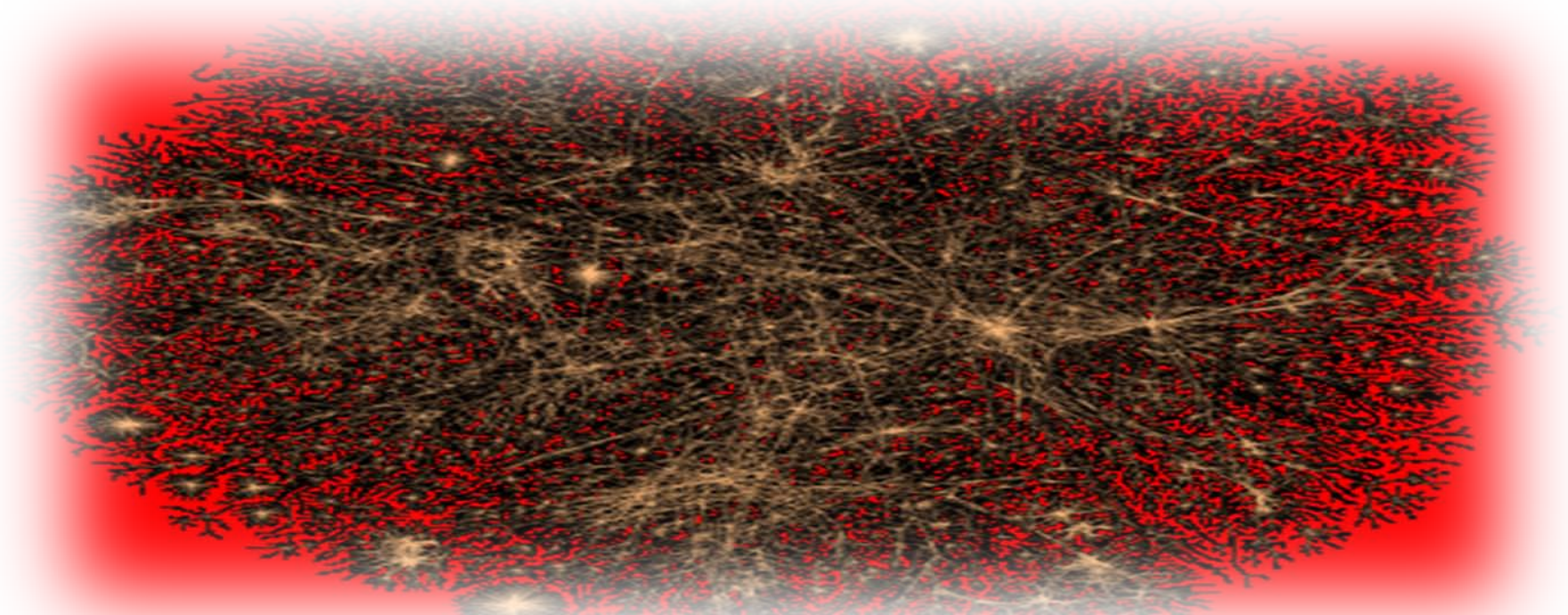


Making the Internet DNS More Secure and Resilient: An ICANN Perspective

Yurie Ito

ICANN, Director Global Security Programs

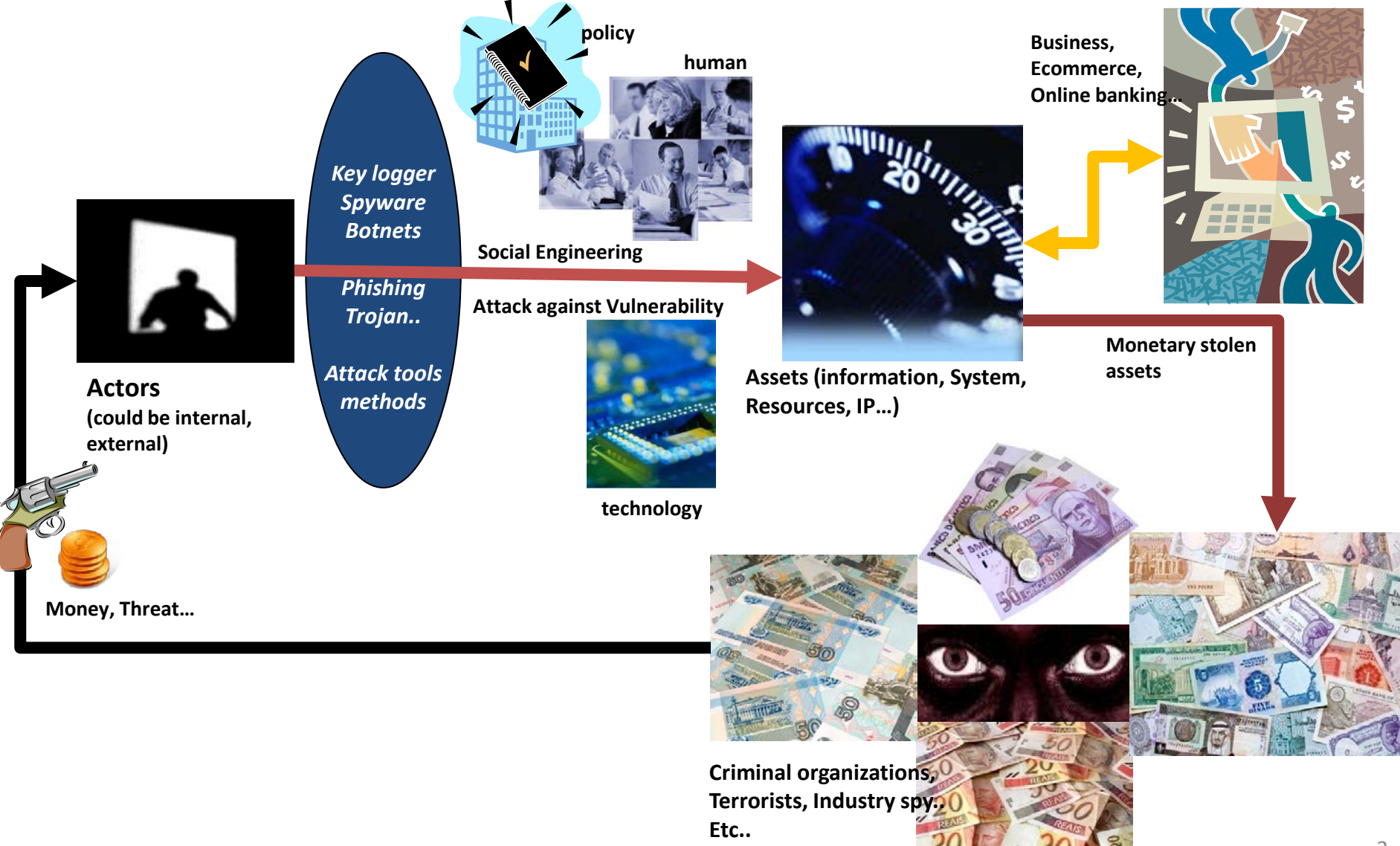


The Internet as an Ecosystem

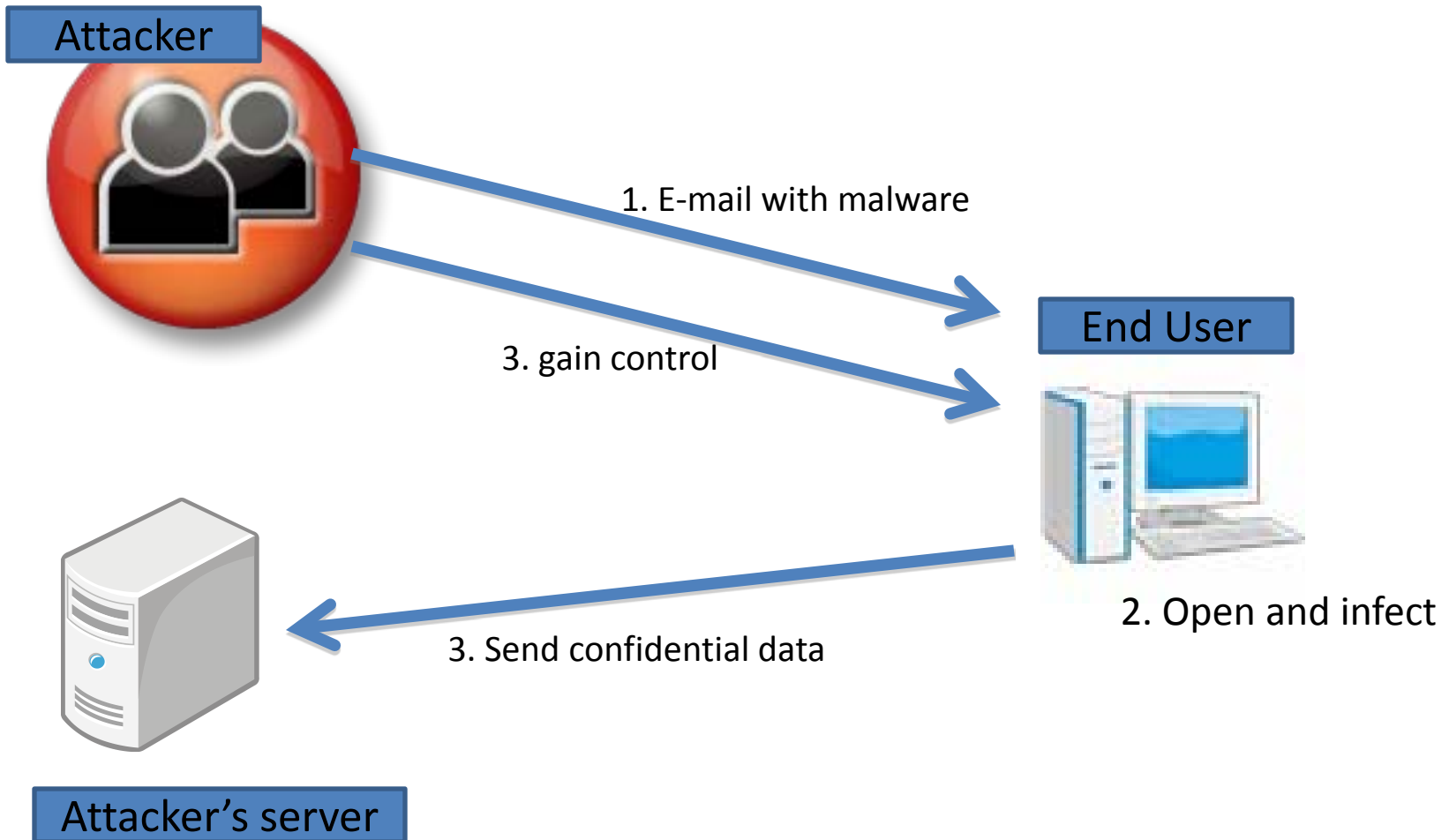
- Built as experiment; now part of everyday life
 - Assumed benign, cooperative users
- Now involves a wide variety of systems, stakeholders, opportunities & risks
 - Governments, corporations, civil society, criminals
- Government regulations are part but not all of answer to provide resilience in key 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 & ability to leverage 3rd Parties for Bad Acts



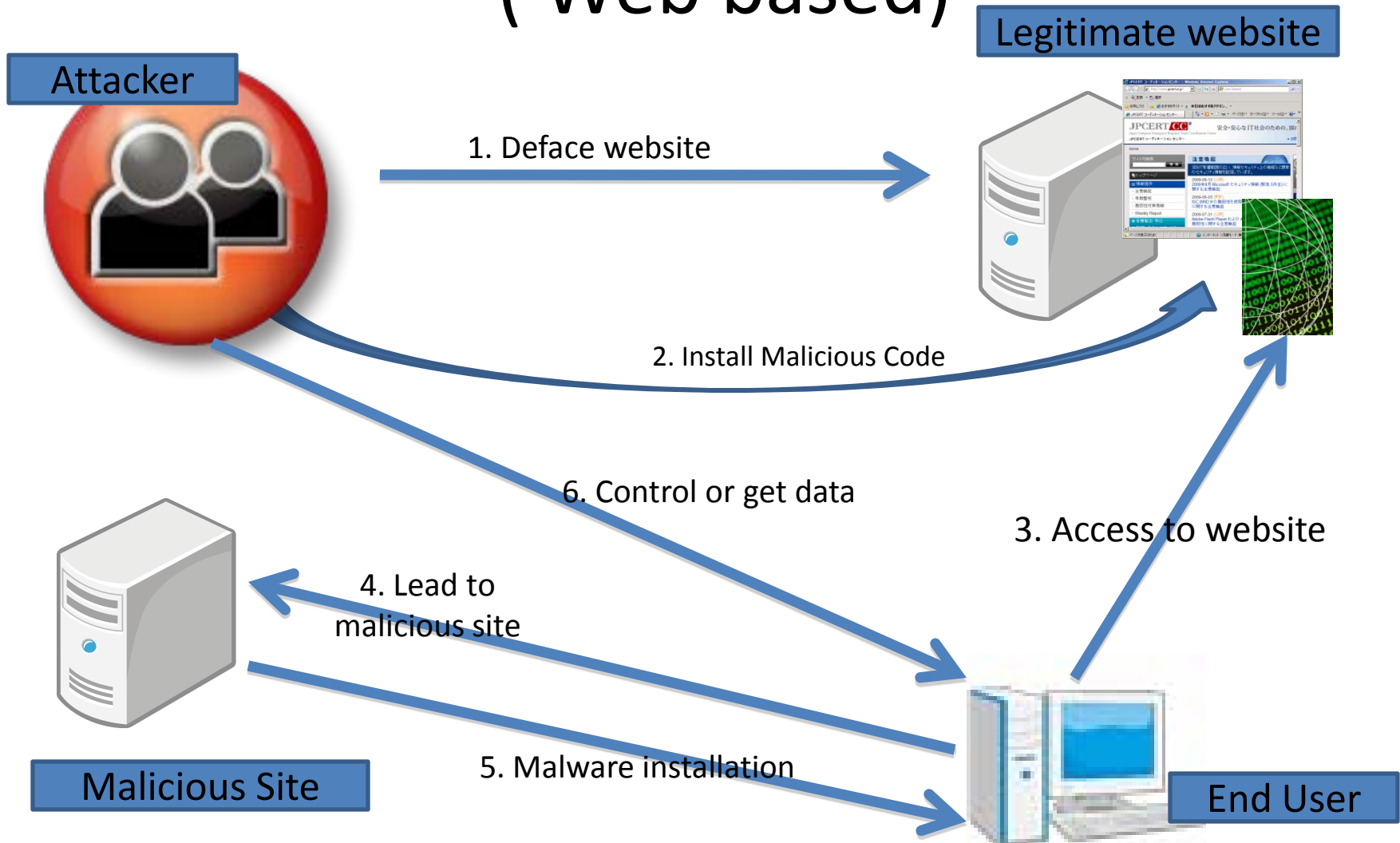
Underground Ecosystem



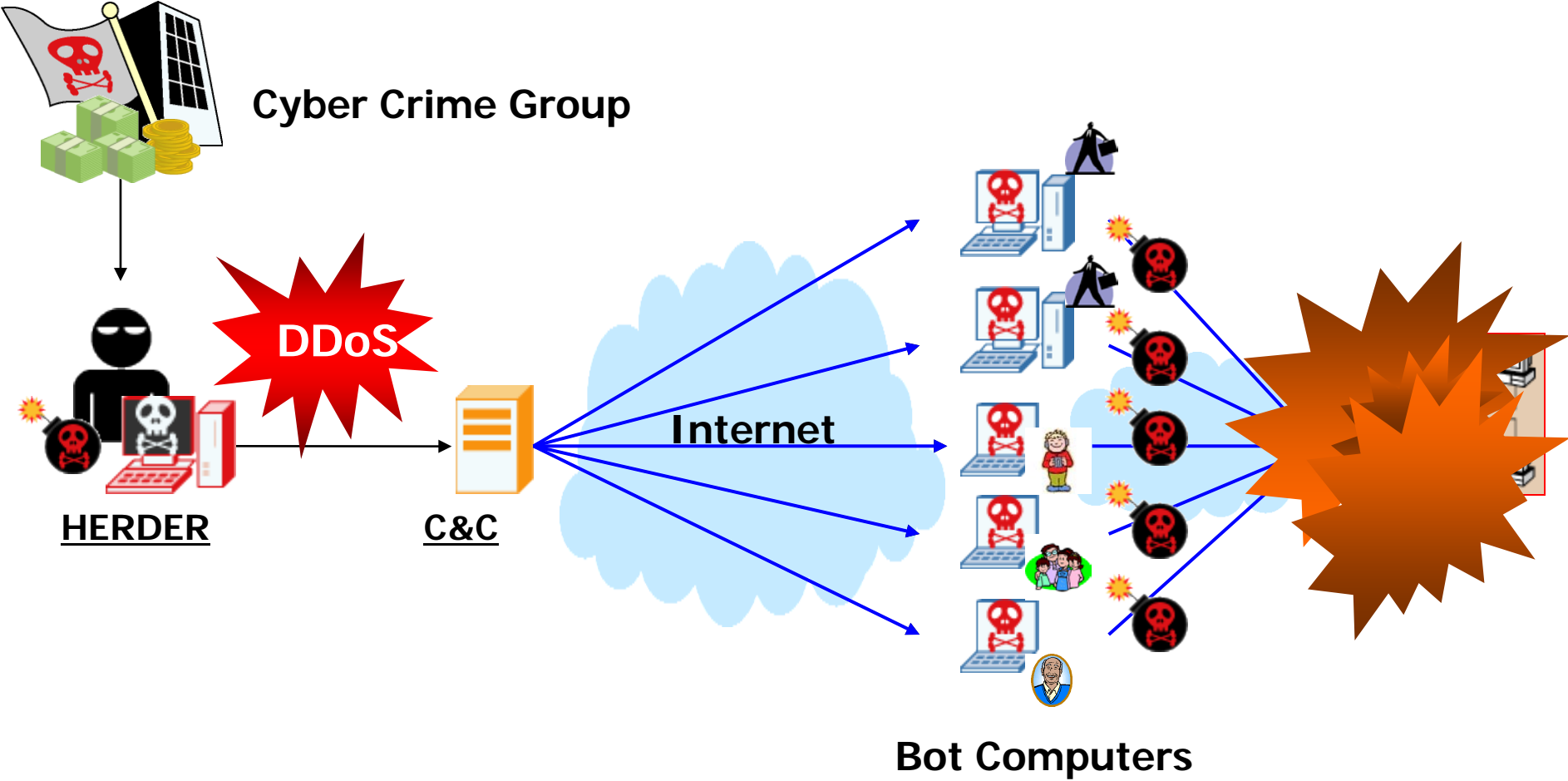
How does Malware compromise PC (Mail based)



How does Malware compromise PC (Web based)



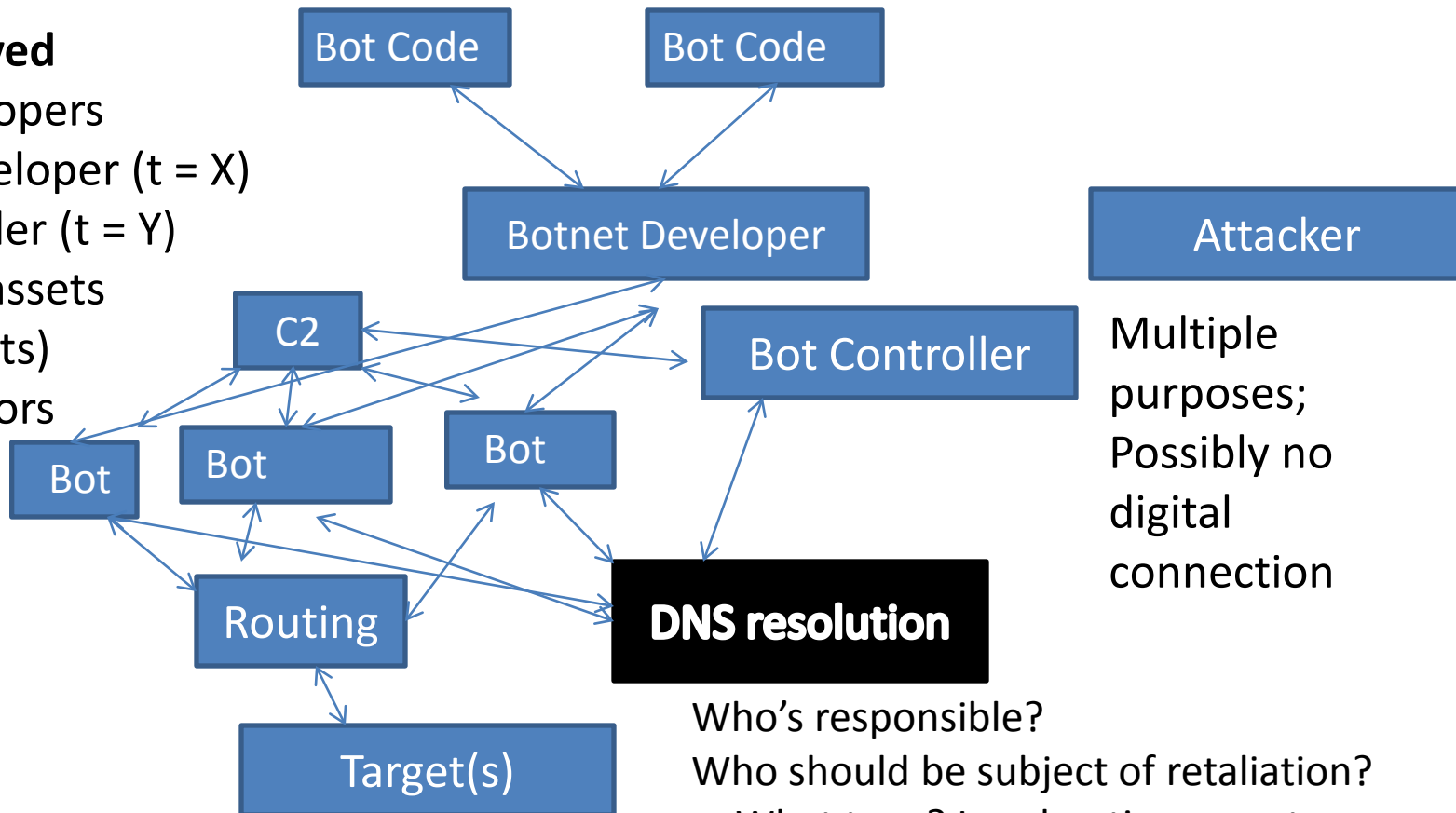
Botnet



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)



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

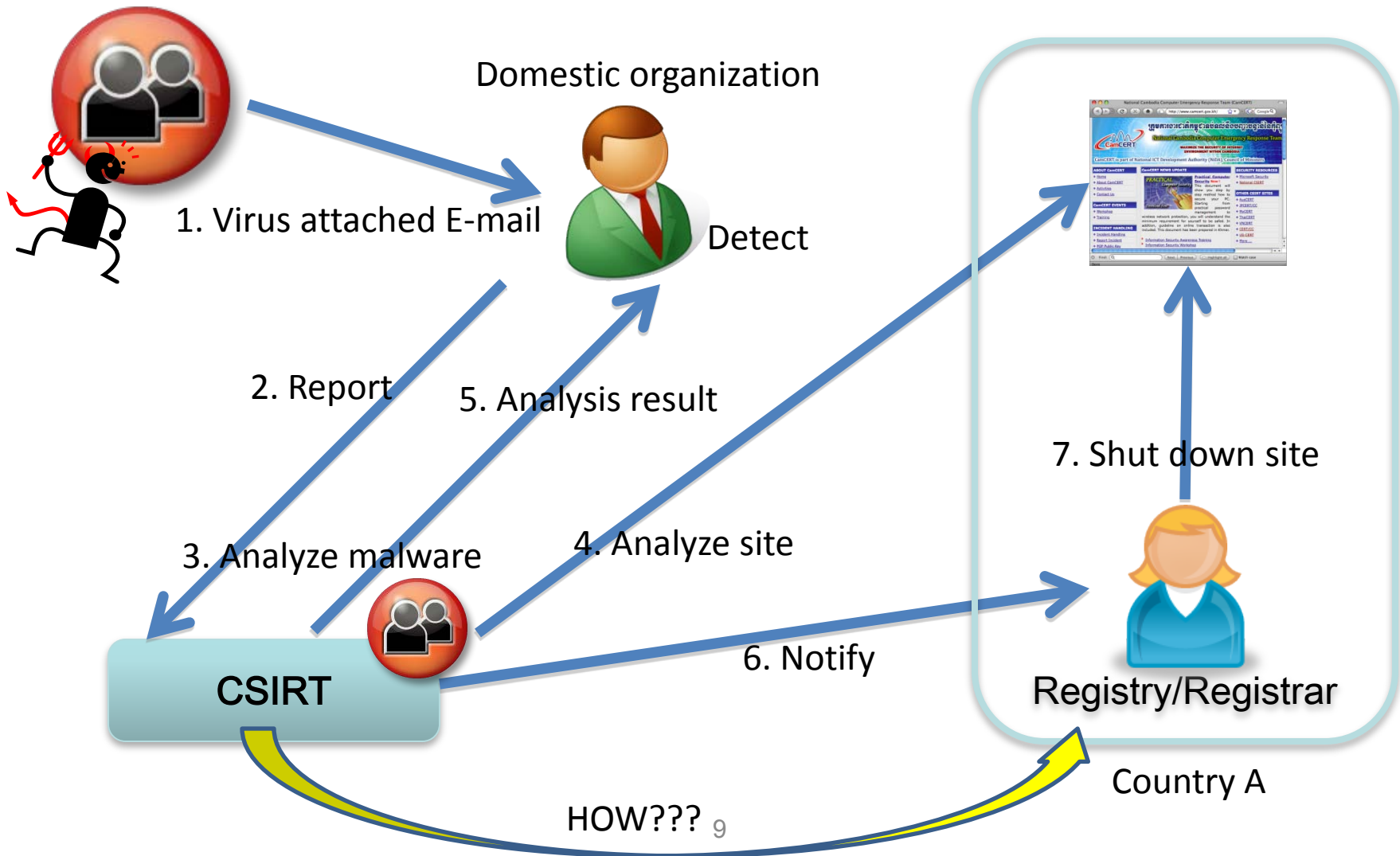
For effective Mitigation and Defense,

International Collaboration !

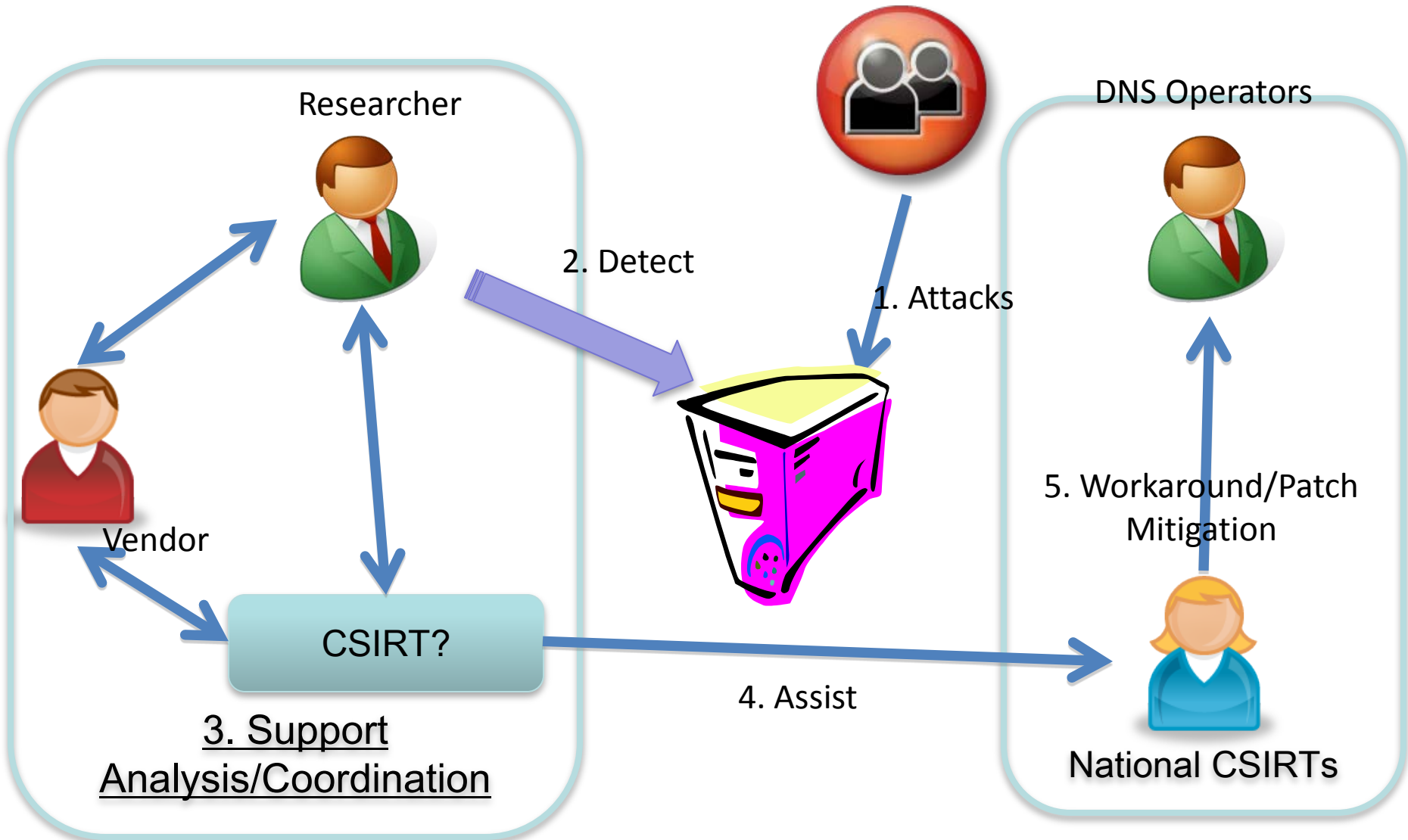
Multi stakeholders Collaboration !

Challenge 1 – To identify the contact point for response

-- Handling Malware Incident



Challenge 2: Access to key DNS expertise resource -- e.g. Vulnerability Handling

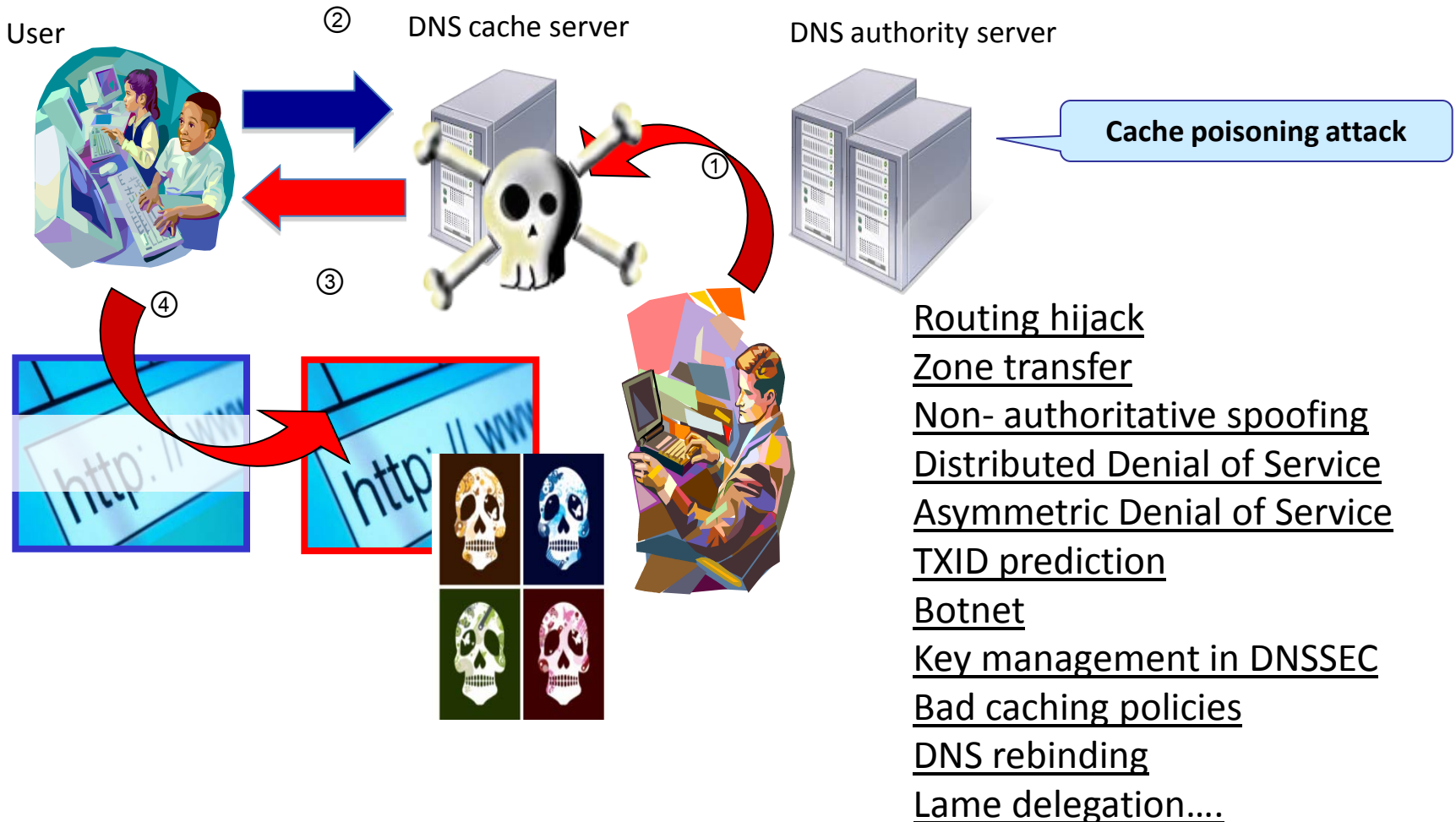


ICANN Roles and Responsibility Related to Security, Stability and Resiliency

- **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

Identifies the threats and Minimize the Risk

DNS vulnerabilities – DNS cache poisoning



DNS System-wide SSR

Coordination, Analysis and Planning

Provide for coherence in concepts of a key sub-system of a larger Internet ecosystem

- Conduct annual DNS SSR symposium. This year in Kyoto in early 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 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
- 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 will be published this week
 - 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!