- Threats
  - Threats
    - Threats to underlying infrastructure
      - Business failure
        - Registry business failure
        - Registrar business failure
        - Scope
          - Depends on which domain?
          - Doubtful that the failure of a registry (perhaps with the exception of .com/.net) will have a substantial impact on the DNS
      - System failure
        - A system failure -- resulting from a hardware or software failure, or configuration error -- could disrupt any or all the services a registrar or registry operator provides. A system failure is likely to be a temporary failure.
        - Possible points of failure
        - Scope
          - Depends on the impact of the failure
          - Refer to SSAC 047 and Registry Failover for ideas about impact
          - Needs further discussion/work before making the scope determination
      - Government interventions
        - Regulatory-imposed shutdown
        - Government Seizure of Registry Operator
        - Government Takeover/Coup
        - Political
      - Physical
        - Facility security
        - Natural disaster
        - Physical disasters
        - Scope -- threat vectors that effect root or TLD infrastructure, otherwise not in scope
      - Depletion of IPv4 address pool -- SAC 12
        - Routing table growth
        - Route fragmentation
      - Fragmentation of the root -- SAC 9
        - Alternate DNS roots
        - Root scaling (SAC 46)
        - Intentional or accidental results of DNS blocking (SAC 50)
      - (FY12) ?? expand
    - Direct Attacks
      - DDOS
      - Packet Interception
      - Recursive vs authoritative nameserver attacks
      - Authority or authentication compromise
      - Domain name hijacking/theft - SAC 7
      - Registrar impersonation phishing attacks -- SAC 28
      - Data poisoning (MITM, Cache)
      - Footprinting
      - Fast Flux
      - IDN attacks (lookalike characters etc. for standard exploitation techniques)
      - Authenticated Denial of Domain Name (RFC 3833)
      - Gain control of account user/password
      - Malicious or unintentional (erroneous) alteration of DNS configuration information SAC 44
      - Malicious or unintentional (erroneous) alteration of contact information SAC 44
    - Indirect attacks
      - 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