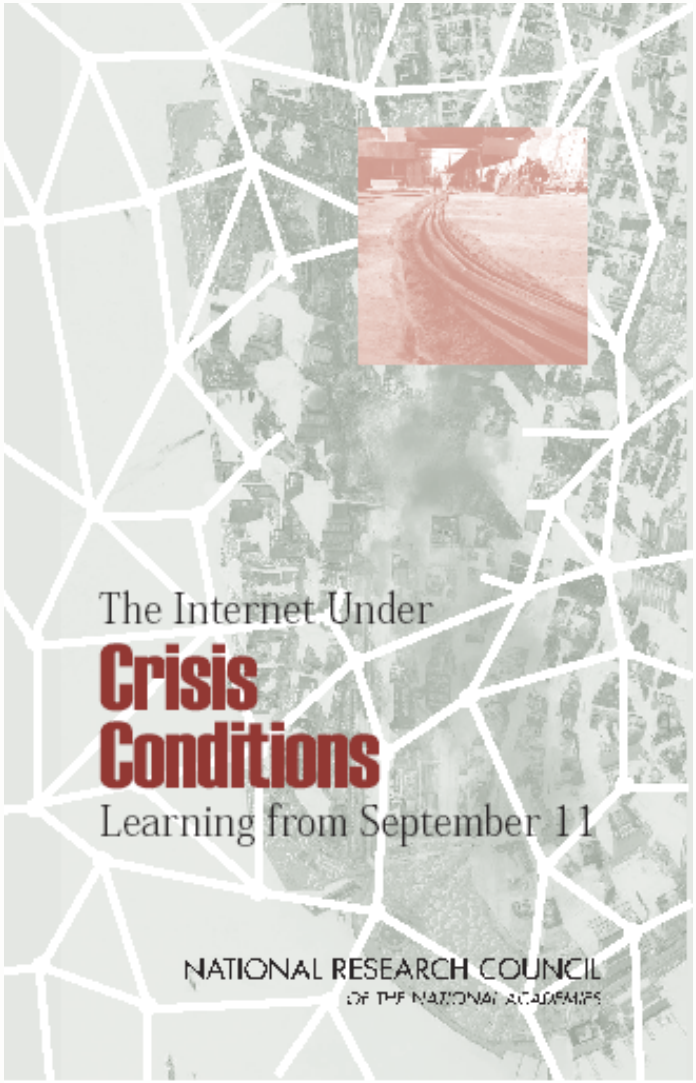
Lessons Learned from the 9/11 Attacks

Jennifer Rexford
Princeton University

Thanks to Craig Partridge for slides from an earlier briefing…



The Internet Under Crisis Conditions:
Learning from September 11

Computer Science and Telecommunications Board

The National Academies

Public release: Nov 2002

Study committee: Craig Partridge (Chair), Paul Barford, David D. Clark, Sean Donelan, Vern Paxson, Jennifer Rexford, and Mary Vernon

CSTB staff: Jon Eisenberg, Marjory Blumenthal, David Padgham, and D.C. Drake

http://www.nap.edu/openbook.php?isbn=0309087023

A 9/11 Timeline

Early Morning

- Up until 8:46 fairly routine
  - Some network upgrades during the night
  - Traffic beginning to increase with the work day
- 8:46 AA 11 crashes into WTC1
- 9:02 UA 175 crashes into WTC2
  - Internet news servers rapidly inundated
- 9:37 AA 77 crashes into the Pentagon
- 9:39 NYC without broadcast TV and radio

Mid-Morning

- 10:05 World Trade Center 2 collapses
  - Internet infrastructure in WTC2 destroyed
- 10:28 World Trade Center 1 collapses
  - At least one trans-atlantic link fails
  - Internet traffic loads and connectivity drop
- 11:00 NYC cell phone call demand peaks
- 11:00 Internet connectivity close to normal
- 11:39 www.cnn.com now handling demand

Afternoon

- 1:16 Part of the national 1-800 telephone network fails
- 4:35 First major electrical outage in NYC
  - Substation in WTC 7
  - Internet connectivity dips 2%
- 5:20 WTC 7 collapses
  - Extensive damage to Verizon facility
  - Internet connectivity dips 1%

Evening

- Three remaining data-comm centers in lower Manhattan struggle to keep operations running
  - Dust causes air conditioning problems
  - Operator error turns off generator at one facility
  - Access limited
- Restoration of service in NYC underway
- Feeding network operators difficult
- Operational issues continue several days

Report Findings

Findings

- The Internet was mostly fine
  - Little effect on Internet services as a whole
  - Network displayed considerable flexibility
- Limited measurements hamper analysis
  - Limited data, and limited archiving of data
  - Lack of a good "typical day" for baseline
- Major effect on some Internet services
  - 2500% growth in demand for CNN site
  - 1300% growth in cell phone demand (11am)

Findings

- Use of Internet services was not typical
  - Television and phone were primary services
  - Internet servers as a backup for TV (news Web sites) and phone (instant messaging, VoIP)
  - Understanding and enhancing the news
- Inadequate redundancy in some parts
  - ISPs concentrating facilities in one location
  - Certain physical attacks could be worse
  - Electronic attacks a more serious concern

Findings

- Subtle operational issues merit attention
  - Network operators' reliance on 1-800 numbers
  - Internet and PSTN sharing fibers and conduits
  - Planning for staff needing to eat and sleep
  - Multi-day power outages, fuel deliveries, etc.
- Better leveraging of Internet in the future
  - Disaster plans should plan for Internet use
  - Give *some* connectivity to all (IM, text msg)

Anecdotes

Anecdotes

- CNN Web site
  - The “one-packet homepage”
  - Repurposing Turner server machines
  - Re-Akamaizing the CNN Web site
- Hidden dependencies
  - South Africa top-level domain name server
  - Authentication server for Florida ISP
  - Intra-hospital network relying on the Internet
- Better Internet stability in some places
  - Network operators went home…

Conclusions

- The Internet on 9/11
  - The Internet was relatively reliable
  - Though some services were badly affected
  - And application usage dramatically shifted
- Lessons learned
  - Better, more systematic measurement
  - Uncovering hidden dependencies
  - Addressing operational concerns