Enhancing Collaborative Response to Security Challenges Involving the DNS

Yurie Ito

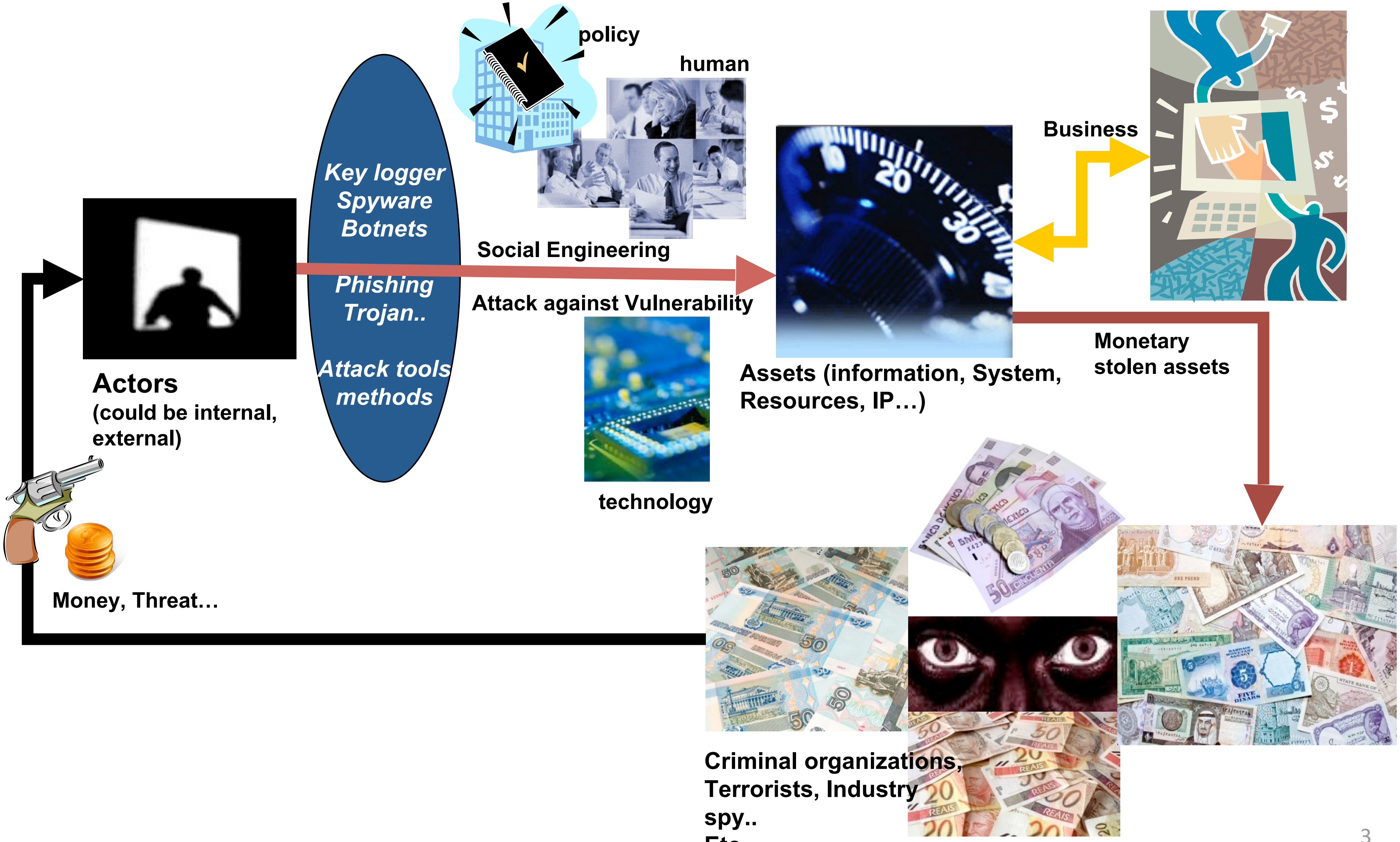
Security Team

Internet Corporation for Assigned Names and Numbers (ICANN)

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
- **Malicious actors now use Internet**
  - Growing centers of gravity – economically, socially, militarily
  - Anonymity & ability to leverage 3rd Parties for Bad Acts
  - Underground economy is developed

Underground Ecosystem



policy

human

Key logger
Spyware
Botnets

Phishing
Trojan..

Attack tools
methods

Social Engineering

Attack against Vulnerability

technology

Business

Actors
(could be internal,
external)

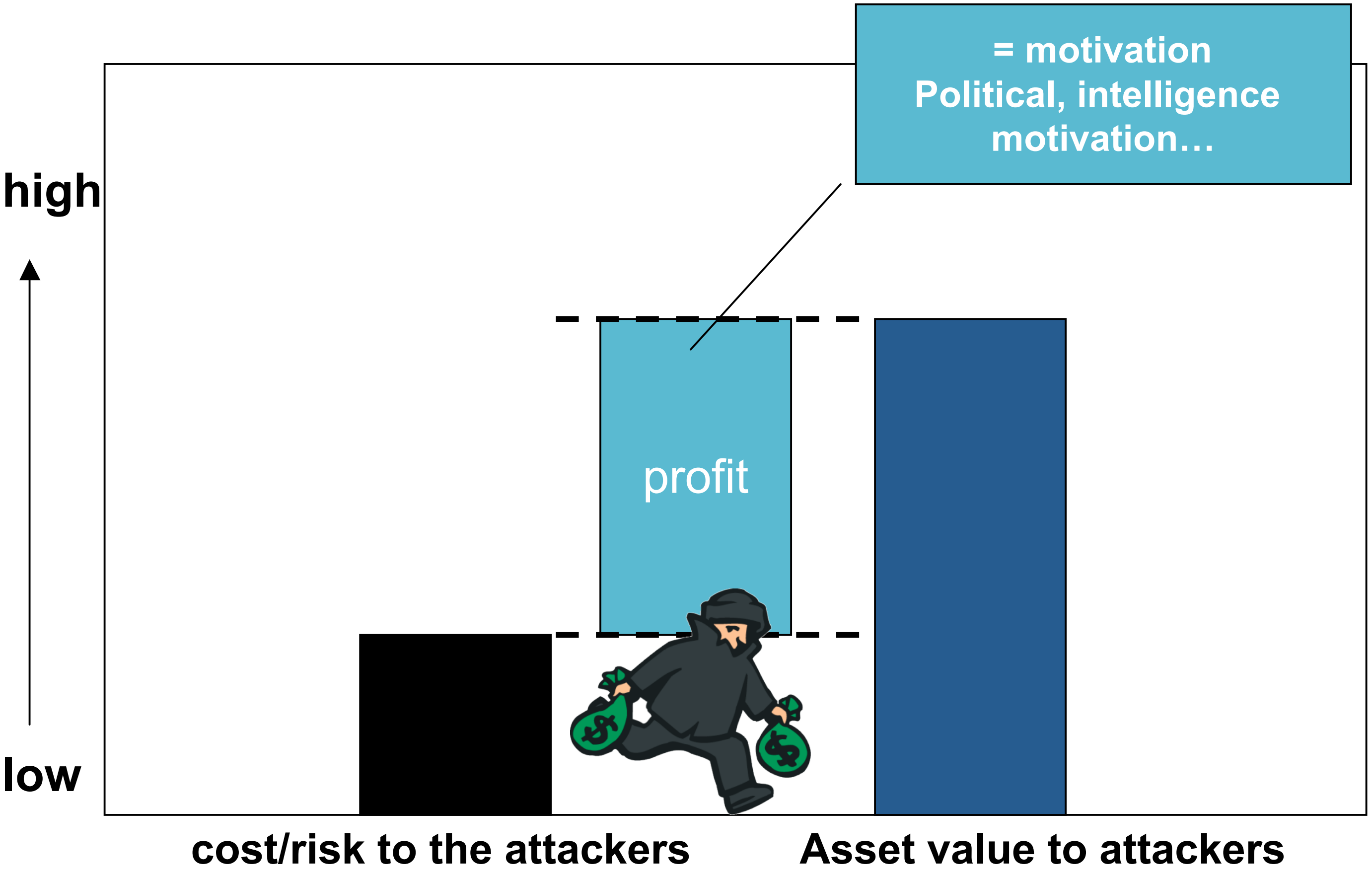
Assets (information, System,
Resources, IP…)

Monetary
stolen assets

Money, Threat…

Criminal organizations,
Terrorists, Industry
spy..
Etc..

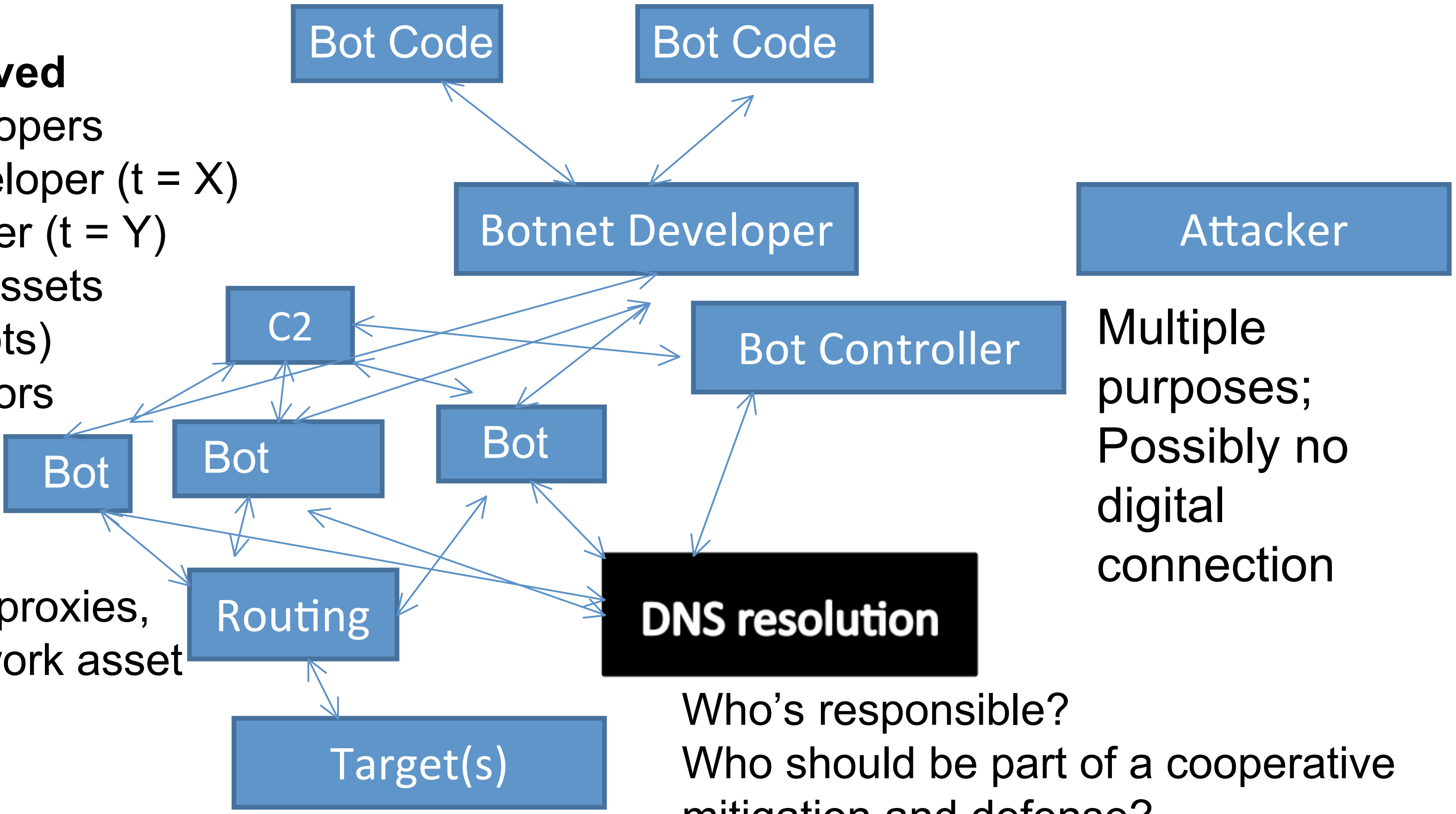
Risk and cost to the attackers vs. Asset value in cyber space



Bot Nets 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)

(to include firewall, IDS, proxies, targeted network asset



Multiple purposes; Possibly no digital connection

Who's responsible?
Who should be part of a cooperative mitigation and defense?
Who should be in a investigation/legal enforcement?

Attack the swamps, not the fever

What is ICANN?

- International, public benefit, non-profit organization managing the Internet unique identifier systems, including the DNS
  - Includes a range of supporting organizations and advisory committees
- Ensuring “Security and Stability” of those systems is a core mission

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**
- Enabler: Work with broader Internet and security communities to **combat systemic DNS abuse**; assist operators to protect DNS registration and publication process
- Contributor: Identification of **risks** to security, stability and resiliency of the DNS as **part of larger cybersecurity** challenges
- **Not involved** in cyber war/espionage or content control

Board approved ICANN Plan for Enhancing Internet Security, Stability and Resiliency
SSR Plan : http://www.icann.org/en/announcements/announcement-2-21may09-en.htm

JPA, Affirmation of Commitments & Security, Stability and Resiliency

- Affirmation replaces JPA as of 1 October; no end date
  - DOC and ICANN make commitments on a number of fronts
- "Preserving security, stability and resiliency" one of four major joint commitments
- Section 9.2 details specific responsibilities
  - Have a DNS SSR plan and update regularly – will do annually
  - Community review every 3 years; first one in a year
  - Focus areas:
    - security, stability and resiliency matters, both physical and network, relating to DNS
    - ensuring appropriate contingency planning;
    - maintaining clear processes

ICANN Security Staff

- Greg Rattray: Chief Internet Security Advisor
- John Crain: Senior Director of SSR
- Geoff Bickers: Director of Security Operations
- Yurie Ito: Director, Global Security Programs

Key Initiative: Internet Assigned Numbers Authority (IANA) Operations

- Supporting the implementation of DNS Security Extensions (DNSSec)
  - Working with USG/VeriSign to sign root by end of yr
- Initiate improving root zone management through automation
- Improve authentication of communication with TLD managers

Key Initiative: DNS Root Server Operations

- Continuing to seek mutual recognition of roles and responsibilities and initiate a voluntary effort to conduct contingency planning and exercises
- Secure, resilient L-root operation

Key Initiative: Collaboration with TLD Registries and Registrars

- Establishing New gTLDs and IDNs: Ensure establishment of new gTLD and IDN applicants provide for stable operations & enhanced security controls
- gTLD Registries:
  - Mature the gTLD registry continuity plan and test the data escrow system
  - Establish expedited security request and response system
- ccTLD Registries:
  - Mature the joint Attack and Contingency Response Planning (ACRP) program that has been established with the regional TLD associations
  - Facilitate the ccTLD working group on incident response
- Registrars: Enhance registrar accreditation and data escrow requirements

Key Initiative: ccTLD Security and Resiliency Capacity Building Initiative

- Partnered with ccTLD regional organizations to provide training/exercise events to develop capacity
  - Managerial-level Attack and Crises Response Planning course – process & best practice
  - Technical-level hands-on defense techniques in simulated threat environment
  - Workshop to establish exercise programs
- Multiple events planned for Spring 09/Summer 09
  - Exercise Training Workshops Jordan, Seoul
  - Technical Training w/ LACTLD Association in Santiago (Sep)

Looking to leverage lessons and partners

Key Initiative: contractual compliance

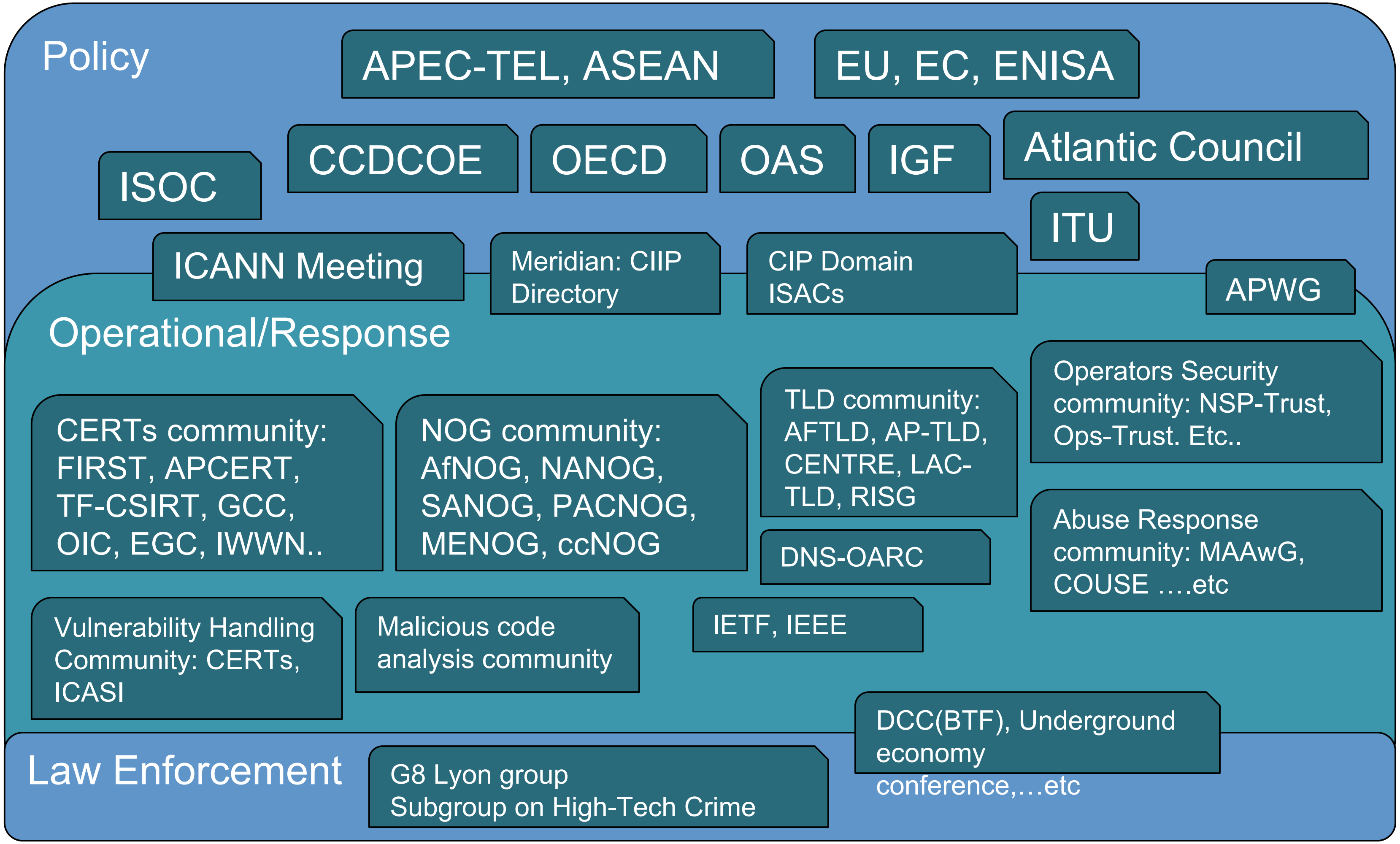
- Contractual Compliance
  - continue to enhance the scope of contractual enforcement activities involving gTLDs
  - initiating audits of contracted parties as part of implementing the March 09 amendments to Registrar Accreditation Agreement (RAA)
  - identify potential involvement of contracted parties in malicious activity for compliance action.

Key Initiatives: Ensure Global Engagement and Cooperation

- Enhance partnerships to include the Internet Engineering Task Force (IETF), Internet Society (ISOC), regional internet registries and network operators groups, the DNS Operations, Analysis and Response Center (DNS-OARC), and global incident response community such as Forum of incident response security Teams (FIRST).

- Engage in global dialogues to foster understanding of the security, stability, and resiliency challenges that face the Internet ecosystem and how to engage these challenges with multi-stakeholder approaches

Global Cyber Security Community



Policy

APEC-TEL, ASEAN

EU, EC, ENISA

ISOC

CCDCOE

OECD

OAS

IGF

Atlantic Council

ITU

ICANN Meeting

Meridian: CIIP Directory

CIP Domain ISACs

APWG

Operational/Response

CERTs community: FIRST, APCERT, TF-CSIRT, GCC, OIC, EGC, IWWN..

NOG community: AfNOG, NANOG, SANOG, PACNOG, MENOG, ccNOG

TLD community: AFTLD, AP-TLD, CENTRE, LAC-TLD, RISG

Operators Security community: NSP-Trust, Ops-Trust. Etc..

DNS-OARC

Abuse Response community: MAAwG, COUSE ….etc

Vulnerability Handling Community: CERTs, ICASI

Malicious code analysis community

IETF, IEEE

DCC(BTF), Underground economy conference,…etc

Law Enforcement

G8 Lyon group Subgroup on High-Tech Crime

Global DNS SSR Symposium

- Co-Hosted with Georgia Tech, George Mason University, DNS OARC: Over 90 participants - technologists, academia, operators, security experts, vendors
- Major themes
  - Combating malicious abuse of the DNS
  - Enterprise DNS risk and remediation
  - DNS security in resource constrained environments

Initial findings

- Need for improved collaborative response
- Need for training across all sectors of the industry to raise both skills and awareness

- Other findings are available in the symposium report at
  - http://www.gtisc.gatech.edu/icann09

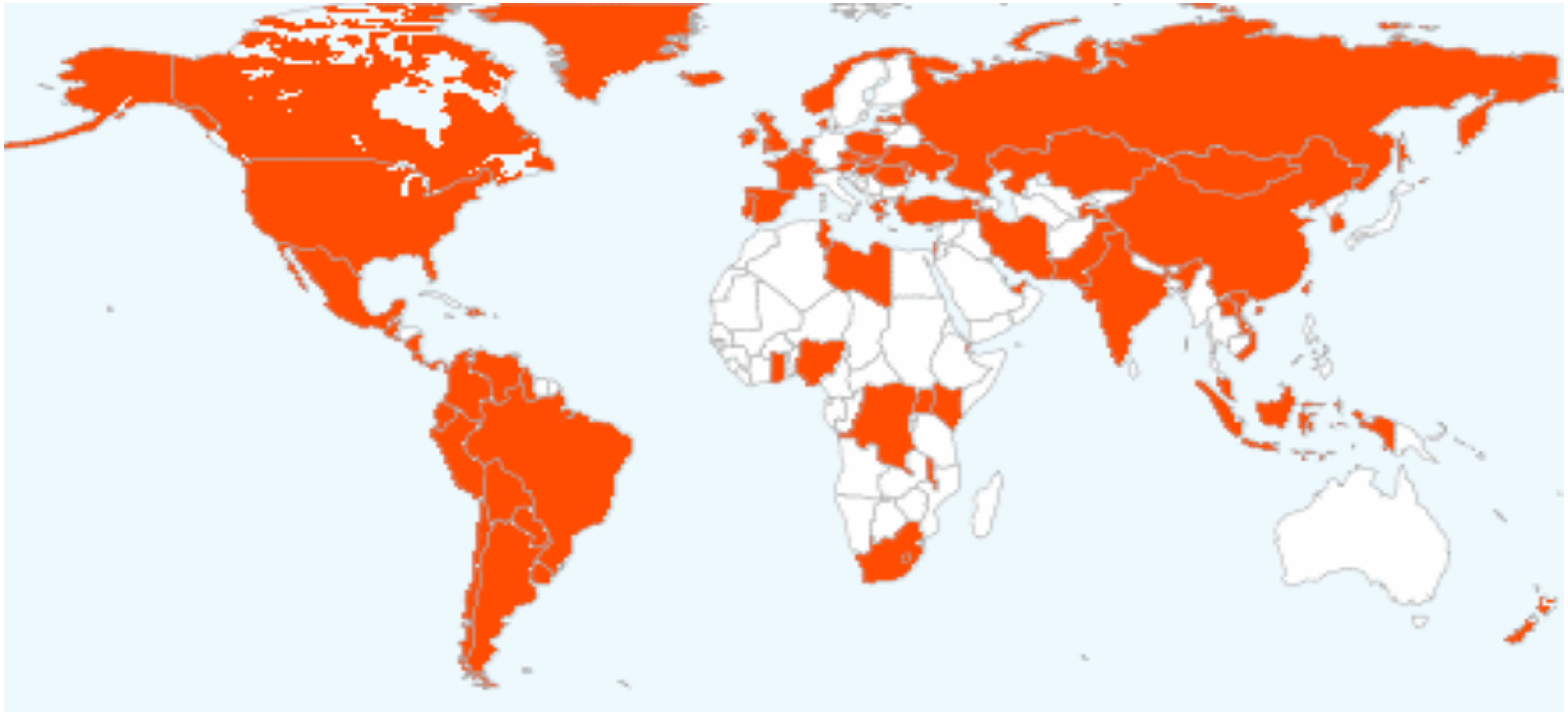
Collaborative Response to Malicious Abuse of Domain Name System

- ICANN will collaborate to mitigate malicious conduct enabled by the use of the DNS with:
  - DNS registries and registrars
  - Security research community
  - Security response community
  - Software and security/anti-virus vendors
  - Law Enforcement as appropriate

What is Conficker?

- An Internet worm
  - Self-replicating malicious code
  - Uses a network for distribution
- Uses various methods to spread the infection (network file shares, map drives removable media)
- Conficker code is *injected* into Windows Server Service
  - Variants disable security measures
  - Provides the attacker with remote control, execution privileges, and ability to download more malware
- Enlists the infected computer into a botnet
  - Conficker bots query rendezvous points for additional malware or instructions for already present malware

Affected Country Code TLDs – Conficker C



Positive Lessons learned

- Security and DNS communities can work effectively together, at an operational level, to contain global security threats
  - Trust was a critical element in ad hoc partnership
- Communications channels are essential in coordinating operational response
  - ICANN's role in enabling communications and staff participation in ad hoc partnership was appreciated
- Security and DNS communities need each other
  - Leverage competencies rather than duplicate them
  - Collective, global expertise is essential for effective response

Problems not yet solved

- Collaborative response forced botnet operators out of comfort zone but not out of business
- Botnet writers are agile and elusive
  - Cannot put them out of business without adopting a similarly agile model for response
- Collaboration can be difficult to sustain
  - Numerous and complex, harder to build and maintain, more fragile than botnets
- The risk-reward equation favors worm creators

Must have public – private collaboration

Way Forward on DNS Collaborative Response

- Efforts to block Conficker use of the DNS should be sustained
  - Must address challenges of long-term engagement
- Broader collaborative efforts within both the security and DNS communities should be considered
  - Security community dialogue about future collaboration models on-going
- In the DNS community, key players have continued to discuss how to organize effectively
  - Country code DNS TLD operators established working group

ICANN is active participating in these efforts

ccNSO IR WG update

- The purpose of the Incident Response Working Group (IR WG) is to develop sustainable mechanisms for the engagement of and interaction with ccTLD registries during incidents that may impact the DNS.
- In considering feasible methods the IR WG should take into account and be guided by:
  - The overarching requirement to preserve the security and stability of the DNS;
  - The non-binding relationship of the ccTLD registries to any one particular entity except possibly with their own governments;
  - Diversity of language, timezone, resources, expertise;
  - Particular policies and practices by which ccTLDs may be guided.

How can ICANN/DNS community and MENOG collaborate?

- Do network operators have incident response contacts? Do they have on-going dialogue? Exercise response?
- What can we do more to collaborate with you?