Cyber Security In-The-Large

Ed Lazowska

Bill & Melinda Gates Chair in
Computer Science & Engineering
University of Washington

October 12, 2005

Cyber security in this course

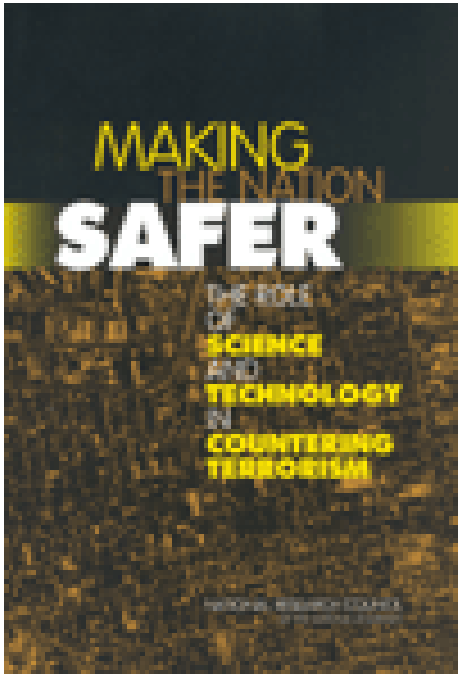
- October 5: computer security primer
- October 12: cyber security and critical infrastructure protection (financial, urban, port)
- "Red Team" project
- November 9: attacks (ddos, extortion, phishing, spam, botnet reselling, spyware)
- November 16: defenses (incentive-based strategies, suppressing Internet outbreaks, intrusion detection systems)

- November 23: defenses (software quality, white-hat attacks, exposing/publicizing vulnerabilities)
- November 30: information awareness (IT and intelligence)
- December 7: cyberforensics (what constitutes evidence of cybercrime, and how can it be obtained)
- [Term Project]

Tonight

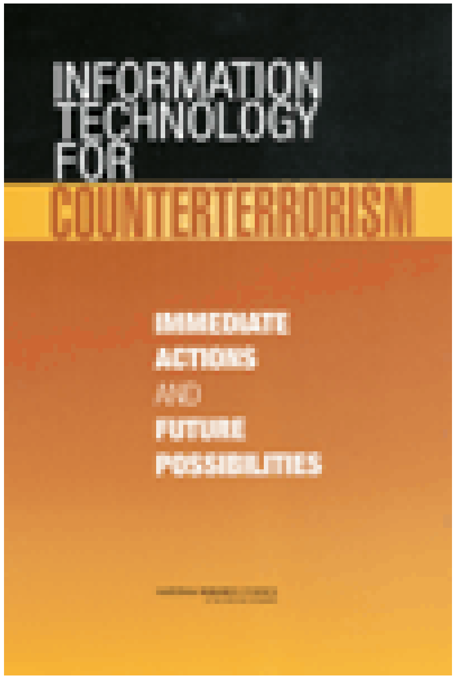
- Cyber Security In-The-Large
  - Ed Lazowska, UW
- The Resiliant Enterprise
  - Phil Venables, Goldman Sachs
- Cyber Security at the Local Level: The City of Seattle and the Port of Seattle
  - Kirk Bailey, UW (ex - City of Seattle) and Ernie Hayden, Port of Seattle

Cyber Security In-The-Large



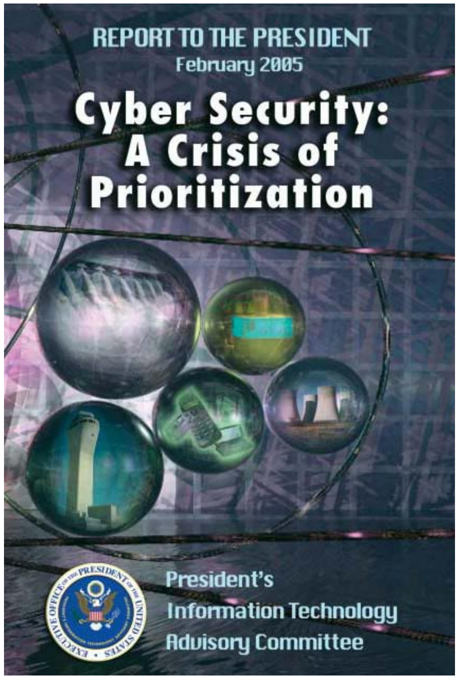
MAKING THE NATION SAFER

THE ROLE OF SCIENCE AND TECHNOLOGY IN COUNTERING TERRORISM



INFORMATION TECHNOLOGY FOR COUNTERTERRORISM

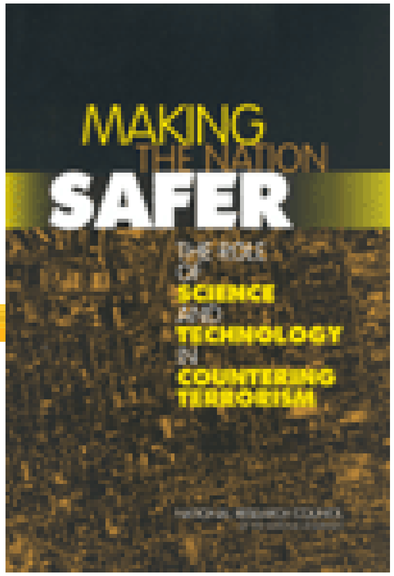
IMMEDIATE ACTIONS AND FUTURE POSSIBILITIES



REPORT TO THE PRESIDENT
February 2005

Cyber Security: A Crisis of Prioritization

President's
Information Technology
Advisory Committee


MAKING
THE NATION
SAFER
THE ROLE
OF
SCIENCE
AND
TECHNOLOGY
IN
COUNTERING
TERRORISM

INFORMATION TECHNOLOGY FOR COUNTERTERRORISM
IMMEDIATE ACTIONS AND FUTURE POSSIBILITIES

- Focus: catastrophic terrorist acts
  - Thousands of lives
  - Billions of dollars
  - Patient, smart, disciplined adversaries with ample resources (people, money, time)

- IT is essential to all of the nation’s critical infrastructures
  - nuclear power plants, dams, electric power grid, air traffic control system, financial institutions
  - corporate operations
  - distribution of food and energy
  - embedded computing in all devices and environments; networking of these systems
  - technological underpinning of all communication systems

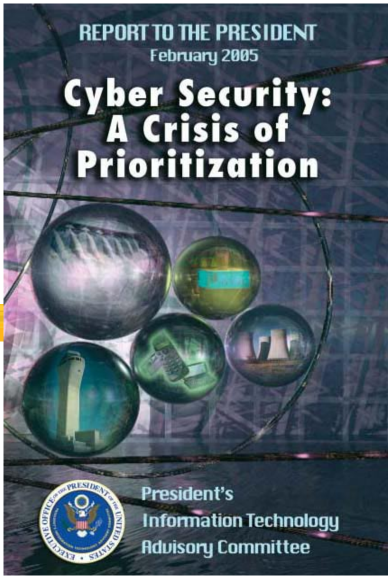
- IT also is a critical infrastructure itself
- IT is a critical component in responding to attacks
  - Emergency response, information dissemination
- IT can serve as an amplifier of physical attacks
  - Widen damage (false information, delayed response)
  - Heighten terror (misinformation)
- IT can help prevent attacks
  - Information awareness

- Thus, IT can be:
  - a target
  - a vehicle for launching or exacerbating an attack on other critical infrastructures
  - a way to interfere with attempts to respond (including spreading FUD)
  - a way to prevent, detect, and mitigate attacks
- A target, a weapon, a defense
- A key component of our "infrastructure system" - including the organizational context

- Short-term recommendation 1: Develop a program that focuses on the communications and computing needs of emergency responders
  - State of the art IT
  - C3I (command, control, communications, and intelligence) systems upgrades for emergency responders

- Short-term recommendation 2: Promote the use of best practices in security in all relevant public and private organizations
  - Deploy adequate security tools
  - Utilize red-team penetration attacks
  - Require strong authentication
  - Employ improved configuration validation tools, etc.
  - Model good security behavior in the federal government

- Long-term recommendation: Invest in R&D in:
  - Information and network security
  - IT and C3I for emergency response
  - Information fusion
  - Privacy and confidentiality
  - Robots, sensors, simulation
  - Organizational aspects of security
  - Human-centered design

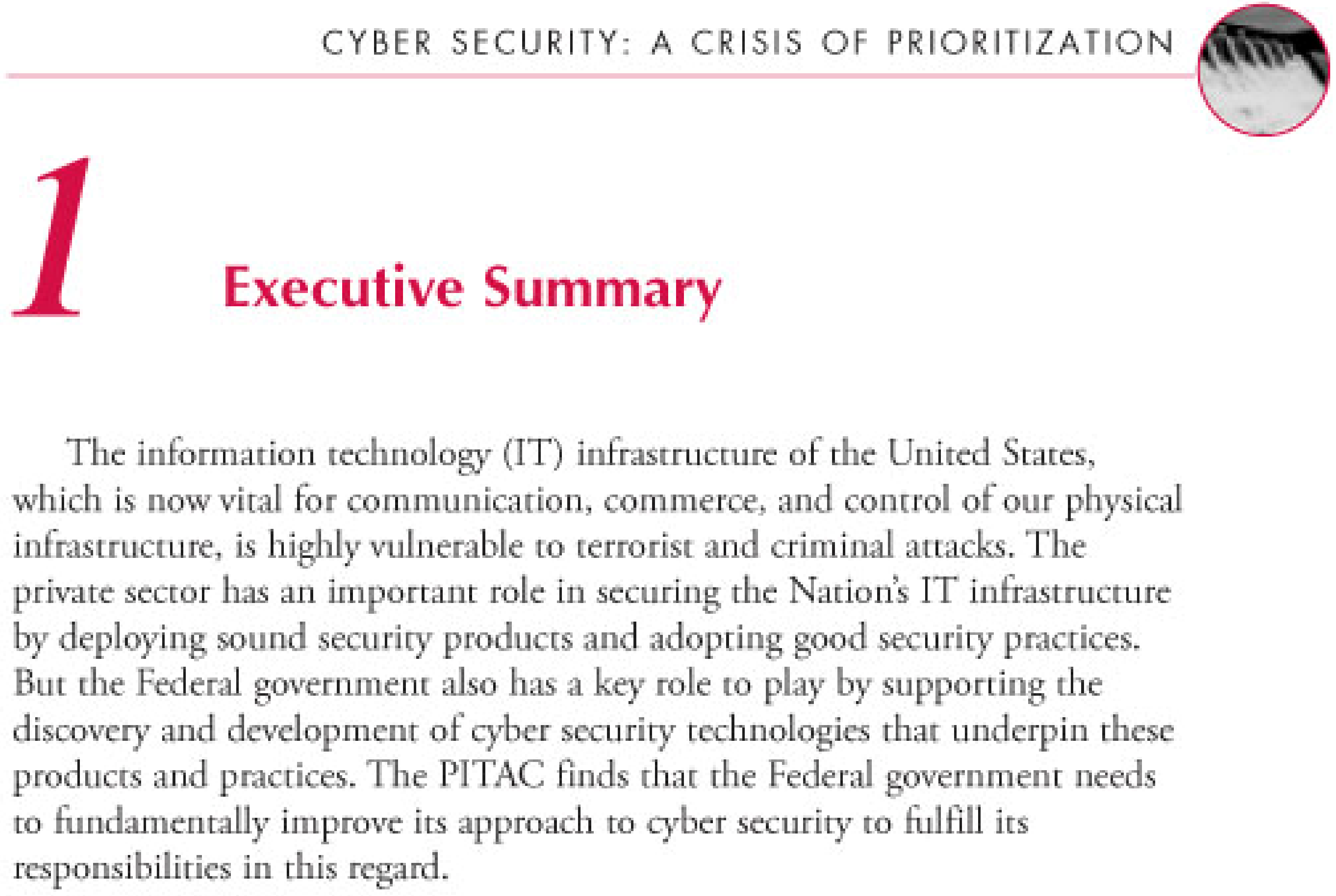


REPORT TO THE PRESIDENT
February 2005

Cyber Security:
A Crisis of
Prioritization

President's
Information Technology
Advisory Committee

- The concern is not that eBay will be inaccessible!
- Rather, the concern is that *IT systems are in the control loop of every element of the nation's critical infrastructure* – the electric power grid, the air traffic control grid, the financial grid, etc.
- This constitutes a significant vulnerability

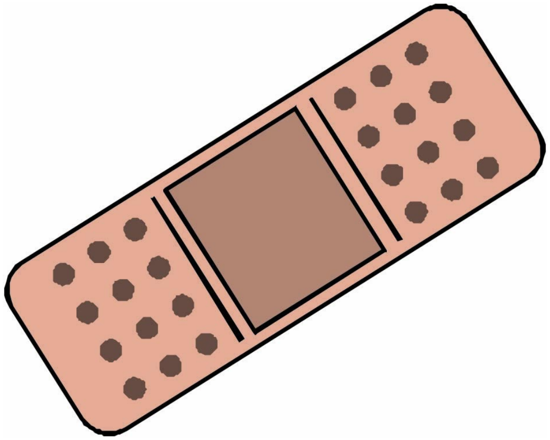


CYBER SECURITY: A CRISIS OF PRIORITIZATION

1 Executive Summary

The information technology (IT) infrastructure of the United States, which is now vital for communication, commerce, and control of our physical infrastructure, is highly vulnerable to terrorist and criminal attacks. The private sector has an important role in securing the Nation's IT infrastructure by deploying sound security products and adopting good security practices. But the Federal government also has a key role to play by supporting the discovery and development of cyber security technologies that underpin these products and practices. The PITAC finds that the Federal government needs to fundamentally improve its approach to cyber security to fulfill its responsibilities in this regard.

Original text: "The committee finds that the U.S. government is largely failing in its responsibilities in this regard."



Finding 1

The Federal R&D budget provides inadequate funding for fundamental research in civilian cyber security.

Recommendation 1

The NSF budget for fundamental research in civilian cyber security should be increased by $90 million annually. Funding for fundamental research in civilian cyber security should also be substantially increased at other agencies, most notably DHS and DARPA. Funding should be allocated so that at least the ten specific areas listed in the “Cyber Security Research Priorities” section of this chapter are appropriately addressed. Further increases in funding may be necessary depending on the Nation’s future cyber security posture.

Finding 2

The Nation's cyber security research community is too small to adequately support the cyber security research and education programs necessary to protect the United States.

Recommendation 2

The Federal government should intensify its efforts to promote recruitment and retention of cyber security researchers and students at research universities, with a goal of at least doubling the size of the civilian cyber security fundamental research community by the end of the decade. In particular, the Federal government should increase and stabilize the funding for fundamental research in civilian cyber security, and should support programs that enable researchers to move into cyber security research from other fields.

Finding 3

Current cyber security technology transfer efforts are not adequate to successfully transition Federal research investments into civilian sector best practices and products.

Recommendation 3

The Federal government should strengthen its cyber security technology transfer partnership with the private sector. Specifically, the Federal government should place greater emphasis on the development of metrics, models, datasets, and testbeds so that new products and best practices can be evaluated; jointly sponsor with the private sector an annual interagency conference at which new cyber security R&D results are showcased; fund technology transfer efforts (in cooperation with industry) by researchers who have developed promising ideas or technologies; and encourage Federally supported graduate students and postdoctoral researchers to gain experience in industry as researchers, interns, or consultants.

Finding 4

The overall Federal cyber security R&D effort is currently unfocused and inefficient because of inadequate coordination and oversight.

Recommendation 4

The Interagency Working Group on Critical Information Infrastructure Protection should become the focal point for coordinating Federal cyber security R&D efforts. This working group should be strengthened and integrated under the Networking and Information Technology Research and Development (NITRD) Program.

- The nation is perilously under-invested in fundamental research in civilian cyber security
  - Work that discovers fundamentally new security architectures, rather than improved band-aids
  - Work that takes advantage of the talent of the nation's full research community
  - Work that impacts the civilian infrastructure and its technologies (upon which all else, including the military, relies)

- DHS
  - Simply doesn't get it!
    - 90% of S&T budget is for deployment, vs. research
      - DHS is generally ignoring research
    - <2% of budget is for cyber security
  - DHS is generally ignoring the nation's infrastructure
    - The agency is focused almost entirely on WMD threats (bio, chem, rad) against individuals

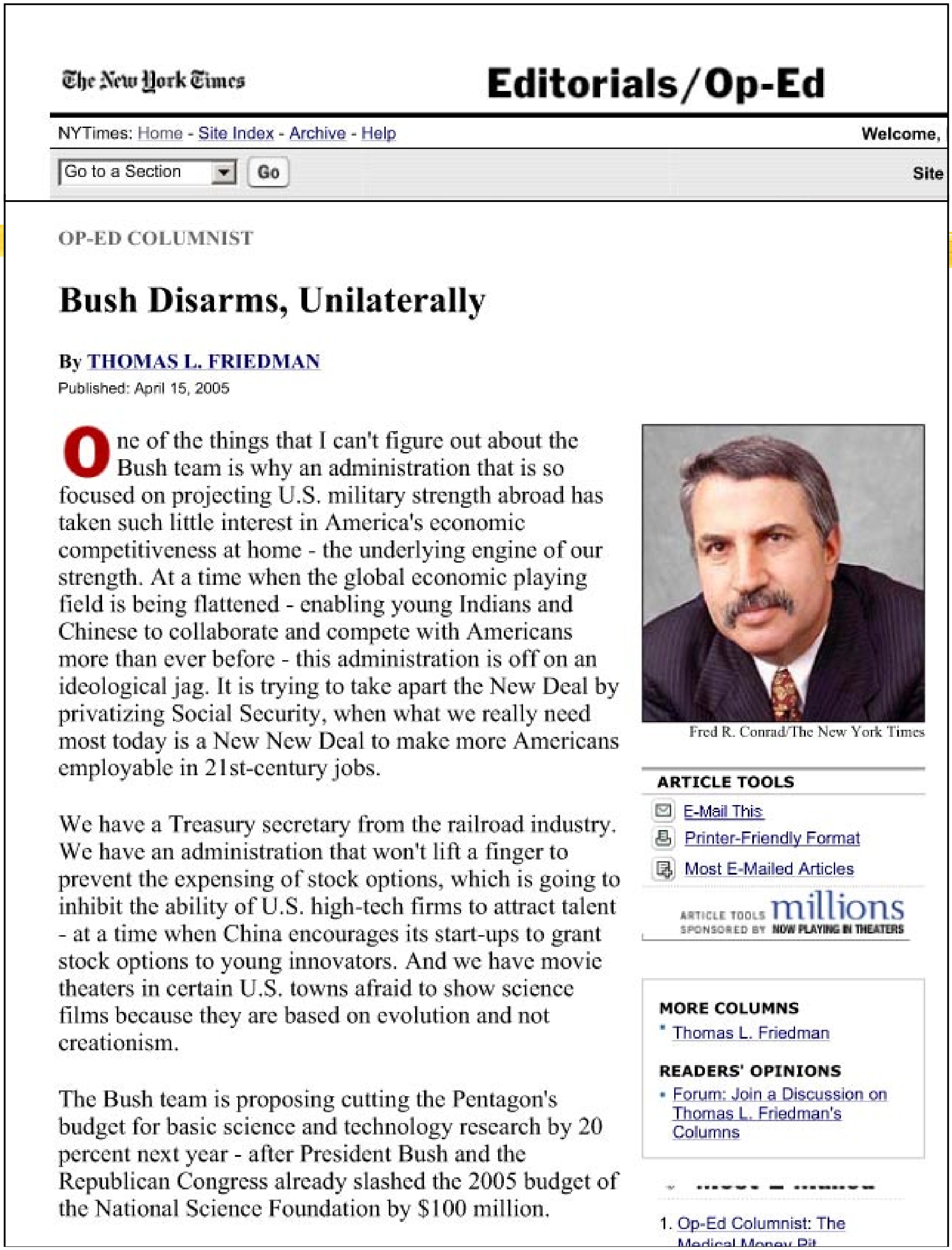
- DARPA
  - New program starts in cyber security have been classified
    - Precludes participation by the university community
      - Eliminates many of the best researchers
      - No students
    - Reduces impact on commercial networks and systems – upon which much of the government, and much of the nation's critical infrastructure, and much of the military, rely

- NSF
  - FY04 Cyber Trust program, 9/21/2004
    - Funded **8%** of proposals
      - 32 of 390
        - 2 of 25 Center proposals
        - 12 of 135 Team proposals
        - 18 of 230 Small Group proposals
    - Awarded **6%** of requested funds
      - $31.5M of $510M

Multi-agency coordination is not working!

- The Federal IT coordinating process (NCO, etc.) should recognize the gaps that exist, and compensate

Beyond IT



The New York Times **Editorials/Op-Ed**

OP-ED COLUMNIST

Bush Disarms, Unilaterally

By THOMAS L. FRIEDMAN

Published: April 15, 2005

One of the things that I can't figure out about the Bush team is why an administration that is so focused on projecting U.S. military strength abroad has taken such little interest in America's economic competitiveness at home - the underlying engine of our strength. At a time when the global economic playing field is being flattened - enabling young Indians and Chinese to collaborate and compete with Americans more than ever before - this administration is off on an ideological jag. It is trying to take apart the New Deal by privatizing Social Security, when what we really need most today is a New New Deal to make more Americans employable in 21st-century jobs.

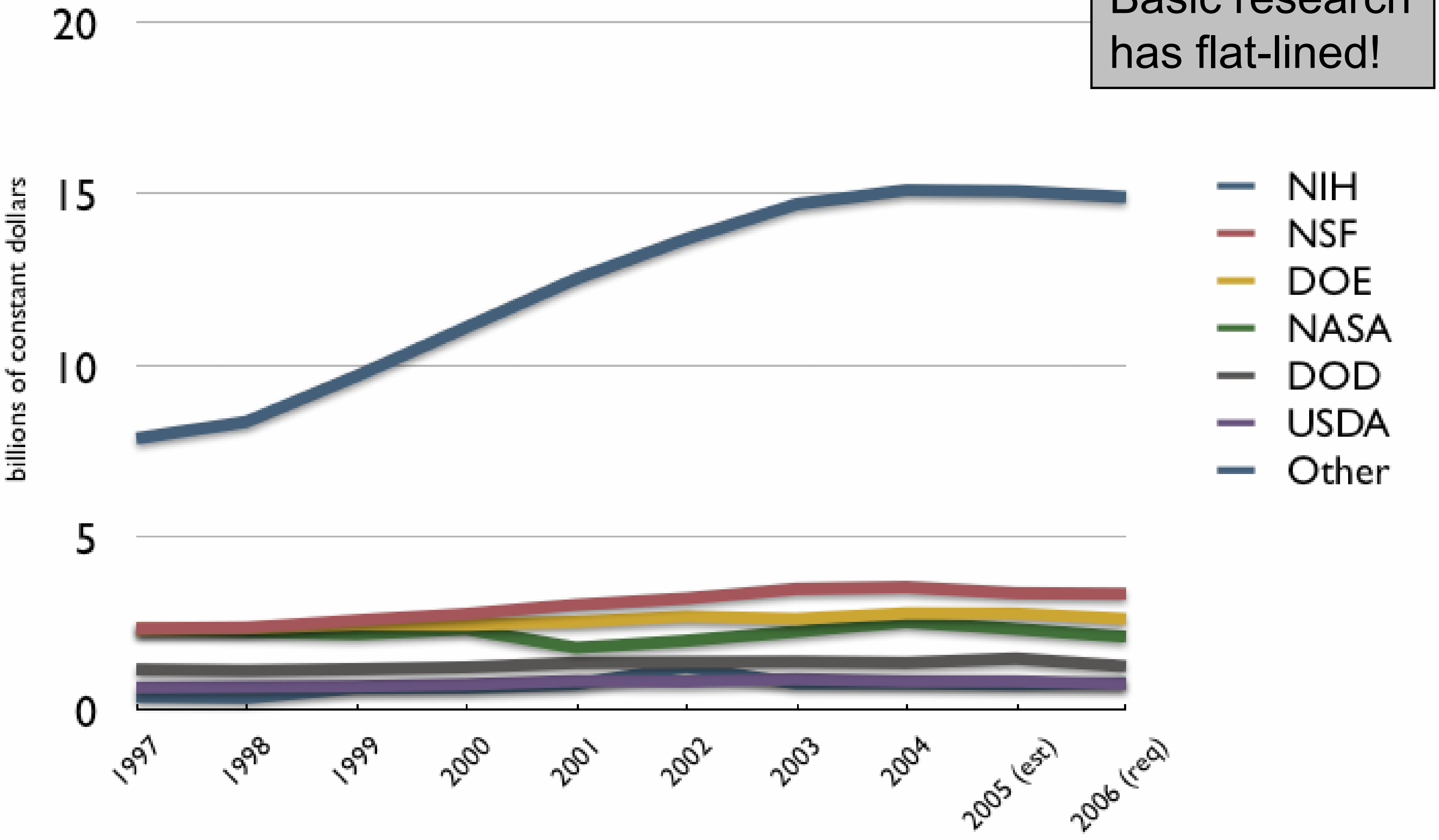
We have a Treasury secretary from the railroad industry. We have an administration that won't lift a finger to prevent the expensing of stock options, which is going to inhibit the ability of U.S. high-tech firms to attract talent - at a time when China encourages its start-ups to grant stock options to young innovators. And we have movie theaters in certain U.S. towns afraid to show science films because they are based on evolution and not creationism.

The Bush team is proposing cutting the Pentagon's budget for basic science and technology research by 20 percent next year - after President Bush and the Republican Congress already slashed the 2005 budget of the National Science Foundation by $100 million.

Fred R. Conrad/The New York Times

ARTICLE TOOLS
E-Mail This
Printer-Friendly Format
Most E-Mailed Articles
ARTICLE TOOLS SPONSORED BY millions NOW PLAYING IN THEATERS
MORE COLUMNS
Thomas L. Friedman
READERS' OPINIONS
Forum: Join a Discussion on Thomas L. Friedman's Columns
1. Op-Ed Columnist: The Medical Money Pit

Trends in Basic Research, by Agency
FY 1997 - 2006



Basic research has flat-lined!

Source: AAAS Reports I through XXX, based on OMB and agency R&D budget data.
Includes conduct of R&D and R&D facilities.
Constant dollar conversions based on OMB's GDP deflators from the FY 2006 budget.

SPEED
LIMIT
25