ResiliNets: Motivation, Challenges, and Disciplines

James P.G. Sterbenz, David Hutchison, E. Çetinkaya, A Jabbar, J.P. Rohrer, M. Schöller, P. Smith

www.itc.ku.edu/resilinets - www.comp.lancs.ac.uk/resilinets

- Pervasive network infrastructure with increasing...
  - dependence by individuals, businesses, nations
  - consequences of disruption to lives, security, commerce
  - attractiveness as target from bad guys
- Networks are now part of critical infrastructure
  - on which other critical infrastructure depends
    - power grid, transportation, financial markets, ...
- Resilience
  - ability to provide & maintain acceptable level of service
    in the face of challenges to normal operation

Challenges to Resilience

- Challenges
  - unintentional misconfiguration and operational mistakes
  - large-scale natural disasters
  - malicious attacks including terrorists and DDoS crackers
  - comm. environment: wireless, mobile, delay
  - unusual but legitimate traffic (e.g. flash crowd)
  - lower level service failures including due to faults
- From faults to service failures
  - dormant faults triggered by challenges or operation
  - active faults manifest as errors
  - errors may degrade network operation (fault tolerance)
  - degraded network operation may lead to service failure

ResiliNets Approach

- ResiliNets: resilient and survivable networking
- Strategy for resilience: D²R² + DR
  - D²R²: real-time loop defend, detect, remediate, recover
  - DR: background actions of diagnose and refine
- Principles to guide design of resilient networks
  - prerequisites, tradeoffs, enablers, behaviour
- 2-dimensional system state space
  - operational space
    - normal, partially degraded, severely degraded
  - service space
    - acceptable, impaired, unacceptable