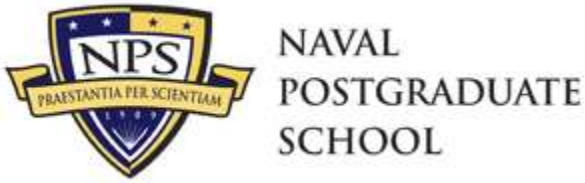
What do we want in a future information infrastructure?

David Alderson
Operations Research Department
Naval Postgraduate School



MS&E 91si: U.S. National Cybersecurity
November 16, 2006

Acknowledgements

- Caltech: John Doyle
- AT&T: Walter Willinger
- CISAC: Kevin Soo Hoo, Mike May, David Elliott, William Perry
- MS&E 91SI: Martin, Keith

The Internet* has become a critical information infrastructure.

- Individuals
- Private corporations
- Governments
- Other national infrastructures

The Internet* has become a critical information infrastructure.

- Personal communication
  - email, IM, IP telephony, file sharing
- Business communication
  - Customers, suppliers, partners
- Transaction processing
  - Businesses, consumers, government
- Information access and dissemination
  - web, blog

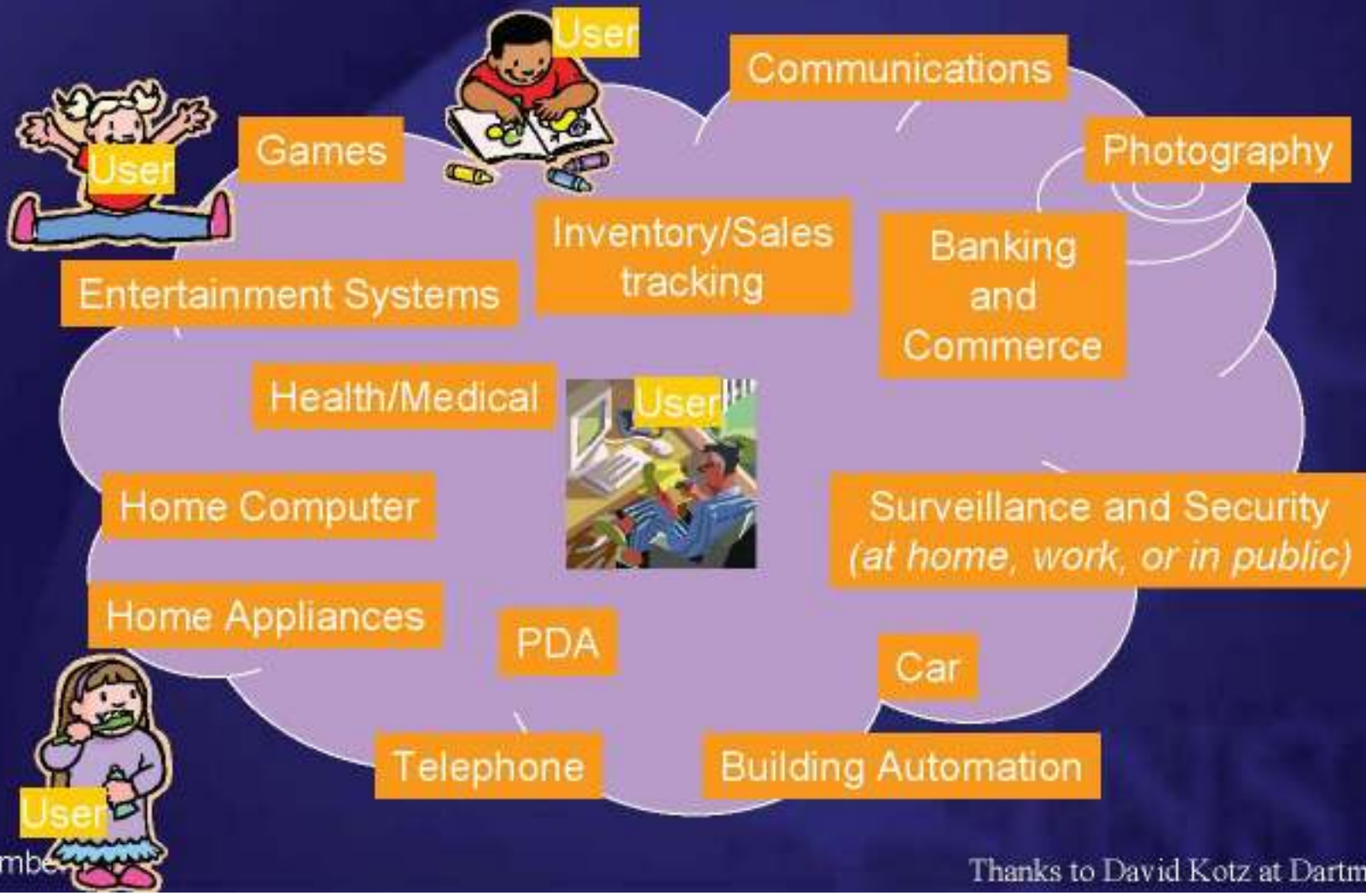
What do we want in a future information infrastructure?

(time for class participation…)

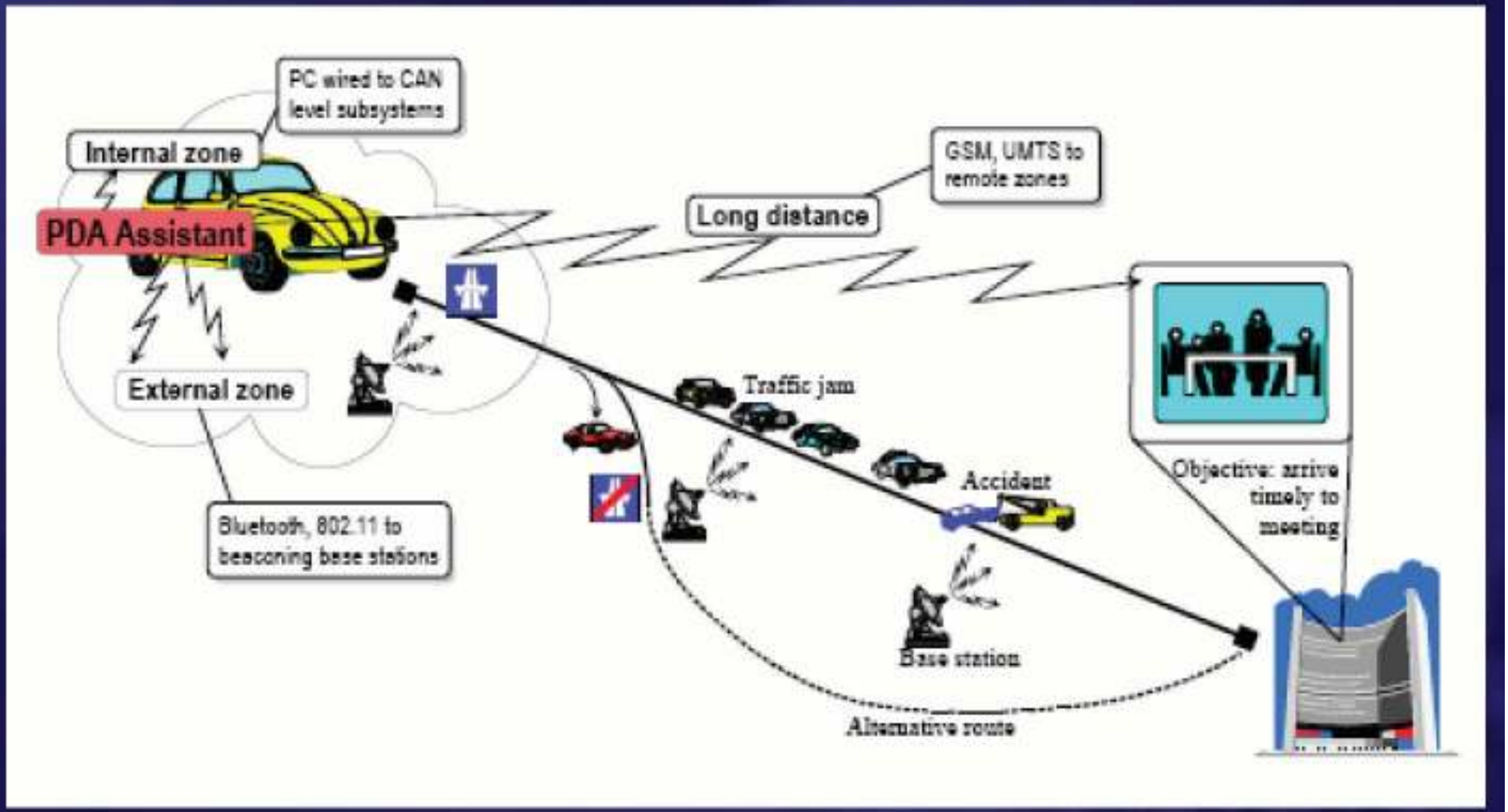
Some slides from an NSF program director presented at a recent meeting…

Digital Living *2010*

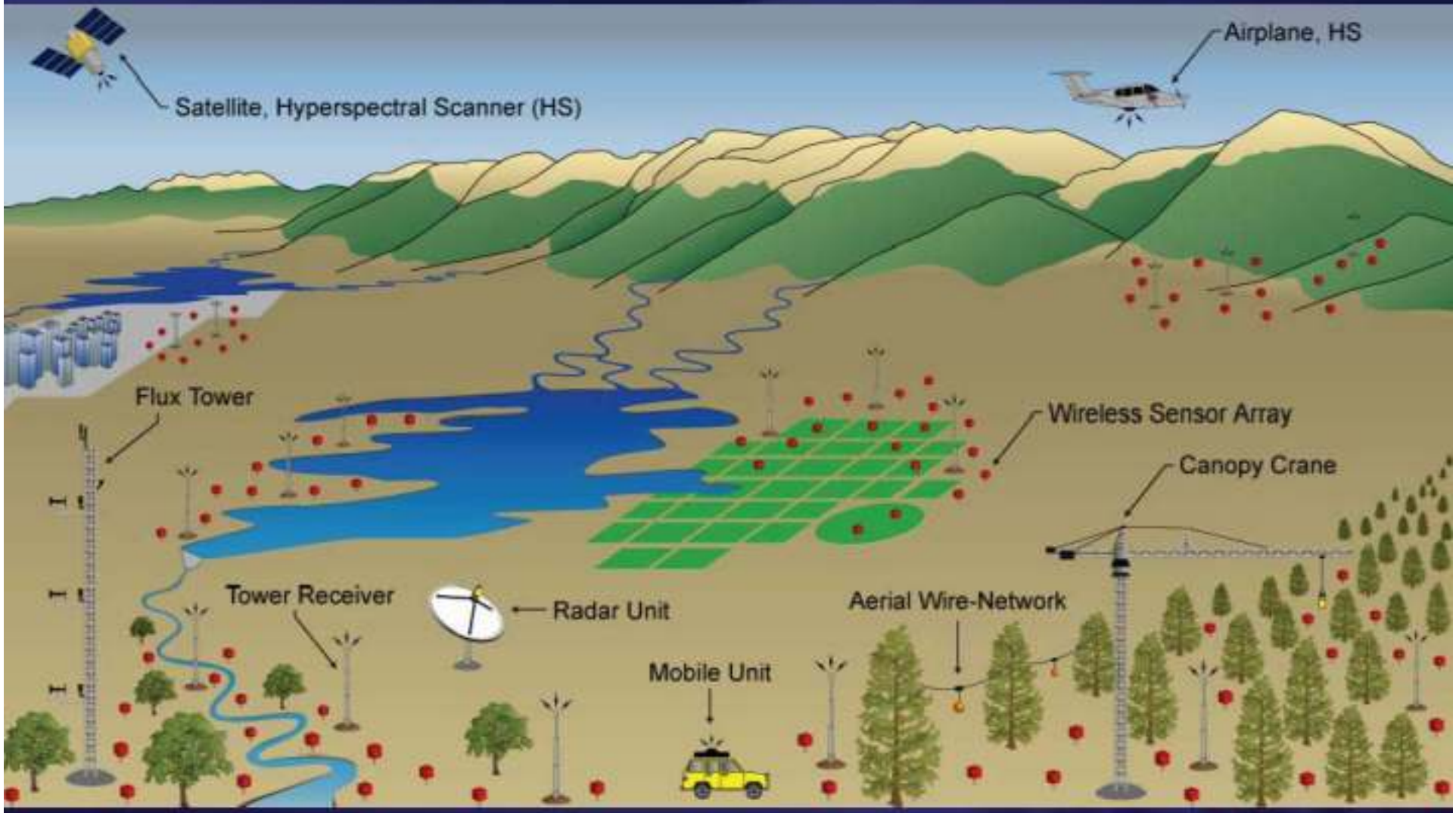
Tomorrow's users will be surrounded by pervasive devices, embedded sensors and systems… all connected to the Internet.



Networked Embedded Systems

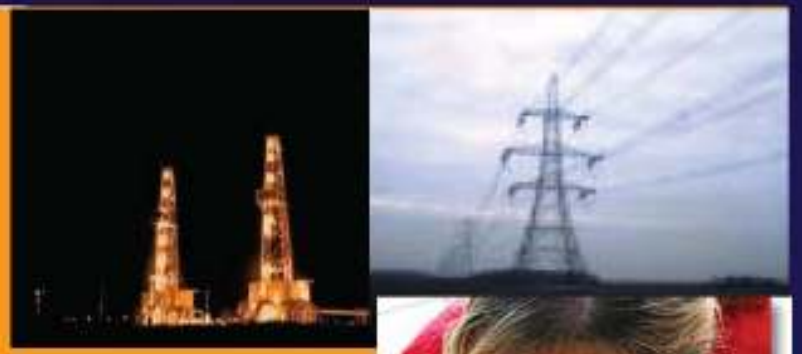


NEON:
National Ecological Observatory Network



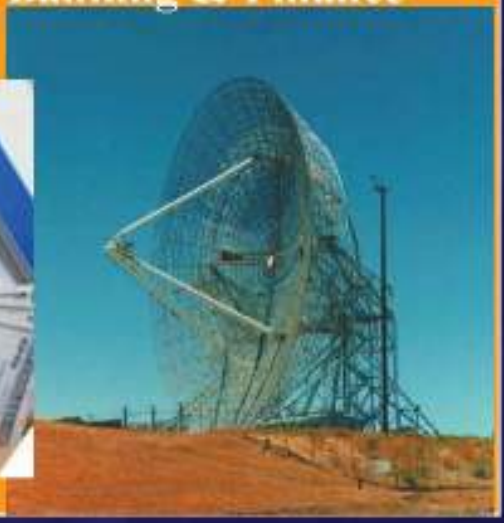
Network Centric Critical Infrastructures

Transportation



Essential Utilities

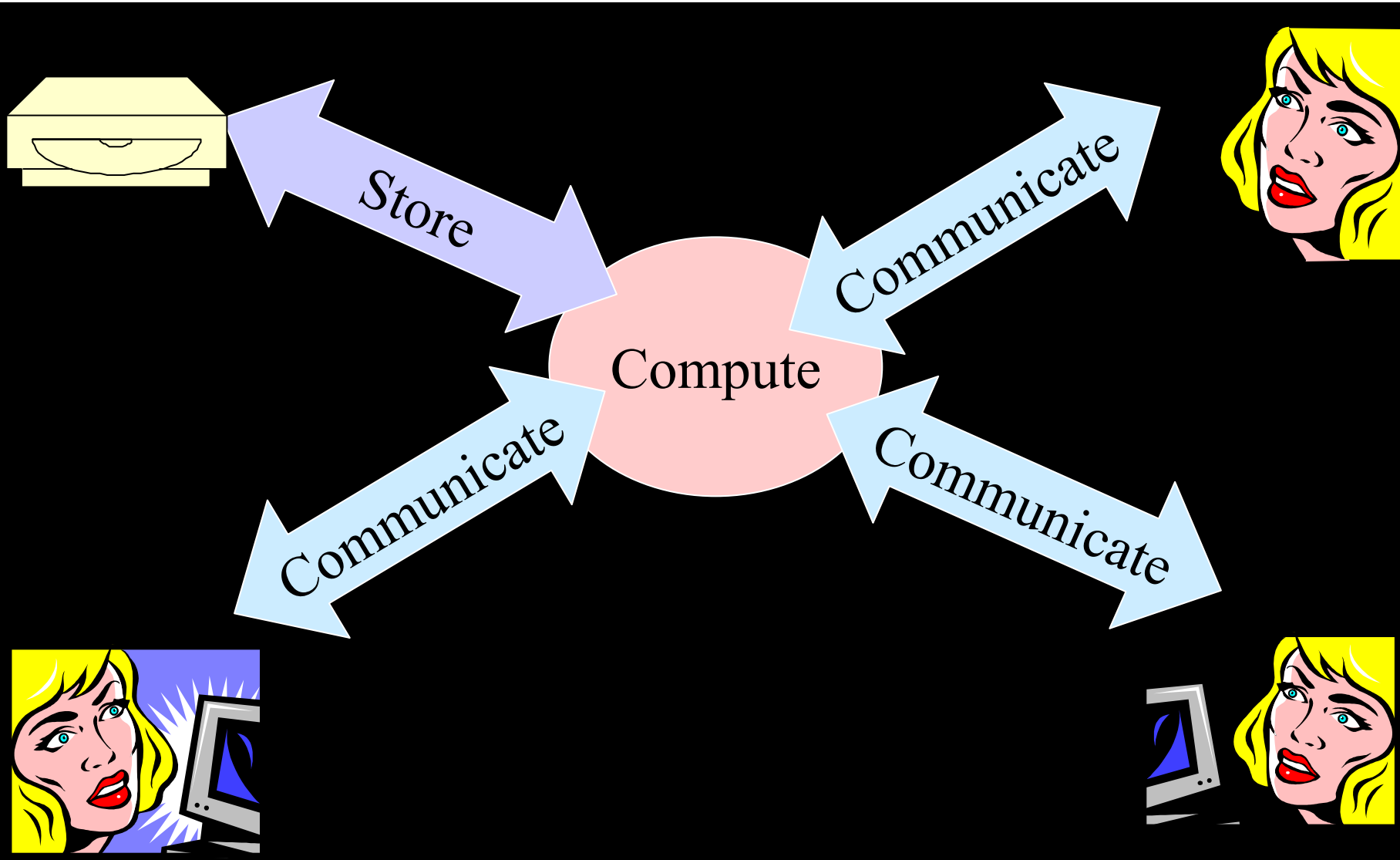
Telecommunications
Banking & Finance



The Internet* has become a critical information infrastructure.

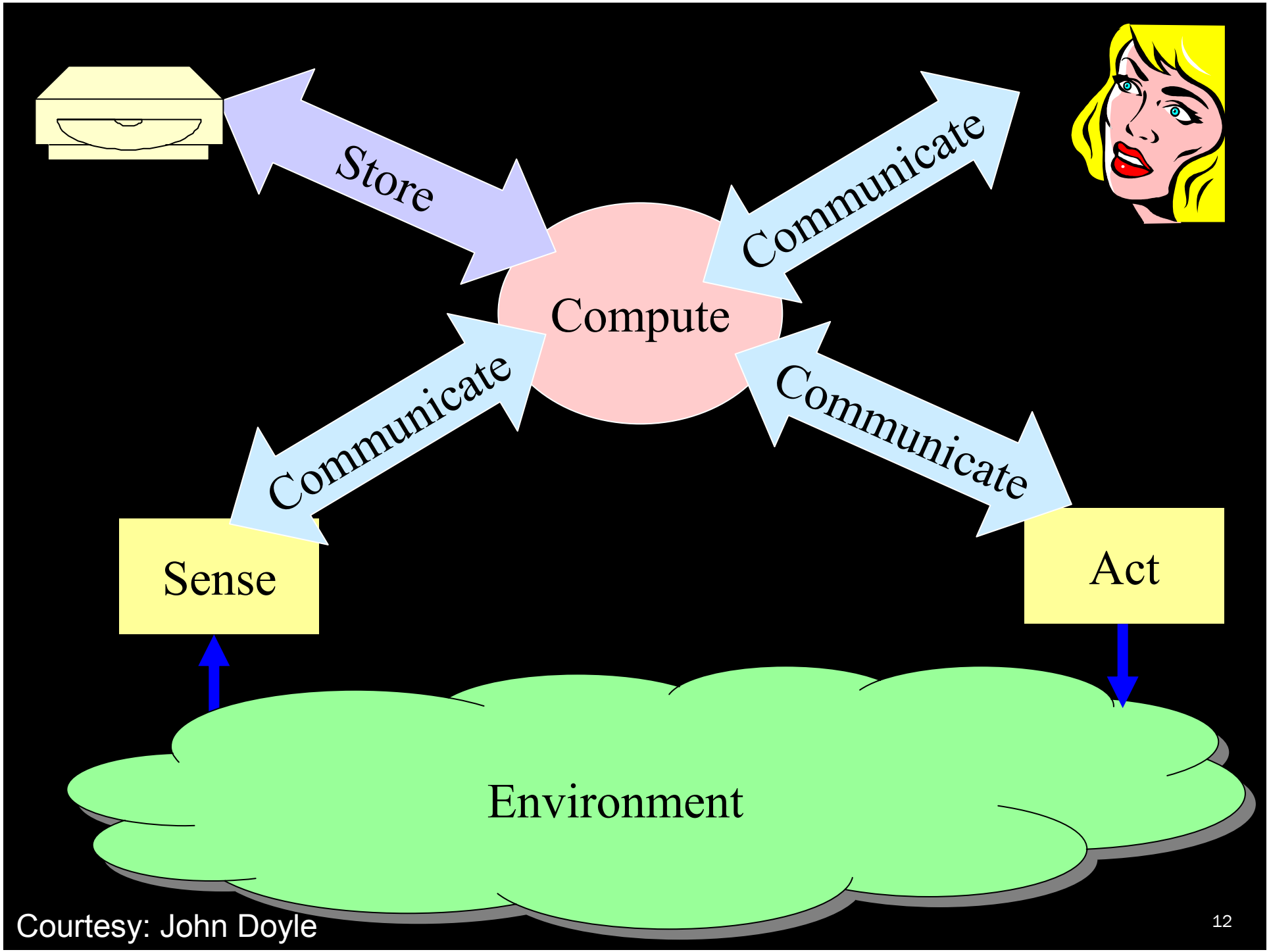
Our dependence on the Internet is only going to increase.

This will be amplified by a fundamental change in the way that we use the network.

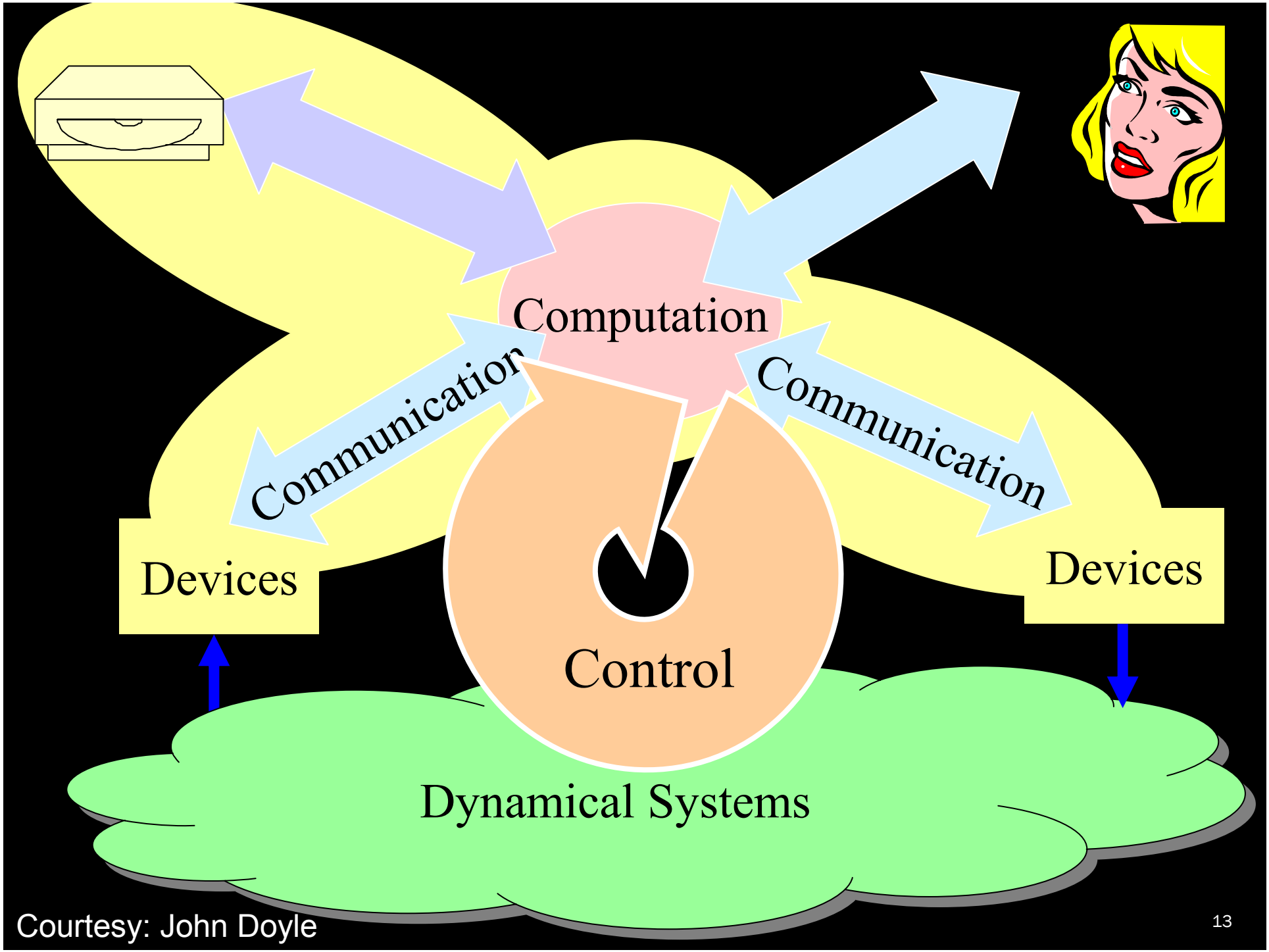


Communications and computing

Courtesy: John Doyle



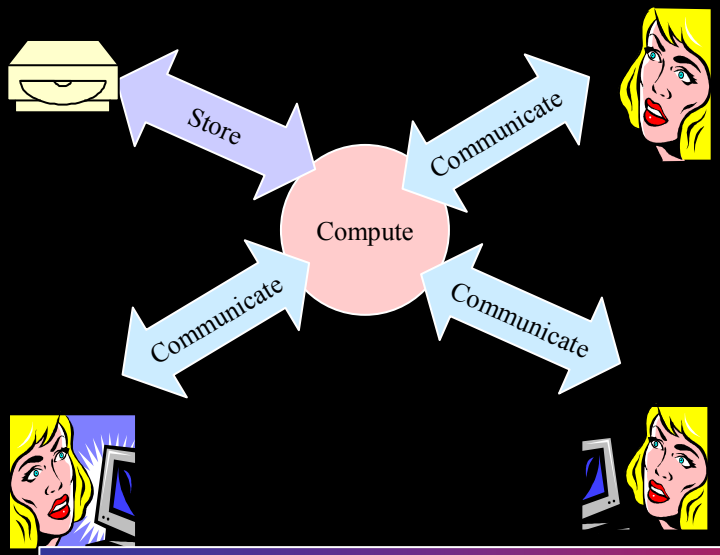
Courtesy: John Doyle



Courtesy: John Doyle

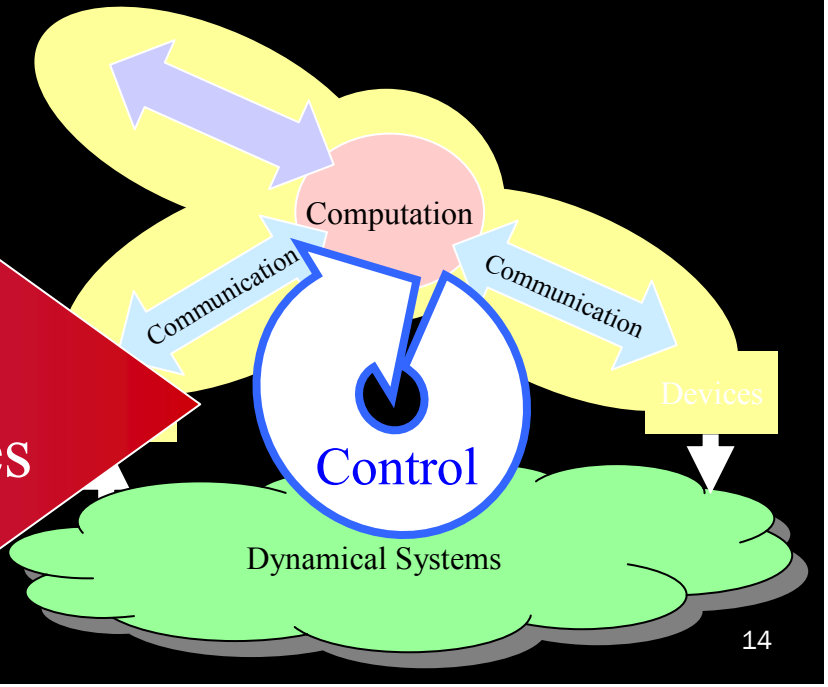
From

- Software to/from human
- Human in the loop



To

- Software to Software
- Full automation
- Integrated control, comms, computing
- Closer to physical substrate



- New capabilities & robustness
- New fragilities & vulnerabilities

Courtesy: John Doyle

Are we ready?

- This represents an enormous change, the impact of which is not fully appreciated
- Few, if any, promising methods for addressing this full problem
- Even very special cases have had limited theoretical support

Courtesy: John Doyle

The Internet* has become a critical information infrastructure.

The Internet has become a type of public utility
(like electricity or phone service) that underlies many important public and private services.

$\Rightarrow$ Internet disruptions have a "ripple effect" across the economy.

The Internet is a control system

for monitoring and controlling our physical environment.

$\Rightarrow$Hijacking the Internet can be even more devastating than interrupting it.

can we get there from here?

"...in the thirty-odd years since its invention, new uses and abuses, along with the realities that come with being a fully commercial enterprise, are pushing the Internet into realms that its original design neither anticipated nor easily accommodates."

"Freezing forevermore the current architecture would be bad enough, but in fact the situation is deteriorating. ... These architectural barnacles—unsightly outcroppings that have affixed themselves to an unmoving architecture—may serve a valuable short-term purpose, but significantly impair the long-term flexibility, reliability, security, and manageability of the Internet."

Source: "Overcoming Barriers to Disruptive Innovation in Networking", NSF Workshop Report, 2005.

NSF Future INternet Design (FIND)

- previous slides from NSF meeting 5 Dec 2005
- presentation by Guru Parulkar, NSF program director
  http://find.isi.edu/presentation_files/Guru_Parulkar-FIND-IMeeting-final.pdf
- launch initiative on Future INternet Design (FIND)
- overcome Internet ossification that is preventing innovation
- advocates a "clean slate" approach to Internet redesign

<u>NSF Organizational Hierarchy</u>:

Computer & Information Science & Engineering (CISE) Directorate

- Computer & Network Systems (CNS)
  - Networking Technology and Systems (NeTS)
    - Future INternet Design (FIND): Darleen Fisher, Allison Mankin
    - Networking of Sensor Systems (NOSS): David Du
    - Wireless Networks (WN): David Goodman
    - Networking Broadly Defined (NBD): Darleen Fisher

What do we want in a future information infrastructure?

What do we have with our current information infrastructure?

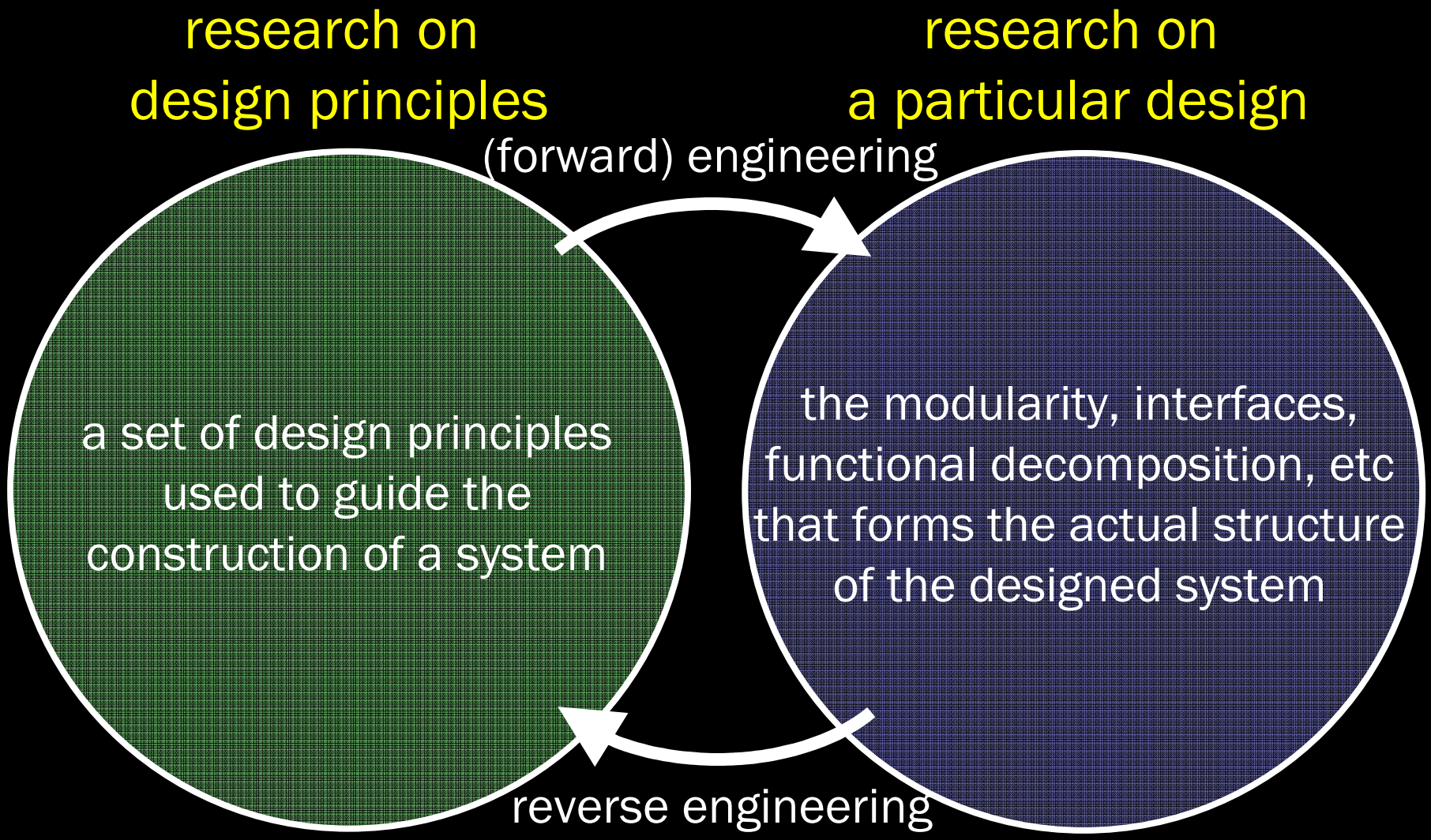
understanding what we already have

- the current Internet
  - "design" = tinkering/intuition + experimentation
  - a largely empirical view (e.g., validation via simulation or prototype)

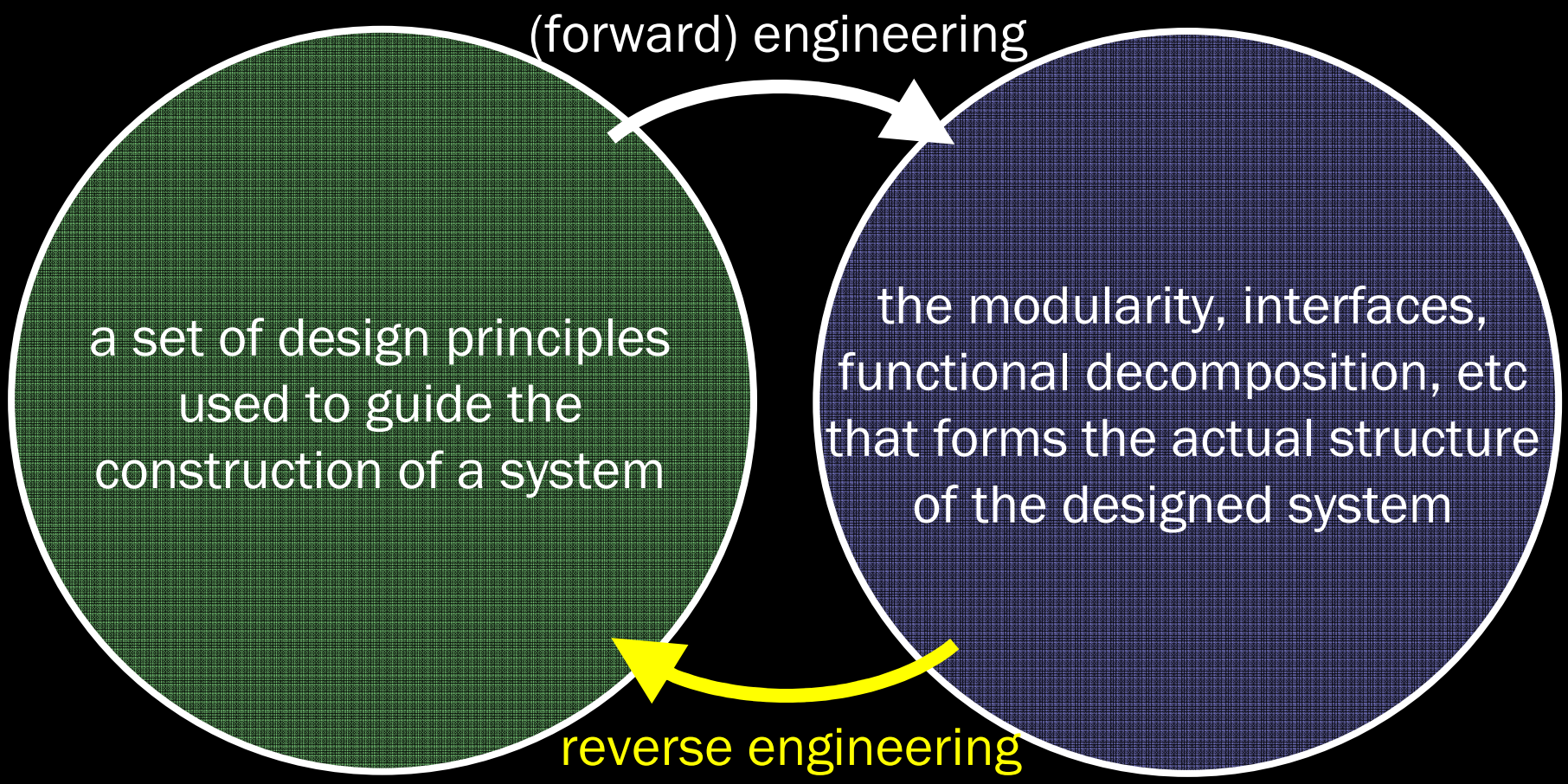
- the need for theory
  - better at "trial and error via deployment" than provable guarantees on performance, stability, etc.
  - how "good" is the current architecture?

- how might a "theory of architecture" drive future design?
  - next-generation wired Internet?
  - embedded/wireless systems?

studying Internet architecture



studying Internet architecture



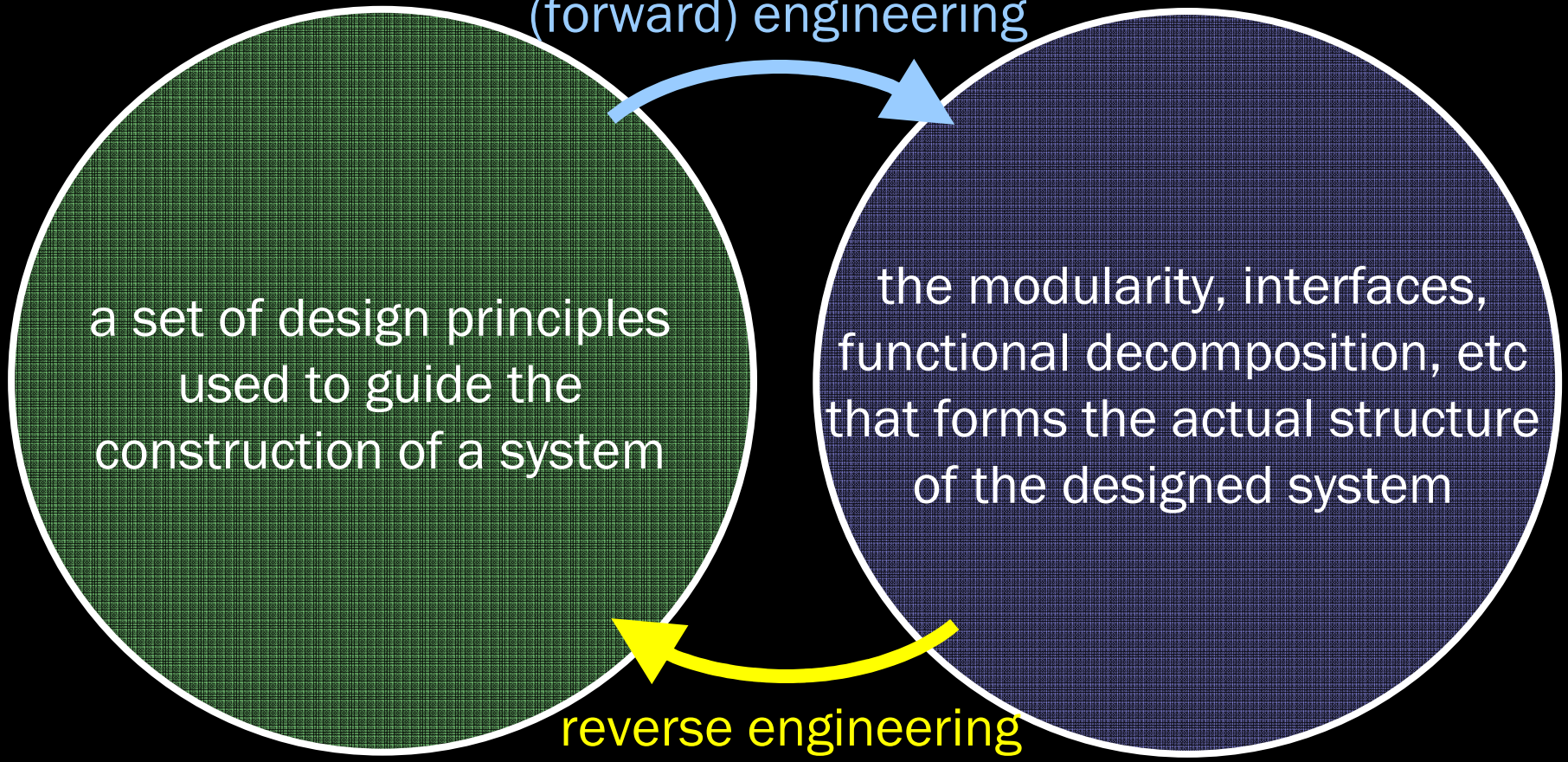
identify key design principles

study the implementation of the current Internet

studying Internet architecture

propose new (improved) designs & implementations

(forward) engineering



reverse engineering

identify key design principles

study the implementation of the current Internet

current Internet: dual decomposition

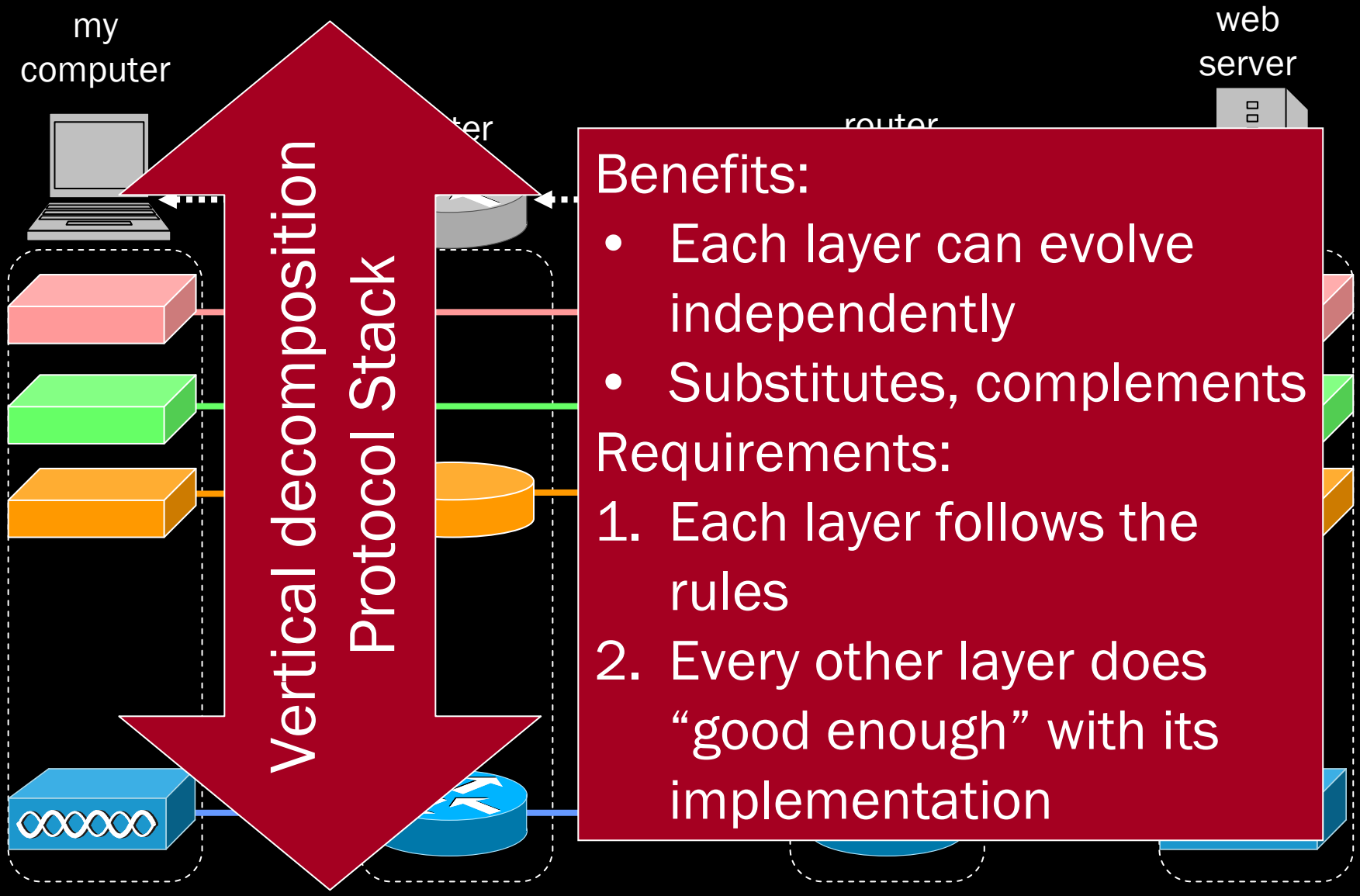
as a solution to a particular design problem:

- physical constraints on components
  - distance/delay, capacity
- functional constraints on the system as a whole
  - "X-ities": functionality, maintainability, adaptability, evolvability, etc.

design approach: *modularity*

- simplify the problem by breaking it up
- but still with provable properties as if it were an integrated whole

current Internet: dual decomposition



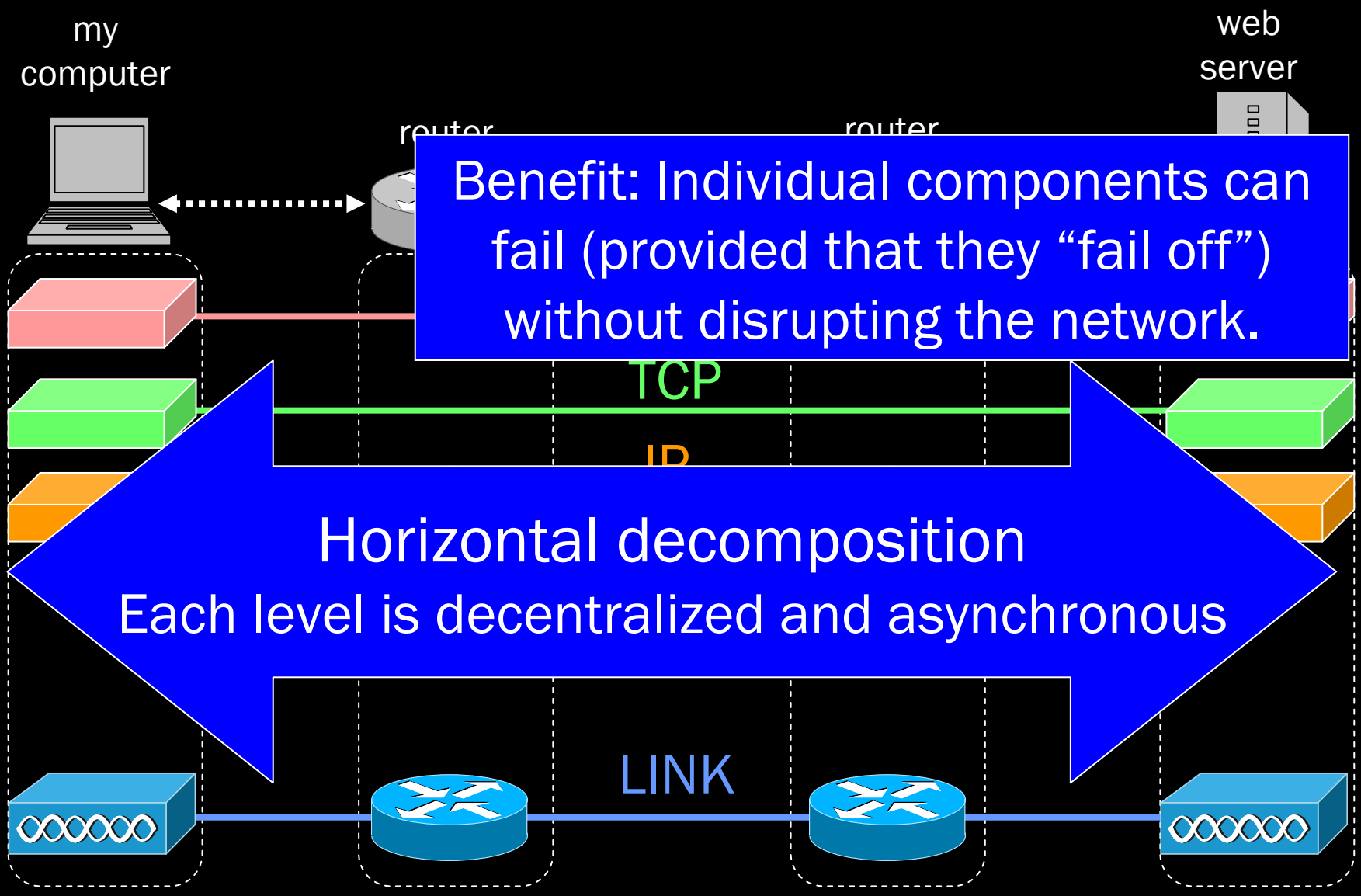
Benefits:

- Each layer can evolve independently
- Substitutes, complements

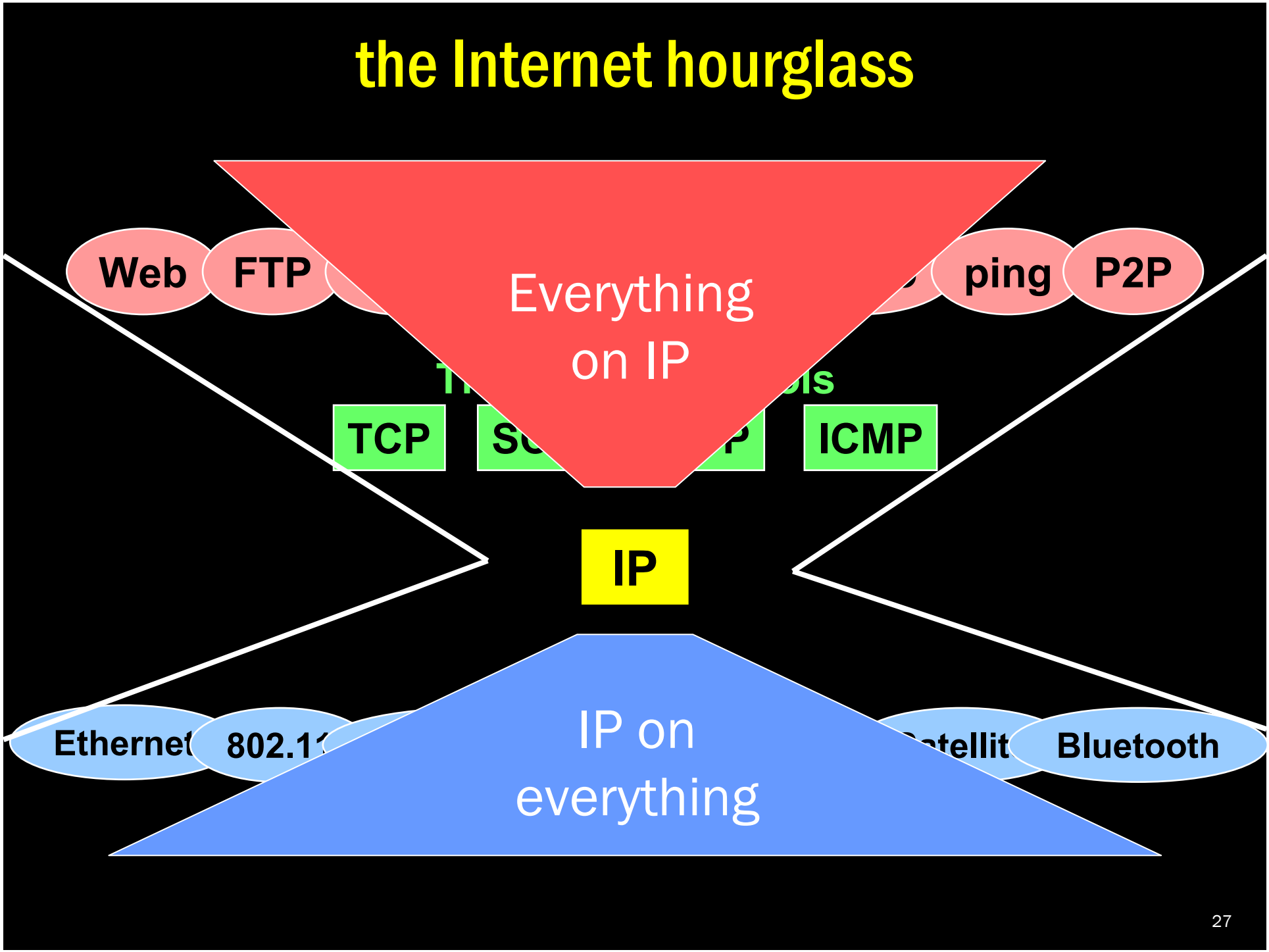
Requirements:

1. Each layer follows the rules
2. Every other layer does "good enough" with its implementation

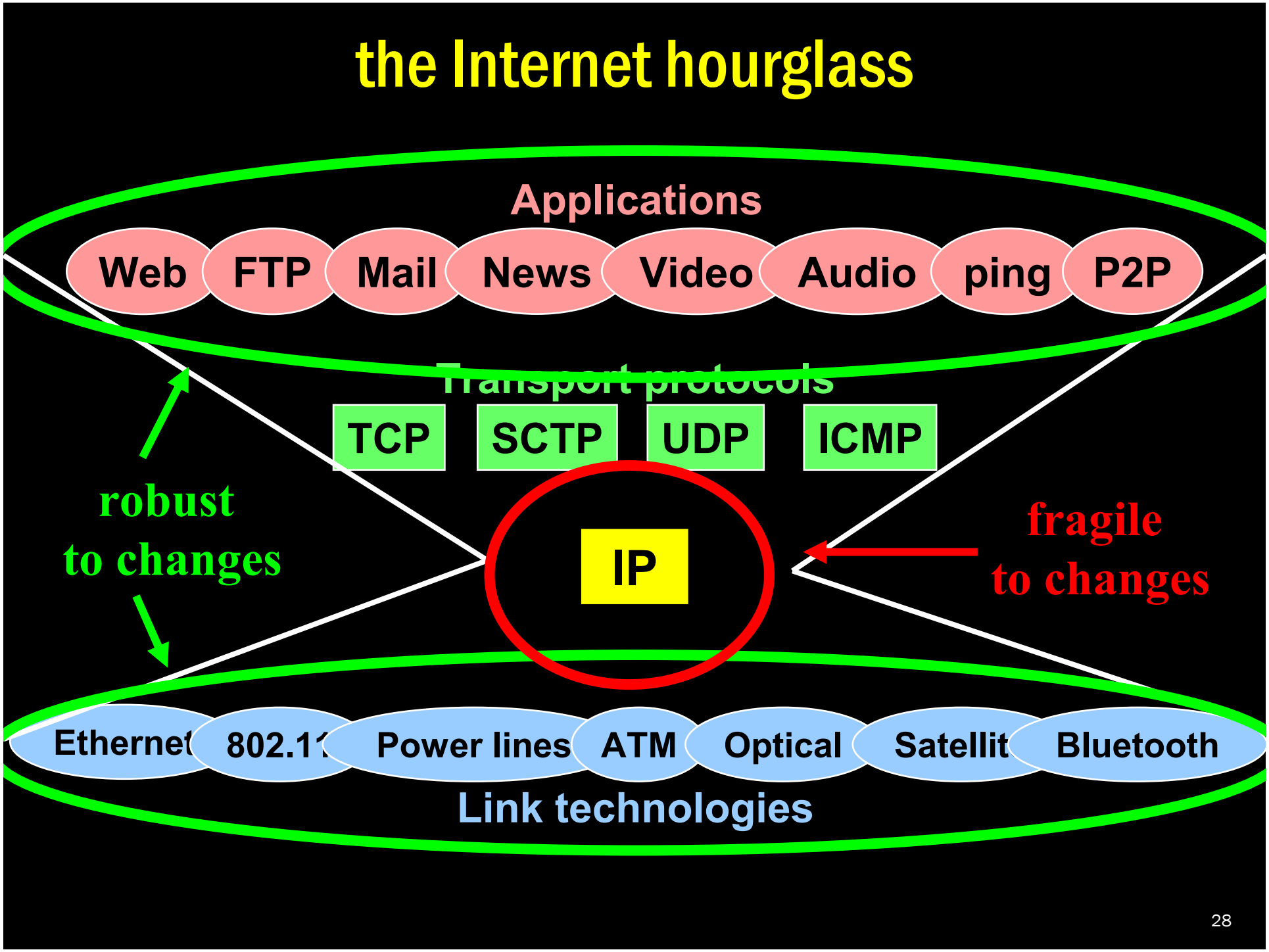
current Internet: dual decomposition



the Internet hourglass



the Internet hourglass



preliminary successes in reverse-engineering

- identifying common design principles
  - decomposition via layering and decentralization
  - universal organizational structures (e.g. hourglass)

- understanding "robust, yet fragile" nature
  - components can come and go: robust to loss or failure
  - BUT… fragile to misbehaving components

  - diverse applications / link technologies: evolvability
  - single routing protocol: fragile to change

What do we want in a future information infrastructure?

What if you could start over and build a new Internet?

What We Have

- Heterogeneity
- Open access
- Compatibility
- Evolvability*
- Anonymity
- Diverse Functionality
- Best Effort Service
- Robustness*
  - Best Effort Service
  - Component loss

Are these attributes important for a critical information infrastructure?

What We Have

- Heterogeneity
- Open access
- Compatibility
- Evolvability
- Anonymity
- Diverse Functionality
- Best Effort Service
- Robustness*
  - Best Effort Service
  - Component loss

What We Need

- Security
- Reliability
- Accountability
  - Clear responsibility
  - Auditability
- Management simplicity
- Limited functionality
- Economic self-sustainability

Are there tradeoffs that we might be willing to make?

Two Distinct Needs

- A public Internet
  - Embraces the ideals of the original Internet
  - A creative commons
  - Open access, anonymity (but at a price)

- A critical information infrastructure
  - Meets the emerging needs of society
  - Secure, reliable, performance guarantees (but at a price)

Is there any reason that they should be the same network?

Remembering History

- Strategic split of ARPANet and MILNet
- Different needs of each merited a split in which separate networks could be optimized to achieve different objectives

What do we want in a future information infrastructure?

A thought experiment

Presumptions

- Private networks (even excluding the military) are a significant portion of all data networks
- Most private networks tend to use public infrastructure somewhere (virtual separation)
- The ISP industry is in tough economic times
- There is a large amount of excess capacity (e.g. dark fiber)
- Most of the technology for a secure network already exists
- The government and corporations are be willing to spend money to solve the problem

A Crazy Idea?

Have the federal government commission a few major ISPs to build and operate an "Internet alternative"

- Semi-private, with restricted access
- Security and reliability as primary objectives
- Built from the best of existing technology
- Strict deployment standards
- Leverage existing and unused capacity
- Limited, but guaranteed functionality
- Exist alongside current "best effort" Internet
- Clear responsibility
  - Licensed users
  - Audit trails
- Mandated use by other critical infrastructure providers
- Available by application to corporations (for a fee)
- Goal: long-term economic self-sustainability

Is this simply GovNet all over again?

Analogy: The Interstate Highway System

- The Interstate Highway system was developed on top of the existing road network
- It did not replace the pre-existing highway system - it complemented it and extended its utility

- Its vastly superior effectiveness and affordability made it irresistible to users.
- Its successful adoption was the result of strong economic incentives for key support industries (gas stations, hotels, restaurants) that benefited tremendously from it.

- While desirable to all, a national system of interstate roads could only be effectively coordinated through federal efforts
- The federal government had to work closely in partnership with the highway owners and operators (the states)
- Roles/responsibilities had to be worked out for each stakeholder: owners and operators, vehicle manufacturers, and users

The Interstate Highway System (2)

The Highway System has clearly defined roles and responsibilities:

- For vehicle manufacturers: there are standards for the types of vehicles that are allowed to travel on our highways.
  - Vehicles must pass safety tests (e.g. crash tests)
  - Vehicles must pass environmental tests (e.g. emissions)
  - Vehicles must follow norms (e.g. left-side steering wheels)
- For owners and operators: there are standards for the way in which the infrastructure must be built and maintained.
  - Roads must comply with standard widths, slopes, surface grades.
  - Roads and bridges must satisfy safety standards (e.g. for earthquakes)
  - Roads must follow norms (e.g. lane markings, signage, lighting)
- For users: there are standards for traveling on the highways
  - Users must obtain a vehicle operator license, updated regularly. There are different classes of operator licenses, based on vehicle type
  - Users must follow prescribed traffic laws (e.g. speed limits)
  - There are norms for vehicle operation (e.g. use of signals, right of way)

The Interstate Highway System (3)

The Interstate Highway System should not be taken as a literal model for building a Future Internet, however…

. . . it can serve as a template thinking about the types of roles and responsibilities that might need to be defined

. . . it may provide inspiration for the types of relationships that the federal government might need to develop with infrastructure owners and operators

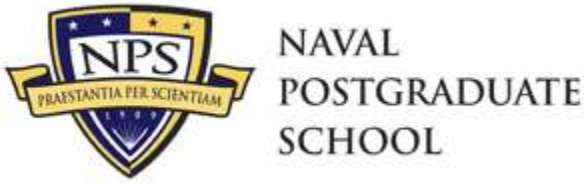
. . . it may yield insight into methods for creating the appropriate economic incentives for the various stakeholders

. . . it can serve as an example for the incremental development, deployment, and adoption of a critical infrastructure

. . . it demonstrates how the federal government can facilitate a management framework that is effective without heavy-handed regulation.

What do we want in a future information infrastructure?

David Alderson
Operations Research Department
Naval Postgraduate School



MS&E 91si: U.S. National Cybersecurity
November 16, 2006