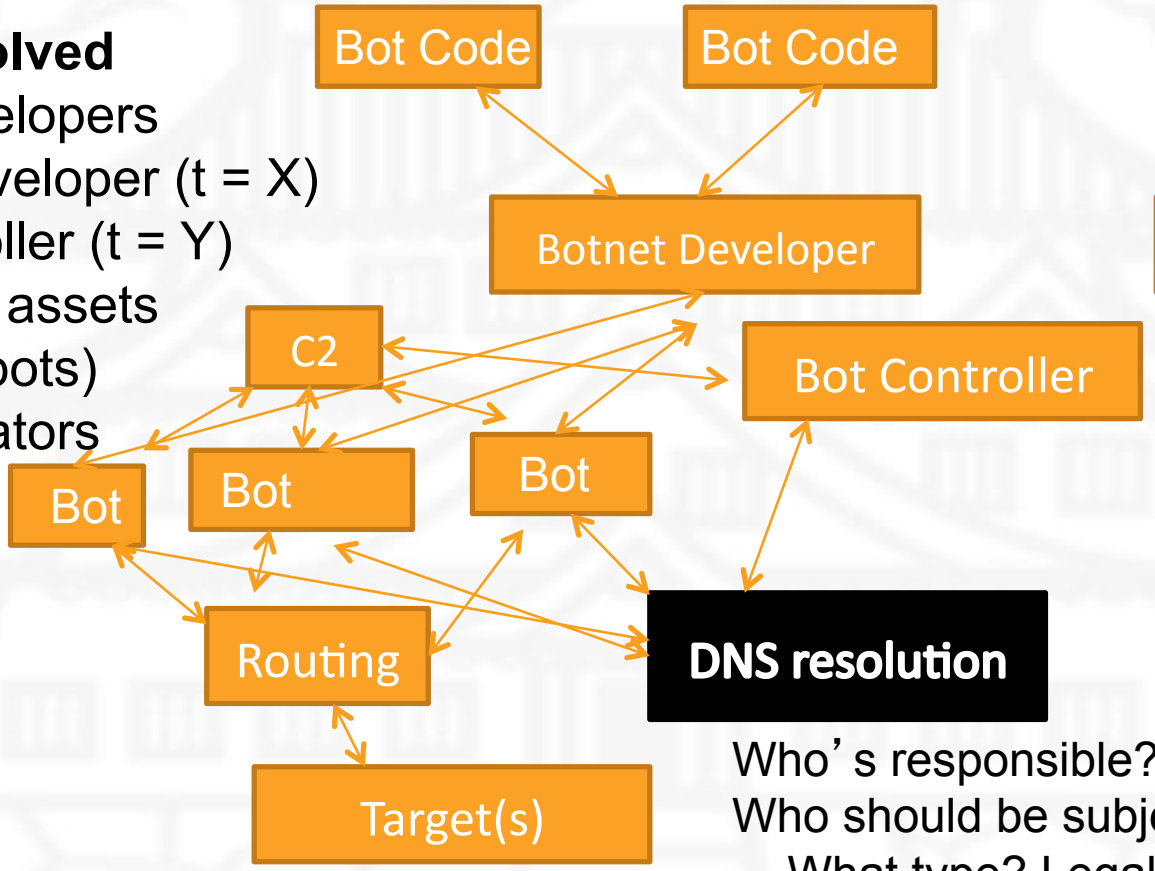
- Built as experiment; now part of everyday life
  - Assumed benign, cooperative users
- Now involves a wide variety of systems, stakeholders, opportunities and risks
  - Governments, corporations, civil society, criminals
- Government regulations are part but not all of the answer to provide resilience in key infrastructures such as DNS.
- Shared responsibility best achieved by involving all important stakeholders is vital.
- Malicious actors now use Internet
  - Growing centers of gravity – militarily, economically, socially
  - Anonymity and ability to leverage 3rd Parties for Bad Acts

Underground Ecosystem



Botnets and Complexity of Attacks

Actors Involved
- Code Developers
- Botnet Developer (t = X)
- Bot Controller (t = Y)
- Owners of assets
  (C2 and bots)
- DNS operators
- ISPs
- Target(s)



Attacker

Multiple purposes; Possibly no digital connection

Who's responsible?
Who should be subject of retaliation?
- What type? Legal notice, arrest, digital disruption?

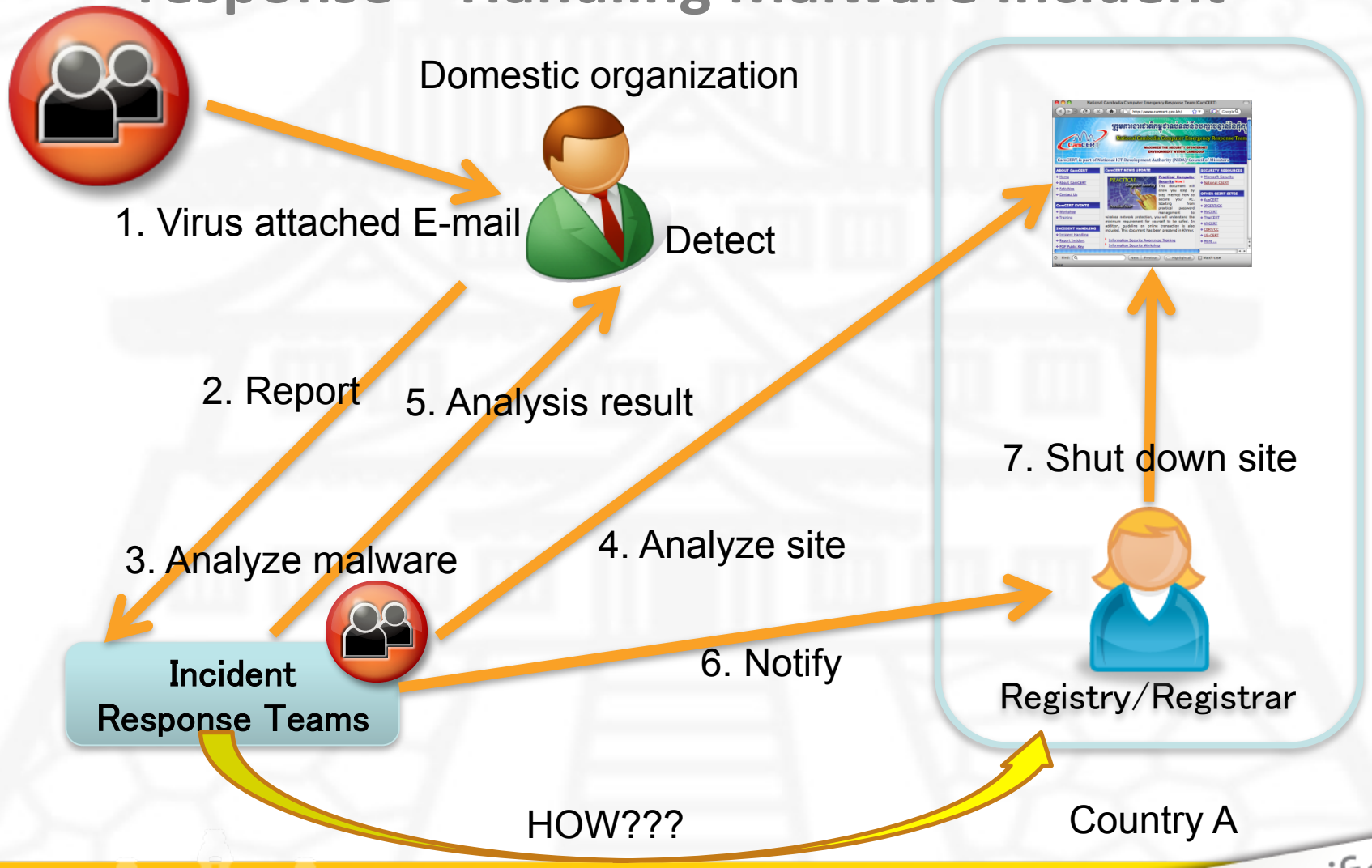
Who should be part of a cooperative mitigation and defense?

Attack the swamps, not the fever

For effective Mitigation and Defense,

International Collaboration
Multi stakeholders Collaboration

Challenge 1 – To identify the contact point for response – Handling Malware Incident



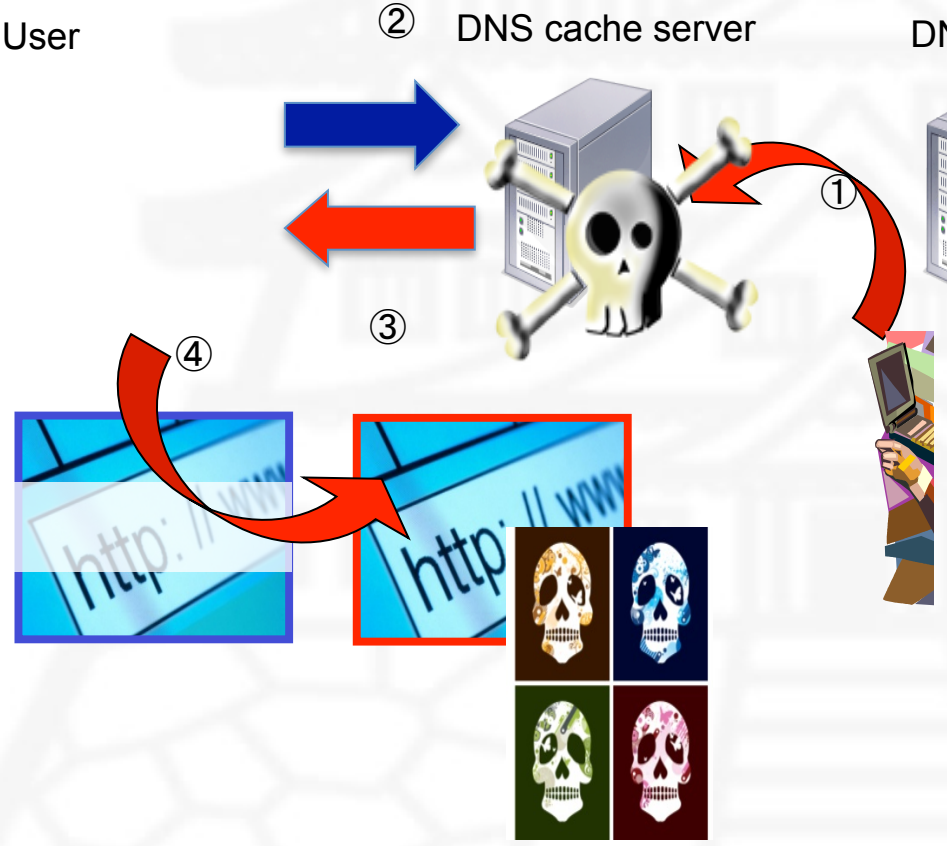
ICANN Roles and Responsibility Related to Security, Stability and Resiliency

- **Bylaws**: To coordinate, overall, the global Internet's system of unique identifiers, and to ensure stable and secure operation of the Internet's unique identifier systems
- **Core**: Ensure DNS system stability and resiliency; enable operator to protect DNS registration and publication process
- **Enabler**: Work the broader Internet and security communities to combat systemic abuse of the unique identifier systems that enable malicious activity.
- **Contributor**: Identification of risks to security, stability and resiliency of the DNS and other identifier systems
- Not involved in content control

www.icann.org/en/security

Identifies the Risks and Minimizes the Risks

DNS vulnerabilities – DNS cache poisoning



Routing hijack
Zone transfer
Non- authoritative spoofing
Distributed Denial of Service
Asymmetric Denial of Service
TXID prediction
Botnet
Key management in DNSSEC
Bad caching policies
DNS rebinding
Lame delegation….

DNS System-wide SSR Coordination, Analysis and Planning

Provide for coherence in concepts of a key subsystem of a larger Internet ecosystem

- Conduct annual DNS SSR symposium
  - 2010' in Kyoto, February focused on Measuring DNS Health
    - Baselined what metrics and measurements exist and where gaps exist in terms of getting more comprehensive
    - Key parameters for DNS health – coherency, integrity, speed, availability, resiliency
      - Report is available – http://icann.org/en/announcements/announcement-26apr10-en.htm
- Developing set of key contingencies for use in ICANN and community efforts related to response and exercise planning
- Finalizing continuity plan for failures of DNS registries to address how to protect registrants

Mitigation of Malicious Conduct in New Top Level Domains

Practical measures for extending the DNS in a more secure and accountable fashion

Ensure applicant evaluation of new gTLD and IDN applicants continues to provide for secure operations

- Requirement for employing key security technology (DNSSEC)
- Prohibition on undermining protocol (Wildcarding)
- Requirements to enhance trust in people (background checks)
- Enable a scalable approach to investigation and response (Zone File Access)
- Proposal is now published
  http://www.icann.org/en/topics/new-gtlds/zone-file-access-en.htm
- A voluntary program for higher trust in key zones (TLD certification program)

DNS Community Collaborative Response

Enabling effective private sector response and leadership

- Working closely with FIRST and national CERT community
  - Joint session in Nairobi; help set up East African CERT
  - DNS Security workshop at FIRST general meeting in June
  - DNS security survey to National CSIRTs
- Working with ccNSO IRPWG
- Continue collaboration in stopping spread of Conficker as well as lessons learned and follow-up efforts
  - Conficker Summary and review is published http://icann.org/en/announcements/announcement-11may10-en.htm
- Continue to have security team incident reporting mechanisms to identify potential systemic DNS incidents
- DNS-CERT business case was discussed at public consultation
  - Workshop report was published
  - Public consultation at Brussels meeting

Capacity Building Programs

Enabling effective security and resilience at the edge of the system

- Continue conduct of ccTLD security and resiliency training program
  - Attack and Contingency Response Program focused on managerial level threat awareness and contingency planning
  - Joint registry operations training program initiated focused on basic, advanced and security DNS technical skill building
- Reaching over 100 DNS ccTLD operators in 41 ccTLDs in the last six months

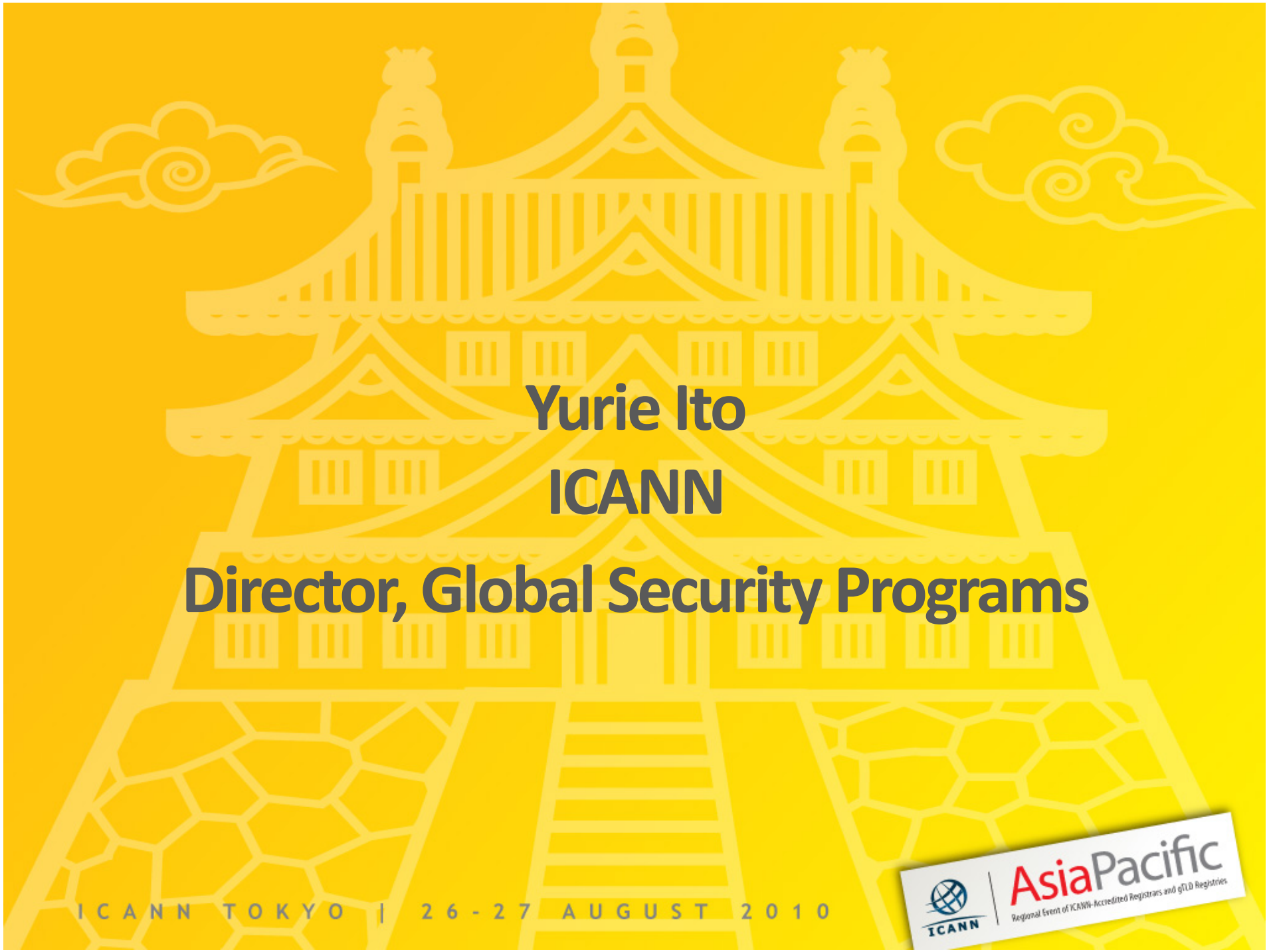
- How can community work more collaboratively to respond threats and risk against DNS?

- What more should we do?

Questions?

- Yurie Ito yurie.ito@icann.org

- Thank you!


Yurie Ito
ICANN
Director, Global Security Programs
ICANN TOKYO | 26-27 AUGUST 2010
ICANN
AsiaPacific
Regional Event of ICANN-Accredited Registrars and gTLD Registries