# Evolving the Core:
## Deployment Challenges and the Internet

J. Scott Marcus
Transatlantic Fellow
The German Marshall Fund of the United States

The author has affiliations with both the FCC and the European Commission. The opinions expressed are his own, and do not necessarily reflect the views of either agency.

# Thought Questions

- Are market incentives alone sufficient to ensure that societally vital enhancements to Internet infrastructure (including security enhancements) will be deployed?
- If not, is it possible to *correctly* identify and prioritize those features that are unlikely to be deployed without “help”?
- What public policy measures are available to foster deployment of those features?
- What are the costs and benefits of those measures?
- What are the prospects that they will be effective?

# Public Goods

“Things that can be consumed by everybody in a society, or nobody at all. They have three characteristics. They are:

- non-rival – one person consuming them does not stop another person consuming them;
- non-excludable – if one person can consume them, it is impossible to stop another person consuming them;
- non-rejectable – people cannot choose not to consume them even if they want to.

Examples include clean air, a national defence system and the judiciary. The combination of non-rivalry and non-excludability means that it can be hard to get people to pay to consume them, so they might not be provided at all if left to market forces ...”

From economist.com.

# A Glacial Pace of Deployment?

- Enhancements to DNS security
- Operational and protocol enhancements to the BGP-4 exterior routing system
- IPv6 (tangentially relevant to security)

See *The National Strategy to Secure Cyberspace*, February, 2003

# Market Forces

- Economic incentives
  - Sufficiency
  - Alignment - Who pays?  Who benefits?
  - Quantifiability
  - Time frame over which benefits are generated
- The economics of network externalities
- Transaction costs and the end-to-end principle

# Economic Incentives

- Who pays?
  - The service provider?
  - Ultimately, the customer?
  - The Government?
- Who benefits?
  - The service provider?
  - Society at large?
  - How can the benefits be quantified?
- In what time frame?
  - Financial markets have short horizons.
  - Difficult to insure against a “30 year flood”.
  - “Après moi, le déluge!”

# The Business Case

“Scott, you don’t have to wait a year or two to find out whether we are having problems getting this stuff deployed.  We already know the answer.  There is nothing new in these reports.  All of this has been known for years.  If we were able to craft business cases for our management, all of this would have been done long ago.”

- Participant, ISP Working Group, CIPB

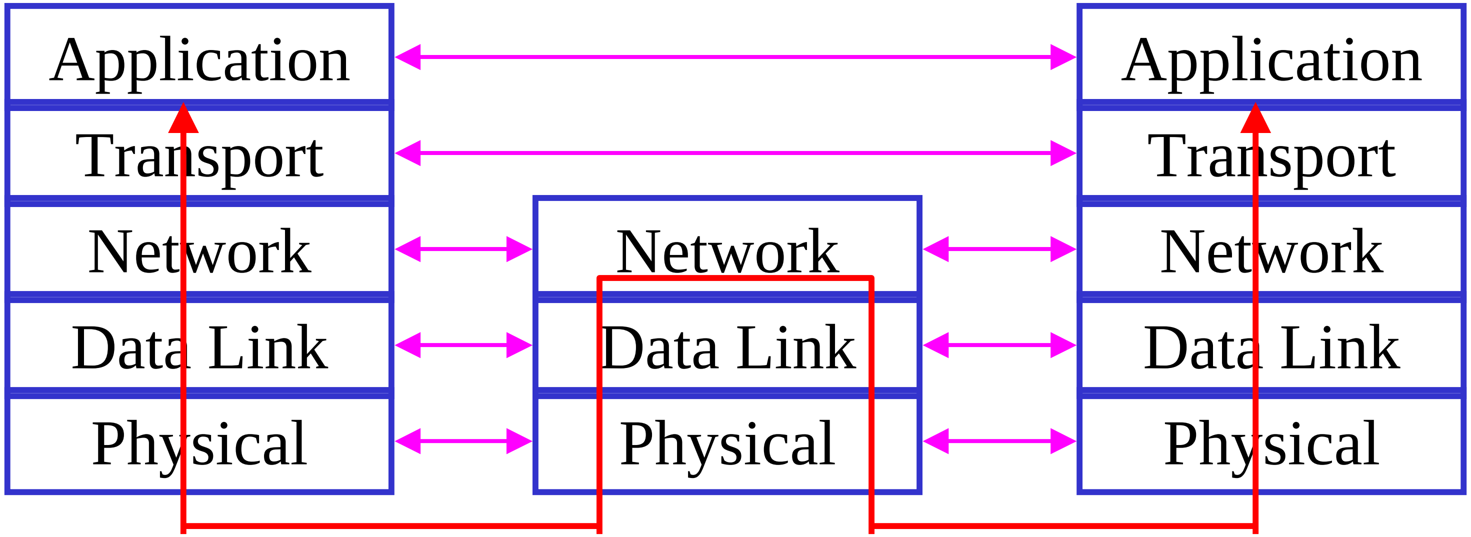
# Network Externalities

- Some capabilities are worth more as more consumers adopt them. Nothing succeeds like success.
- The societally optimal value is not necessarily where the market would settle without “help”.
- Examples of innovations that got over the adoption hump:
  - telephone - Universal Service
  - VCRs - widespread deployment for time shifting antedated the emergence of a rental industry
  - CD players - vertical integration with recording studios
  - black and white TV - industry and government standards

Cf. Rohlffs, *Bandwagon Effects in High-Technology Industries*, 2001.

# The TCP/IP Reference Model

Layers interact with peer layers



Layers derive services from successively lower layers

# The End-to-End Principle

- A guiding principle of Internet architecture.
- Certain features are best implemented, not in the network, but in the end systems that implement the application. It is counterproductive for the network to also provide those same features.
- It is easy to incorporate new innovations at the Application Layer (e.g. the WorldWide Web).
- It is also easy to incorporate new innovations at the Data Link and Physical Layers (e.g. cable modem, DSL, Wi-Fi).
- Innovations that impact the global system may be harder.
  - Requirements for interoperability and upward compatibility.
  - Limited value until ubiquitously (or at least widely) available.
  - Many participants -> high transaction costs.

# Domain Name System Vulnerabilities

- No authentication of the domain name server.
- No assured integrity of the DNS response.
- No assurance that the information in the DNS server has not been maliciously altered.
- Exposure to Denial of Service (DoS) attacks.

# DNS Security Mechanisms

- Secret Key Transaction Authentication for DNS (TSIG)
  - MD5 cryptographic hash/checksum.
  - Authenticates sending system and transmission integrity.
  - Does not authenticate underlying data.
  - Lack of a key distribution mechanism limits applicability.
- Domain Name System Security Extensions (DNSSEC)
  - Public key cryptography facilitates key distribution.
  - Chain of trust proceeds from the DNS root to the leaves.
  - Provides authentication, integrity and object security.
  - Unambiguously deals with lack of existence of a DNS name.

# Deployment Considerations

- TSIG
  - A point solution rather than a general solution.
  - Computational and operational cost are modest.
  - Can be implemented by a pair of DNS servers, e.g. for zone transfers.
  - Transaction costs are low.
  - Deployable today.
- DNSSEC
  - An elegant, general solution.
  - Computational and operational complexity is high.
  - Solution ideally involves a great many components, from DNS root servers to TLDs to SLDs … and finally to DNS clients in end user systems.
  - Transaction costs for global deployment are considerable.
  - DNSSEC has been viewed as difficult and immature.

# Public Policy Considerations

- **Balance**
  - What are the risks of action?
  - What are the risks of inaction?
- **Minimalism**
  - What is the least intrusive intervention that will achieve the desired public policy objective?
  - "That government is best which governs least."
    - Thoreau

# Public Policy Alternatives

- Help industry to coalesce consensus.
- Collect relevant data and statistics.
- Provide “seed money” for research and for interoperability testing.
- Support desired services through government’s own purchasing preferences.
- Provide remedies (e.g. under tort law) where firms fail to achieve a recognized standard of care.*
- Fund the deployment of desired services.
- Mandate the use of desired services.

* - *Critical Information Infrastructure Protection and the Law*, National Academies, 2003

# Helping to Coalesce Industry Consensus

- Government can use the “bully pulpit” to advance public policy goals.
- Support sharing of information on best practices, while protecting sensitive information.
- Mitigate antitrust concerns when competitors discuss joint actions that are not anticompetitive.
- Stimulate standards bodies to focus on relevant problems.

# Impediments to Data Collection and Information Sharing

- Antitrust concerns
- Obligations to make data publicly available
  - FOIA concerns
    - Need for predictability and certainty
    - Perception versus reality
    - DHS enabling legislation
  - State sunshine laws

Cf. *Critical Information Infrastructure Protection and the Law*, National Academies, 2003

# Sobering Case Studies

- Government OSI Protocol (GOSIP) - the purchasing power of the U.S. Government and of governments worldwide was insufficient to drive global adoption of OSI protocols. TCP/IP won out, largely due to network externality advantages.
- Metric conversion - A similar story. The U.S. Government has been officially committed to metric since the Seventies, and most measures short of an outright mandate have been attempted. Progress has nonetheless been glacial.

# Public Policy Considerations

- **Balance**
  - What are the risks of action?
  - What are the risks of inaction?
- **Minimalism**
  - What is the least intrusive intervention that will achieve the desired public policy objective?
  - "That government is best which governs least."
    - Thoreau