Joint SSR-RT/DSSA meeting

DSSA Progress Update

Dakar – October 2011

Goals for today

- Update you on our progress
- Raise awareness
- Solicit your input
- Look for opportunities
- Identify overlaps/conflicts

Charter: Background

- At their meetings during the ICANN Brussels meeting the At-Large Advisory Committee (ALAC), the Country Code Names Supporting Organization (ccNSO), the Generic Names Supporting Organization (GNSO), the Governmental Advisory Committee (GAC), and the Number Resource Organization (NROs) acknowledged the need for a better understanding of the security and stability of the global domain name system (DNS). This is considered to be of common interest to the participating Supporting Organisations (SOs), Advisory Committees (ACs) and others, and should be preferably undertaken in a collaborative effort.

Note: this is purely a Mikey invention that hasn't been reviewed by anybody

SSR Scope

I'm not sure if all of this is in-scope for the SSR team, but I imagine much of it is…

- **Incident response**
  - Provide initial response to an incident
  - Communicate incidents
  - Conduct impact assessments
  - Detect security events (through monitoring, advisories, reports of suspicious activity, etc.)
  - Provide incident resolution and countermeasures
  - Conduct investigations

- **Compliance Monitoring**
  - Measure progress and compliance in the following areas;
    - incident response
    - practices
    - technology
    - management
    - risk-management

- **Security Management**
  - Overall management and direction
  - Security strategy and alignment within overall IT strategy
  - Program management
  - Security metrics
  - Policy
  - Guidelines and standards

- **Operational Practices**
  - Training and awareness
  - Certification and accreditation
  - Legal and regulatory compliance
  - Securing external contractors
  - Rewards and sanctions
  - Acceptable use
  - Business continuity

- **Risk Management**
  - Developing and maintaining an inventory of systems (determining contents, owner, maintainer, location, etc.)
  - Mapping information and systems into security categories
  - Conducting assessments of systems
  - Analyzing risks and identifying mitigation/repair actions

- **Technical Practices**
  - Electronic mail security
  - Network security
  - Operating system security
  - Data security
  - Application security
  - Security for public servers
  - Wireless network security
  - Personal computers and electronic devices

- **Technology management**
  - Routers
  - Vulnerability assessment systems
  - Configuration management systems
  - Patch management systems
  - Firewall systems
  - Backup & recovery
  - Intrusion detection and log-analysis systems
  - Wireless access points

Note: this is purely a Mikey invention that hasn't been reviewed by anybody

DSSA Scope

- **Incident response**
  - Provide initial response to an incident
  - Communicate incidents
  - Conduct impact assessments
  - Detect security events (through monitoring, advisories, reports of suspicious activity, etc.)
  - Provide incident resolution and countermeasures
  - Conduct investigations

- **Compliance Monitoring**
  - Measure progress and compliance in the following areas;
    - incident response
    - practices
    - technology
    - management
    - risk-management

- **Security Management**
  - Overall management and direction
  - Security strategy and alignment within overall IT strategy
  - Program management
  - Security metrics
  - Policy
  - Guidelines and standards

- **Operational Practices**
  - Training and awareness
  - Certification and accreditation
  - Legal and regulatory compliance
  - Securing external contractors
  - Rewards and sanctions
  - Acceptable use
  - Business continuity

- **Risk Management**
  - Developing and maintaining an inventory of systems (determining contents, owner, maintainer, location, etc.)
  - Mapping information and systems into security categories
  - Conducting assessments of systems
  - Analyzing risks and identifying mitigation/repair actions

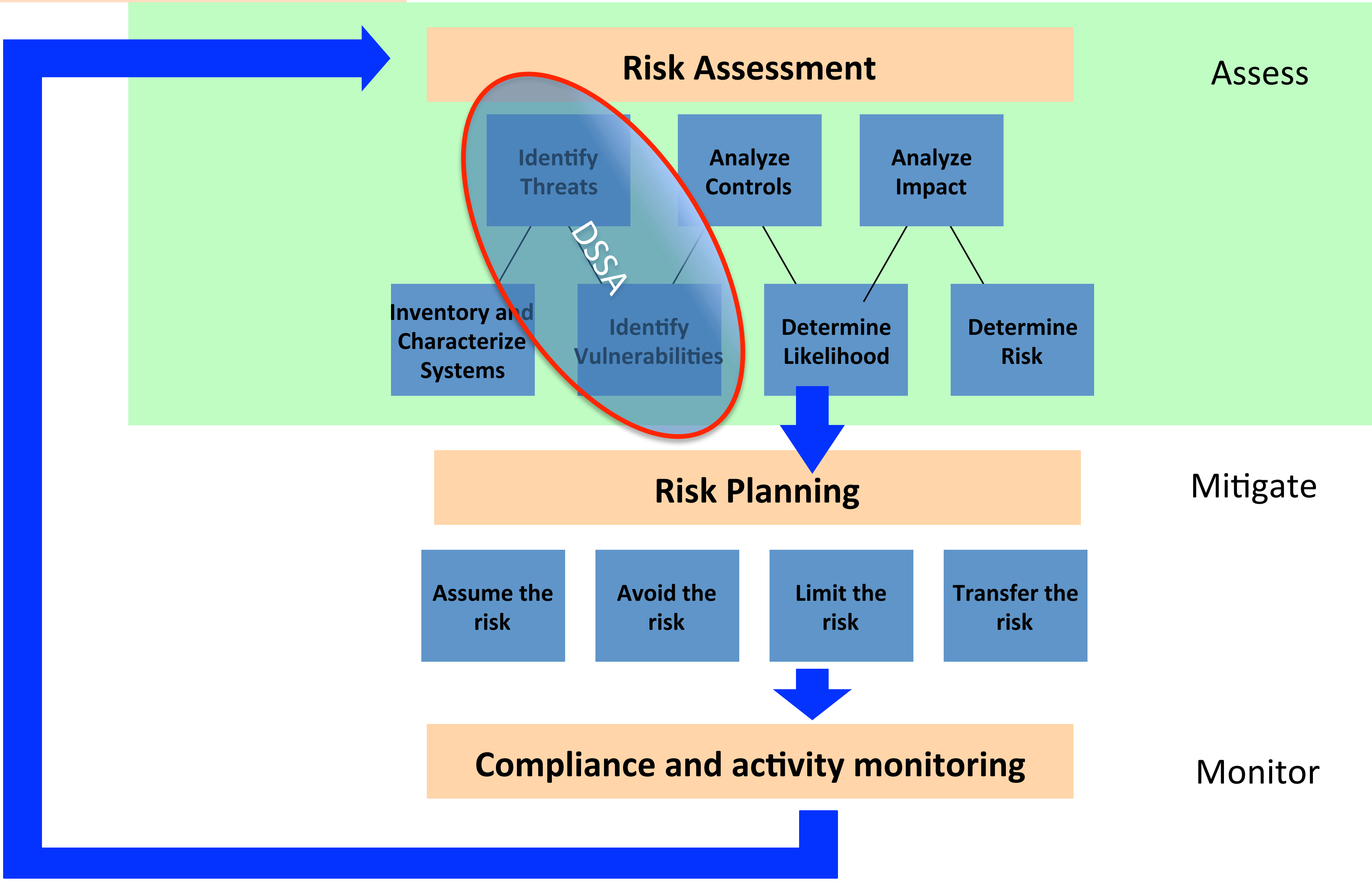
- **Technical Practices**
  - Electronic mail security
  - Network security
  - Operating system security
  - Data security
  - Application security

- **Technology management**
  - Routers
  - Vulnerability assessment systems
  - Configuration management systems
  - Patch management systems
  - Firewall systems
  - Backup & recovery
  - Intrusion detection and log-analysis systems
  - Wireless access points

Our scope is much narrower – more of a deep dive into this one area, only for DNS and TLDs

Risk management process

Note: this is purely a Mikey invention that hasn't been reviewed by anybody



Risk Assessment

Identify Threats

Analyze Controls

Analyze Impact

Inventory and Characterize Systems

Identify Vulnerabilities

Determine Likelihood

Determine Risk

DSSA

Assess

Risk Planning

Assume the risk

Avoid the risk

Limit the risk

Transfer the risk

Mitigate

Compliance and activity monitoring

Monitor

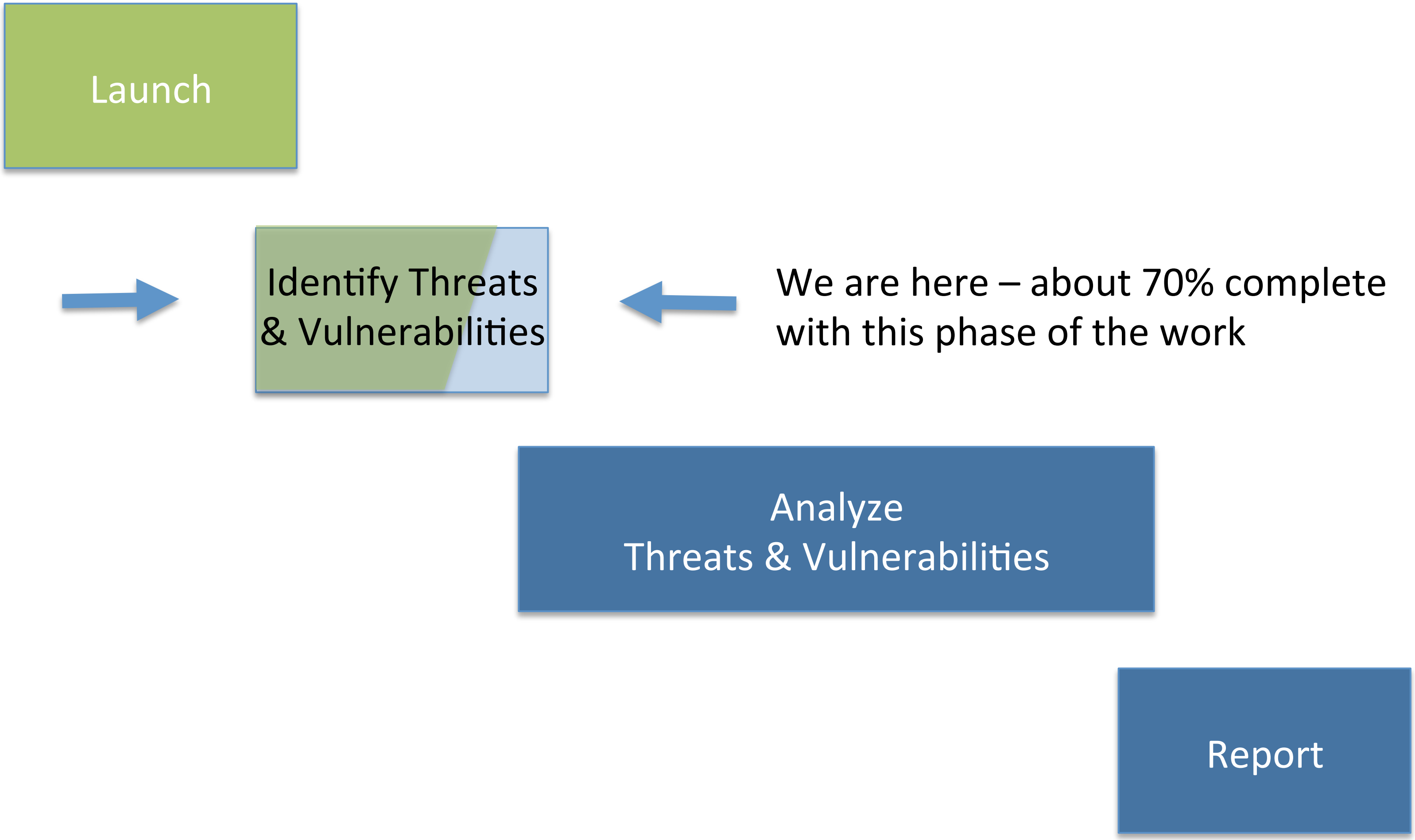
Note: this is from the DSSA Kick-Off deck – reviewed and approved

Goals and Objectives

Report to respective participating SO's and AC's on:

- – Actual level, frequency and severity of threats to the DNS
- – Current efforts and activities to mitigate these threats to the DNS
- – Gaps (if any) in the current response to DNS issues
- – Possible additional risk mitigation activities that would assist in closing those gaps (if considered feasible and appropriate by the WG)

Approach and status



Launch

Identify Threats & Vulnerabilities

We are here – about 70% complete with this phase of the work

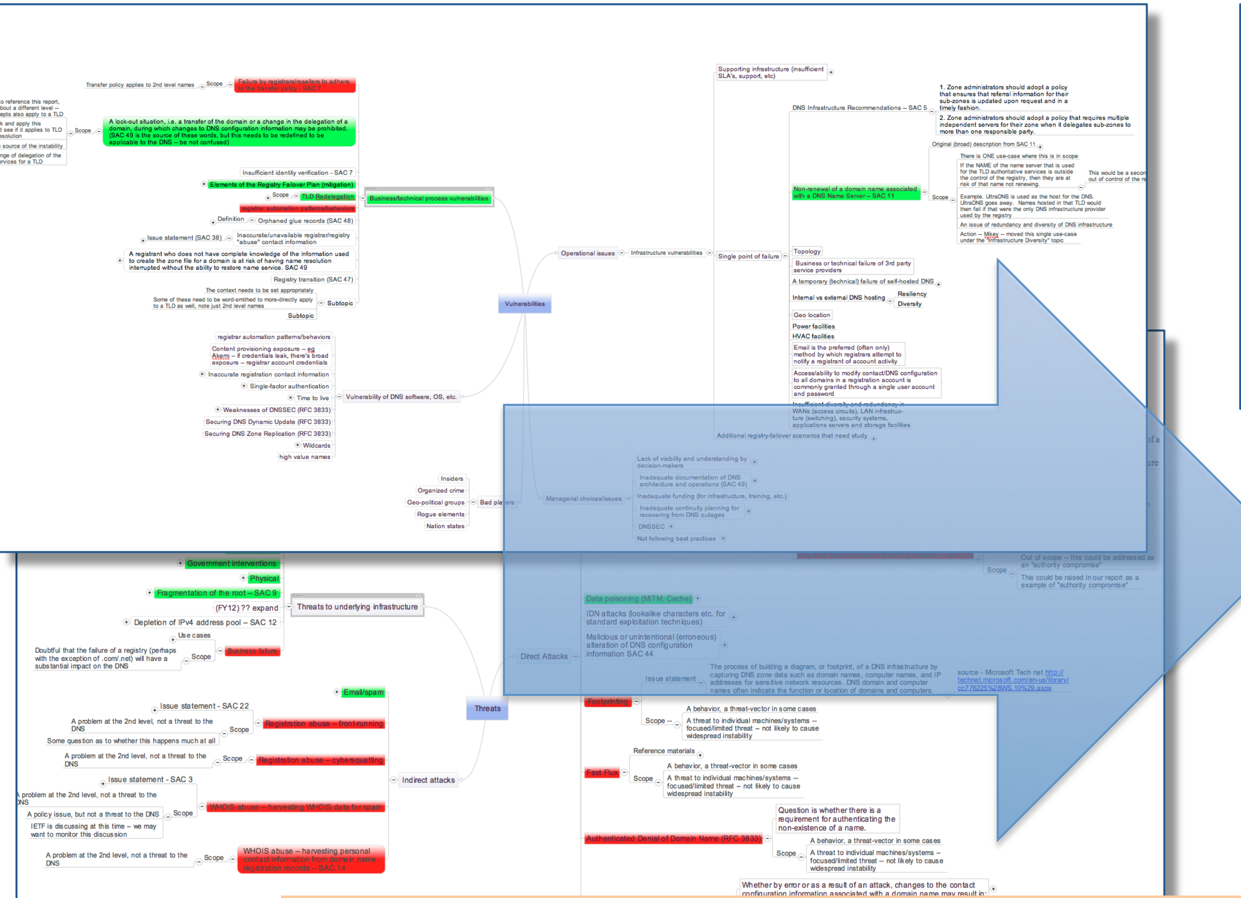
Analyze Threats & Vulnerabilities

Report

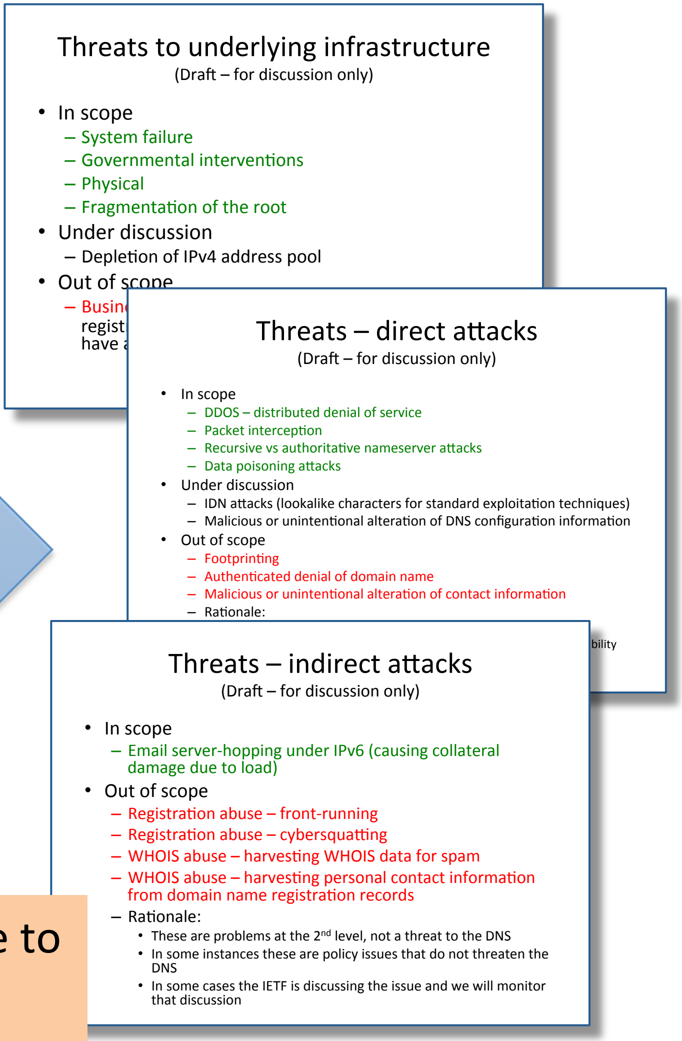
Activity since Singapore
Identify Threats

- The working group has:
  - Developed lists of vulnerabilities and threats (with definitions)
  - Made preliminary choices about which threats are in/out of scope for analysis
  - Developed preliminary criteria and mechanisms for segregating sensitive information
- Remaining work in this phase
  - Solicit additional lists/definitions from other experts and interested parties
  - Arrive at a final (prioritized) list of threats and vulnerabilities

Brainstorming and refining



Vulnerabilities
Business/technical process vulnerabilities
Operational issues
Infrastructure vulnerabilities
Single point of failure
DNS Infrastructure Recommendations – SAC 5
Non-renewal of a domain name associated with a DNS Name Server – SAC 11
Vulnerability of DNS software, OS, etc.
Managerial choices/issues
Bad players
Insiders
Organized crime
Geo-political groups
Rogue elements
Nation states
Elements of the Registry Failover Plan (mitigation)
TLD Redelegation
Threats
Threats to underlying infrastructure
Government interventions
Physical
Fragmentation of the root – SAC 9
Depletion of IPv4 address pool – SAC 12
Business failure
Direct Attacks
Indirect attacks
Data poisoning (MITM, Cache)
Footprinting
Fast Flux
Authenticated Denial of Domain Name (RFC 3833)
Email/spam
Registration abuse – front-running
Registration abuse – cybersquatting
WHOIS abuse – harvesting WHOIS data for spam
WHOIS abuse – harvesting personal contact information from domain name registration records – SAC 14



Threats to underlying infrastructure

(Draft – for discussion only)

- In scope
  - System failure
  - Governmental interventions
  - Physical
  - Fragmentation of the root
- Under discussion
  - Depletion of IPv4 address pool
- Out of scope
  - Busin
    regist
    have a

Threats – direct attacks

(Draft – for discussion only)

- In scope
  - DDOS – distributed denial of service
  - Packet interception
  - Recursive vs authoritative nameserver attacks
  - Data poisoning attacks
- Under discussion
  - IDN attacks (lookalike characters for standard exploitation techniques)
  - Malicious or unintentional alteration of DNS configuration information
- Out of scope
  - Footprinting
  - Authenticated denial of domain name
  - Malicious or unintentional alteration of contact information
  - Rationale:

bility

Threats – indirect attacks

(Draft – for discussion only)

- In scope
  - Email server-hopping under IPv6 (causing collateral damage due to load)
- Out of scope
  - Registration abuse – front-running
  - Registration abuse – cybersquatting
  - WHOIS abuse – harvesting WHOIS data for spam
  - WHOIS abuse – harvesting personal contact information from domain name registration records
  - Rationale:
    - These are problems at the 2nd level, not a threat to the DNS
    - In some instances these are policy issues that do not threaten the DNS
    - In some cases the IETF is discussing the issue and we will monitor that discussion

> "I'm sorry this letter is so long, I didn't have time to make it shorter."
>
> — *George Bernard Shaw, Pascal, Goethe, Wilde, Cicero, DSSA*

Scope

- From our charter, “the working group should focus on "The actual level, frequency and severity of threats *to the DNS*.... The DSSA-WG should limit its activities to considering issues *at the root and top level domains* within the *framework of ICANN’s coordinating role* in managing Internet naming and numbering resources as stated in its Mission and in its Bylaws.”
- The WG refined this to add “we are *not* to look at every threat having to do with, or taking place via, the DNS, or that impacts some party using the DNS. *We are concerned with “the” DNS, i.e. threats to the system itself, and relevant to ICANN’s role.*”

Threats to underlying infrastructure

(**Draft** – for discussion only)

- In scope
  - System failure (e.g. hardware/software failures, etc.)
  - Governmental interventions (e.g. seizure, blocking, etc.)
  - Physical events (e.g. natural disasters, etc.)
  - Fragmentation of the root (e.g. alternate roots, root scaling, etc.)
- Under discussion (**your thoughts?**)
  - Business failure
- Out of scope
  - Depletion of IPv4 address pool
  - Rationale:
    - The concerns (routing table growth and route fragmentation) will happen anyway
    - The DNS is not a heavy consumer of IP addresses, thus depletion is unlikely to have a significant impact

Threats – direct attacks

(**Draft** – for discussion only)

- In scope
  - DDOS – distributed denial of service
  - Packet interception
  - Recursive vs authoritative nameserver attacks (e.g. using vulnerable recursive DNS servers as reflectors to attack TLD DNS servers)
  - Data poisoning attacks
- Under discussion (**your thoughts?**)
  - IDN attacks (lookalike characters for standard exploitation techniques – awaiting results of the Variants project)
  - Malicious or unintentional alteration of DNS configuration information
- Out of scope
  - Footprinting
  - Authenticated denial of domain name
  - Malicious or unintentional alteration of contact information
  - Rationale:
    - These are behaviors or, in some cases, threat vectors
    - These are focused/limited threats, not likely to cause widespread instability

Threats – indirect attacks

(**Draft** – for discussion only)

- In scope
  - Email server-hopping under IPv6 (causing collateral damage due to load)
- Out of scope
  - Registration abuse – front-running
  - Registration abuse – cybersquatting
  - Registration directory service abuse – harvesting registration data for spam
  - Registration directory service abuse – harvesting personal contact information from domain name registration records
  - Rationale:
    - These are problems at the 2nd level, not a threat to the DNS
    - In some instances these are policy issues that do not threaten the DNS
    - In some cases the IETF is discussing the issue and we will monitor that discussion (harvesting registration data for spam)

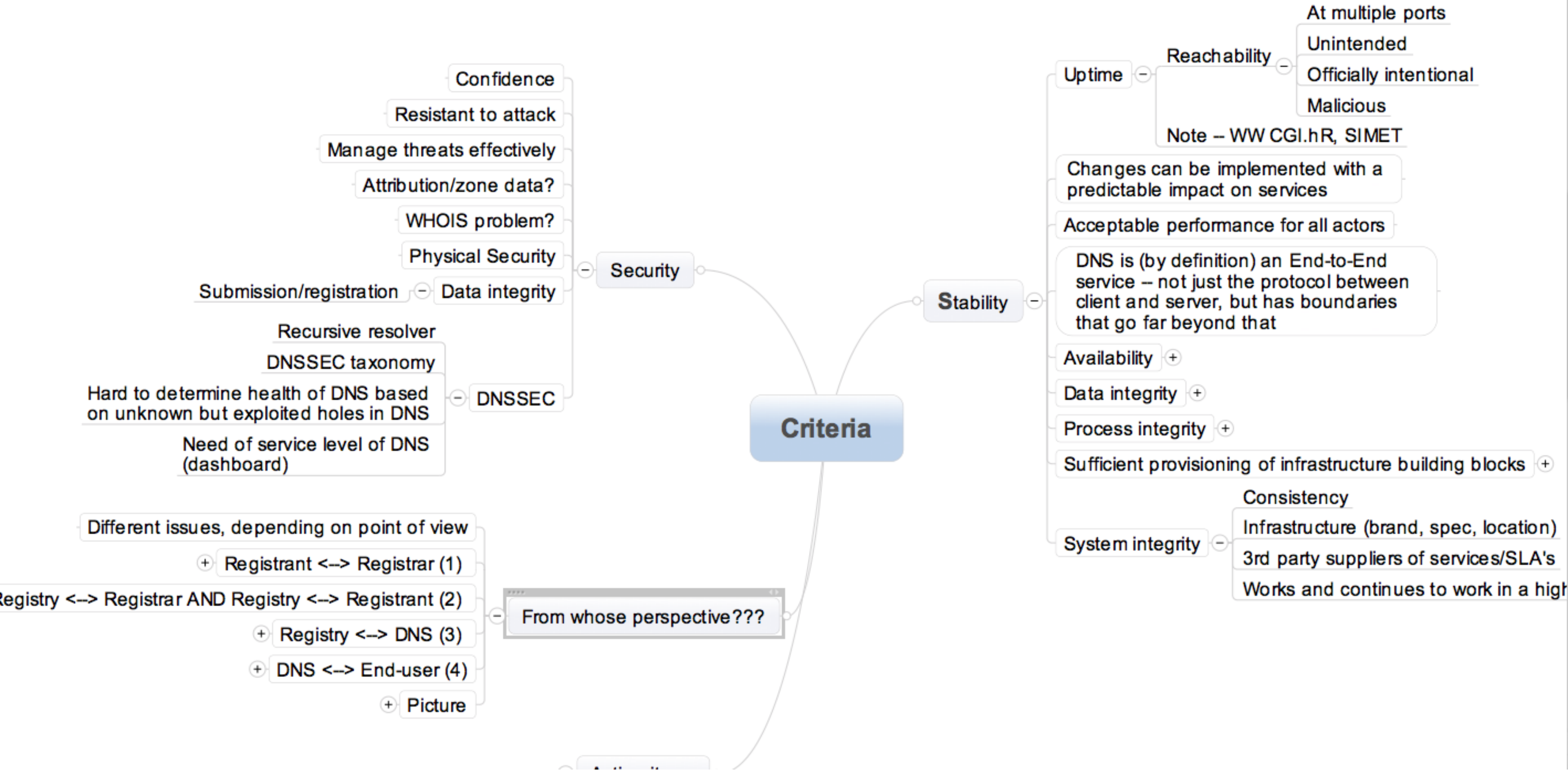
Vulnerabilities

(**Draft** – for discussion only)

- Operational issues
  - Infrastructure vulnerabilities (e.g. single point of failure, DNS software vulnerabilities, insufficient SLA's etc.)
  - Business and technical process vulnerabilities (e.g. orphaned glue records, lock-outs, TLD redelegation, etc.)
- Registry failure and continuity
- Managerial choices/issues
  - Not following best practices (e.g. measures to detect/prevent unauthorized changes, etc.)
  - Gaps in continuity planning (e.g. responsibilities, actions, documentation, etc.)
  - Inadequate funding/resources (for infrastructure, training, staff, etc.)
  - Lack of visibility/understanding by decision-makers

Criteria

(Note: this is very-early **draft**)



- Criteria
  - Security
    - Confidence
    - Resistant to attack
    - Manage threats effectively
    - Attribution/zone data?
    - WHOIS problem?
    - Physical Security
    - Data integrity
      - Submission/registration
    - DNSSEC
      - Recursive resolver
      - DNSSEC taxonomy
      - Hard to determine health of DNS based on unknown but exploited holes in DNS
      - Need of service level of DNS (dashboard)
  - From whose perspective???
    - Different issues, depending on point of view
    - Registrant <--> Registrar (1)
    - egistry <--> Registrar AND Registry <--> Registrant (2)
    - Registry <--> DNS (3)
    - DNS <--> End-user (4)
    - Picture
  - Stability
    - Uptime
      - Reachability
        - At multiple ports
        - Unintended
        - Officially intentional
        - Malicious
      - Note -- WW CGI.hR, SIMET
    - Changes can be implemented with a predictable impact on services
    - Acceptable performance for all actors
    - DNS is (by definition) an End-to-End service -- not just the protocol between client and server, but has boundaries that go far beyond that
    - Availability
    - Data integrity
    - Process integrity
    - Sufficient provisioning of infrastructure building blocks
    - System integrity
      - Consistency
      - Infrastructure (brand, spec, location)
      - 3rd party suppliers of services/SLA's
      - Works and continues to work in a high

Questions?

- This “scoping” work is well along, but not complete. We are interested in your thoughts