- non-adversarial threat sources
  - Notes
  - template
  - Threat source - configuration errors by privileged users
  - Threat source - business failure of key provider
    - Disrupts a "major" zone file (.COM/.NET/.UK/.DE etc.)
      - Extensive plans in place to manage the transition to another provider
      - escrow is in place for the generics -- but the cc's are not escrowed
      - This is an event that would be easy to see coming in advance
    - Disrupts a "lesser" zone file (that is not outsourced to a major provider)
      - KPNQuest bankruptcy is an example
      - bart: KPN Q west is interesting example of what haapnes. The first thing that happened was that the caretakers came in. WHat will happen next depends very much on national law provisions
    - Root zone -- is published incorrectly
    - Root zone -- is not published
    - Disrupts the IANA zone file
    - Disrupts DNSSEC from a "Major" DNSSEC provider
      - we have very small deployment of DNSSEC on the planet
    - Disrupts DNSSEC for a TLD zone
    - Disrupts Critical DNS support files
    - Disrupts provisioning systems between registries and registrars (the result being that registrars can't add/change/delete zones from the TLD)
    - General note -- for final report -- we are making this evaluation in 2012, prior to the arrival of new gTLD providers -- needs to be reassessed in X years time
  - Threat source - nation state -- interventions with accidental or unintended consequences -- tentative disposition, remove
    - Disrupts a "major" zone file (.COM/.NET/.UK/.DE etc.)
      - We're looking at this in different ways
      - Are we talking about *our own* government? or the worst-case?
      - Does the country have the ability to do this?
      - Where is the impact felt -- sovergn perimeter? or whole internet?
      - Concern about the scope of the question is a concern
        - Are we talking
    - Root zone -- is published incorrectly
    - Root zone -- is not published
    - Disrupts the IANA zone file
    - Disrupts DNSSEC from a "Major" DNSSEC provider
    - Disrupts DNSSEC for a TLD zone
    - Disrupts Critical DNS support files
    - Disrupts provisioning systems between registries and registrars (the result being that registrars can't add/change/delete zones from the TLD)
    - General note -- for final report -- we are making this evaluation in 2012, prior to the arrival of new gTLD providers -- needs to be reassessed in X years time
    - Disrupts a "lesser" zone file (that is not outsourced to a major provider)
  - Threat source - key hardware failure (storage, processing, network
  - Threat source - key networking or operating-system software failure
  - Threat source - mission-specific software failure (WHOIS, EPP/RPP/billing)
  - Threat source - root scaling impacts
  - Threat source - natural disaster
  - Threat source - widespread telecommunications infrastructure failure
  - Threat source - widespread power infrastructure failure
- adversarial threat sources