

# DDOS Mitigation

Don Hollander  
APTLD General Manager

# DDOS Mitigation – Why

- Number one threat to ccTLDs today
- Risks are potentially catastrophic for ccTLD managers
- Political, Economic, Personnel
- Collective Approach Available

# Overall DDoS Approach

- Attack & Disaster Response Planning Workshop
- Technical Training Workshop
- Demand Aggregation for AnyCast Services
- 
- APTLD Working Group - .my, .au & .nz

# Attack & Disaster Response Planning (ADRP)

- Partnership Approach
  - ICANN
  - APNIC
  - Others
- Two Day (approx) Workshop

# ADRP Syllabus

- The Philosophy behind Preparing for a Disaster or Attack
- Case Study 1 – The Story of a Disaster
- Establishing Inventories of items at Risk
- Considering the nature of Disasters or Attacks
- Developing the Risk & Threat Assessment Report
- Case Study 2- The Story of an Attack

# ADRP Syllabus – Cont.

- Exercise – Developing a Risk & Threat Assessment Report
- Communications – Channels and Content and Timing
- Exercise – Develop a Disaster/Attack Communications Plan
- Response Constraints
- Case Study 3 – Unusual Attack Vectors

Developing a Mitigation Plan

# ADRP Syllabus – Cont.

- Developing a Response Plan
- Desk Checking the Response Plan
- Training & Testing & Rehearsing the Response Plan
- Case Study 4 – Thwarted Attack
- Exercise, Evaluate, Review, Repeat

# ADRP Management Training

- Is there a need?

# ADRP Technical Training

- Syllabus still being developed

# ADRP – Anycast Demand Aggregation

- Is there interest
- Issues to consider