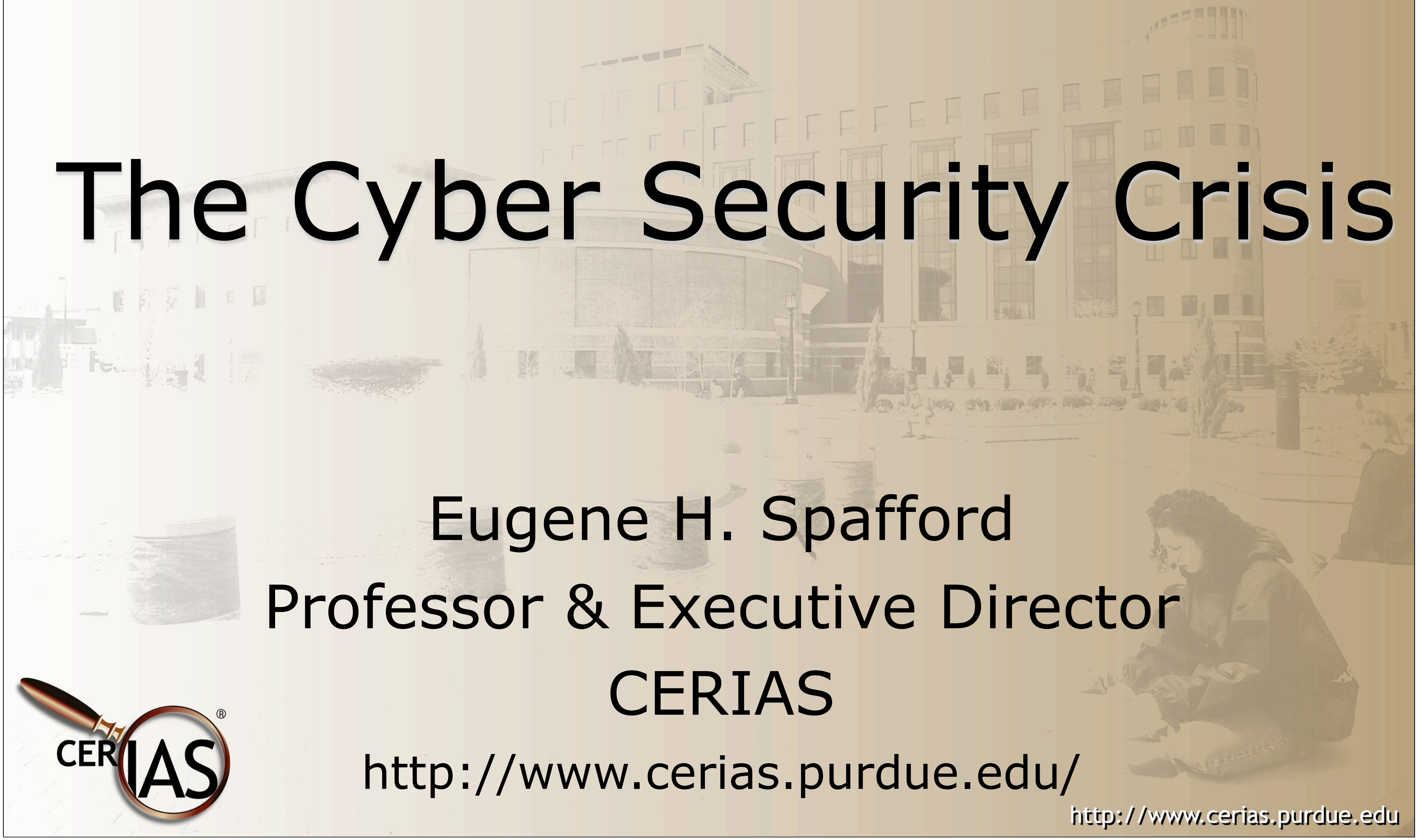


The Cyber Security Crisis

Eugene H. Spafford
Professor & Executive Director
CERIAS
http://www.cerias.purdue.edu/

The State of Cybersecurity

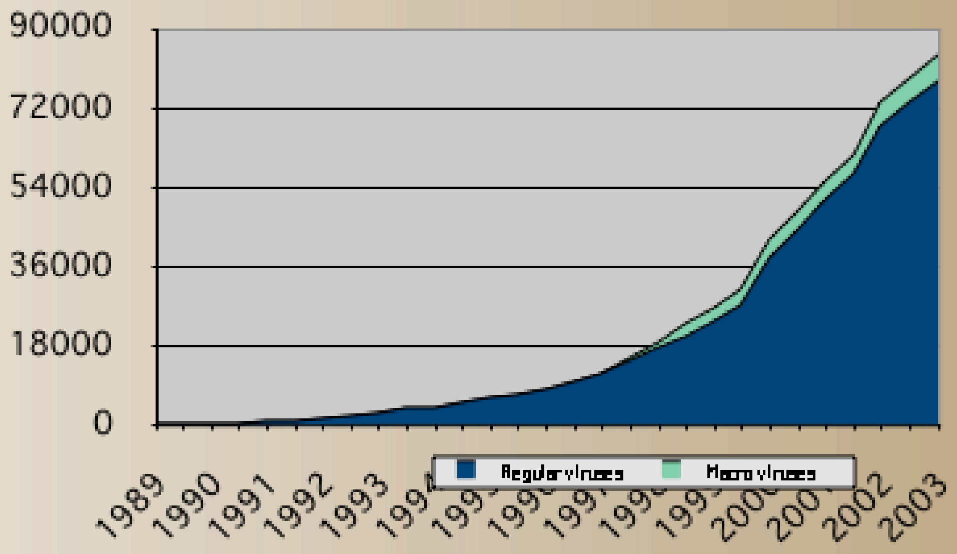
- Overwhelming vulnerabilities
  - About 4000 in each of 2003, 2004
  - Almost 4600 in 2005
  - New ones reported @ 20 per day
  - 3/4 were simple design flaws
- Well over 120,000 known viruses & worms
  - New ones reported at a rate of 50 per day
- Large-scale attacks doubling per year

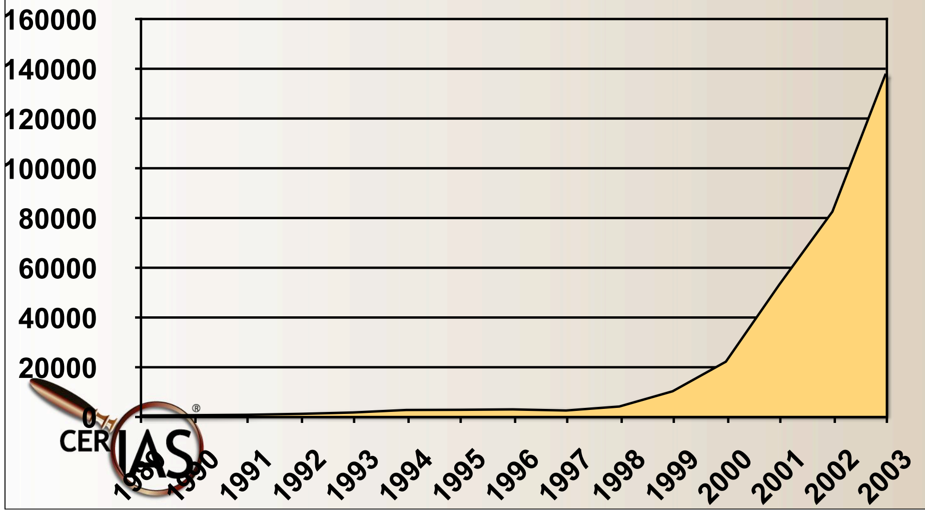
The Problem is Growing

- Damages "hidden" but mounting
  - Viruses alone projected at over $60B damage per year
  - Worldwide losses from all causes in excess of $105 Billion
  - Spam is 90% of email at some ISPs
- Organized cyber crime is increasing
- Identity theft is #1 growth crime in US
- 1 Billion online users; 2 billion by 2015

Recent Trends

Reported Viruses





Attacks Reported
by CERT

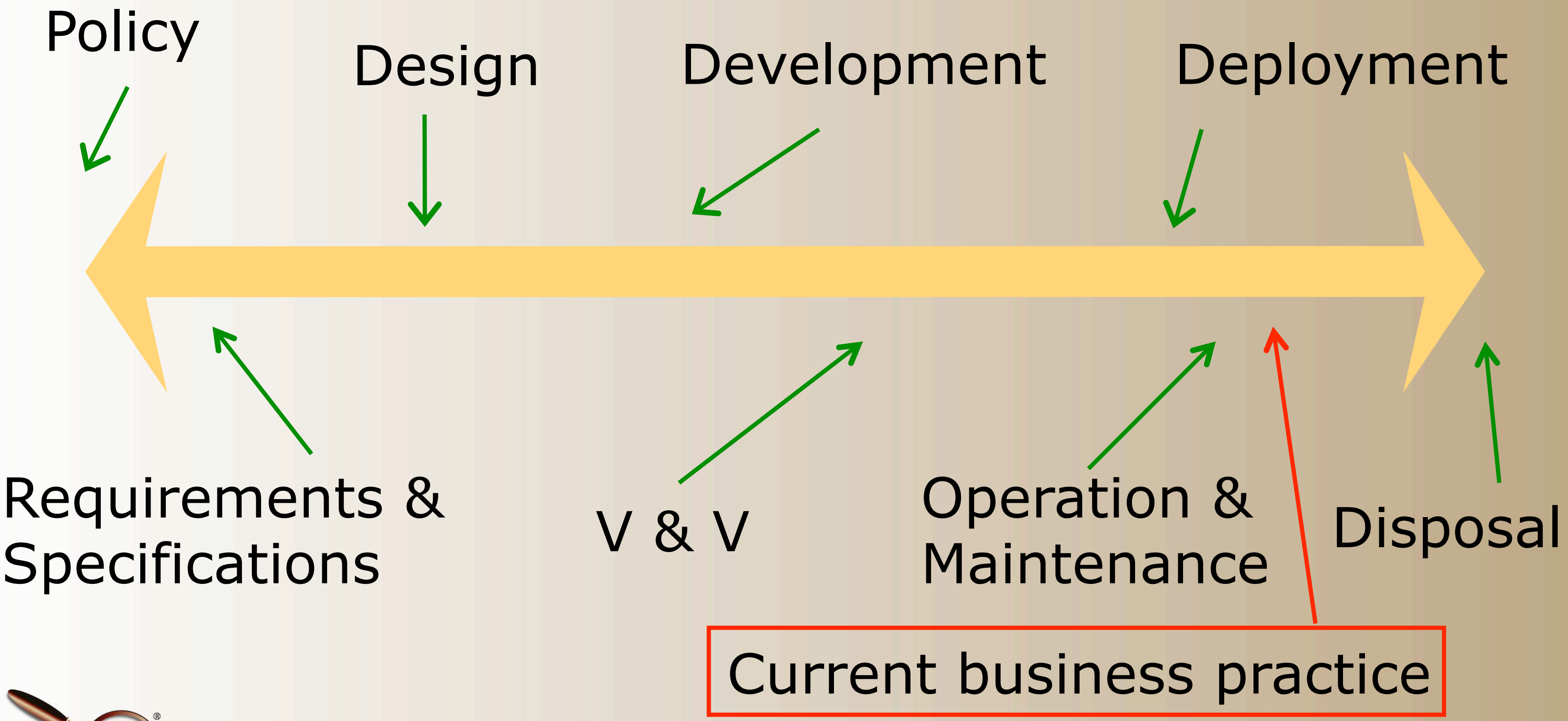
Why?

Why is our information security bad, and getting worse?

Design is unsound

- Increasing features & size of platforms
- Not based on secure design principles
- Coded by untrained personnel
- Confusing & unnecessary options
- Inconsistent configurations
- Forced by revenue cycles

Where We Currently Assure



Policy

Design

Development

Deployment

Requirements & Specifications

V & V

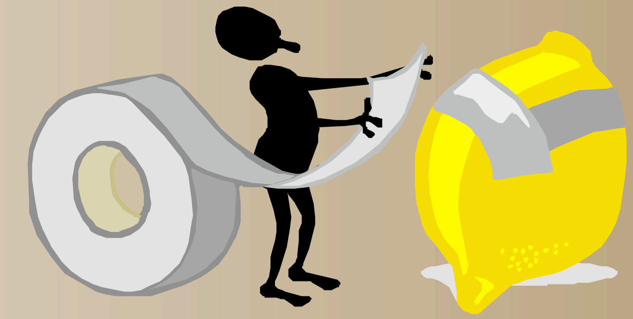
Operation & Maintenance

Disposal

Current business practice

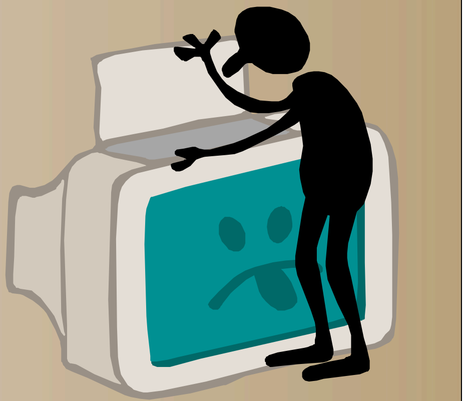
Operation is Unsafe

- Culture of patching
- Overly homogenous
- Acceptance of failures
- Myth of general purpose
- Myth of the perimeter



Insufficient Expertise

- Infosec requires more than CS
- Too few educational programs
- Insufficient support of R&D training
- Mistaking hacking for expertise
- Work overload



Major Failing #1

Failing to understand the problem

It’s the information, not the computer!

Original had copyrighted cartoon. Reproduction would not be fair use.

Major Failing #2

Failing to understand the threat.

Related to not understanding the motives and methods of the attackers.

Major Failing #3

Failing to include the people

Original had copyrighted cartoon. Reproduction would not be fair use.

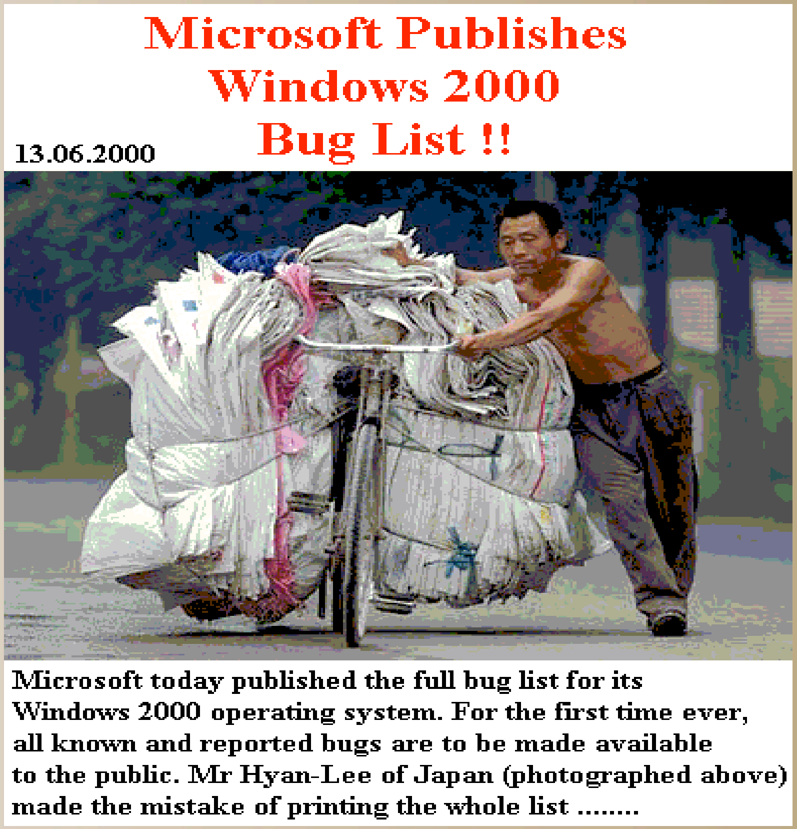
Major Failing #4

- Failure to build to a sound design.

- Too much accommodation of bad legacy code.

Major Failing #5

Placing too much trust in market pressure to provide highly-trustable systems … and then not using the market to good effect!



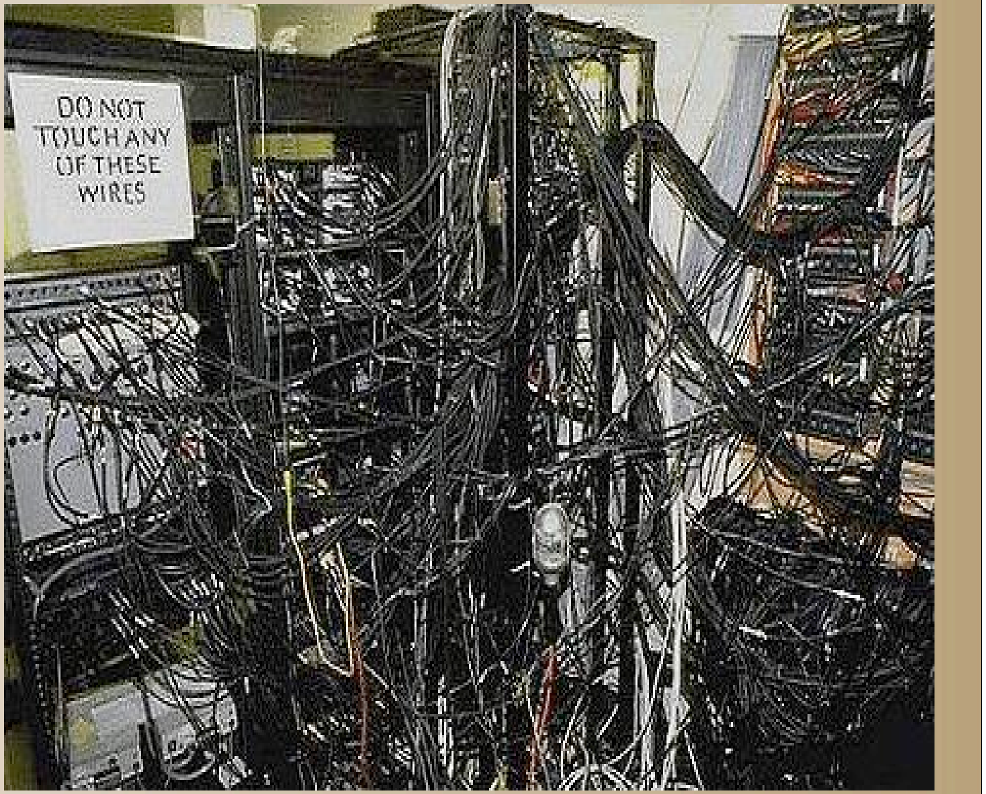
Microsoft Publishes Windows 2000 Bug List !!

13.06.2000

Microsoft today published the full bug list for its Windows 2000 operating system. For the first time ever, all known and reported bugs are to be made available to the public. Mr Hyan-Lee of Japan (photographed above) made the mistake of printing the whole list ....

Major Failing #6

Relying on patching instead of on getting it right the first time.



Major Failure #7

A failure to protect holistically.

Point protection is necessary but not sufficient.

"The chain is no weaker than its strongest link"
Photo by ToHell, 2003-09-23 in Slagsta, SE

Major Failing #8

- Failure to provide any adequate deterrence in addition to protection
    - lack of tools
    - lack of funding
    - lack of priority
    - international

Original had copyrighted cartoon. Reproduction would not be fair use.

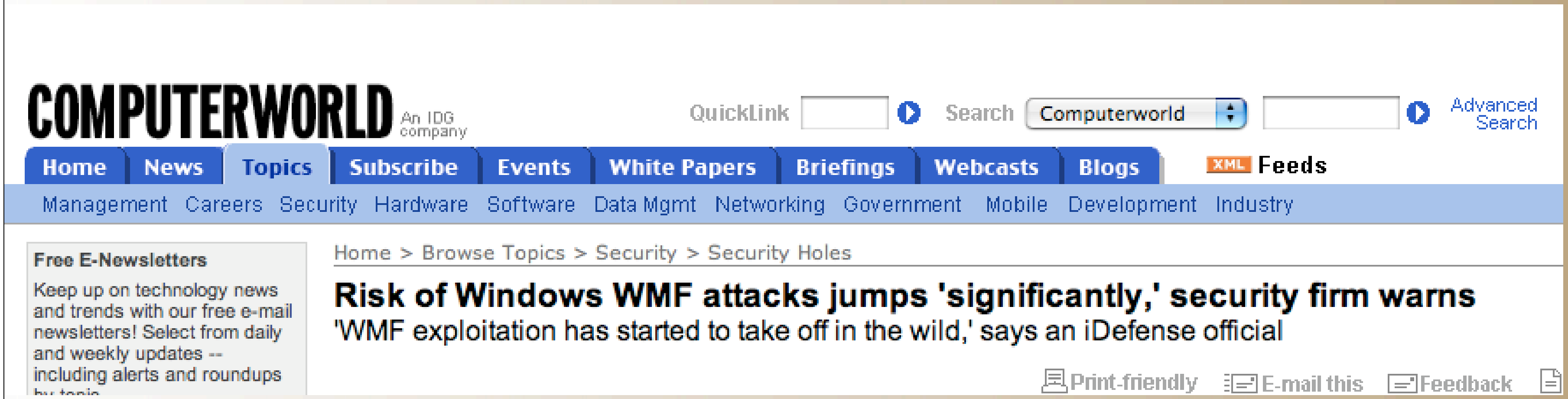
Major Failing #9

- Too much information is kept out of the hands of people who can use it
  - Company reticence
  - Over-classification

Original had copyrighted cartoon. Reproduction would not be fair use.

Who Can We Depend On?

The Vendors?



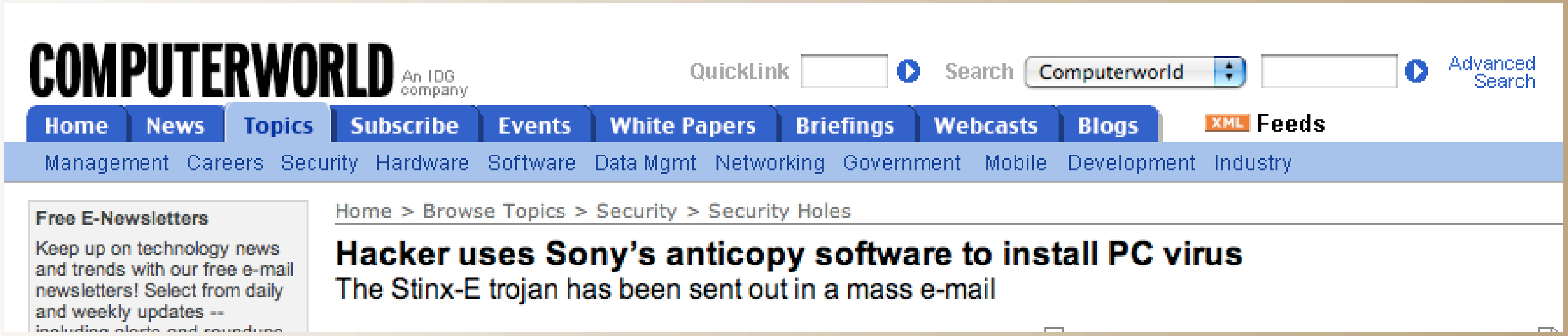
Free E-Newsletters

Keep up on technology news and trends with our free e-mail newsletters! Select from daily and weekly updates -- including alerts and roundups

Home > Browse Topics > Security > Security Holes

Risk of Windows WMF attacks jumps 'significantly,' security firm warns

'WMF exploitation has started to take off in the wild,' says an iDefense official



Free E-Newsletters

Keep up on technology news and trends with our free e-mail newsletters! Select from daily and weekly updates --

Home > Browse Topics > Security > Security Holes

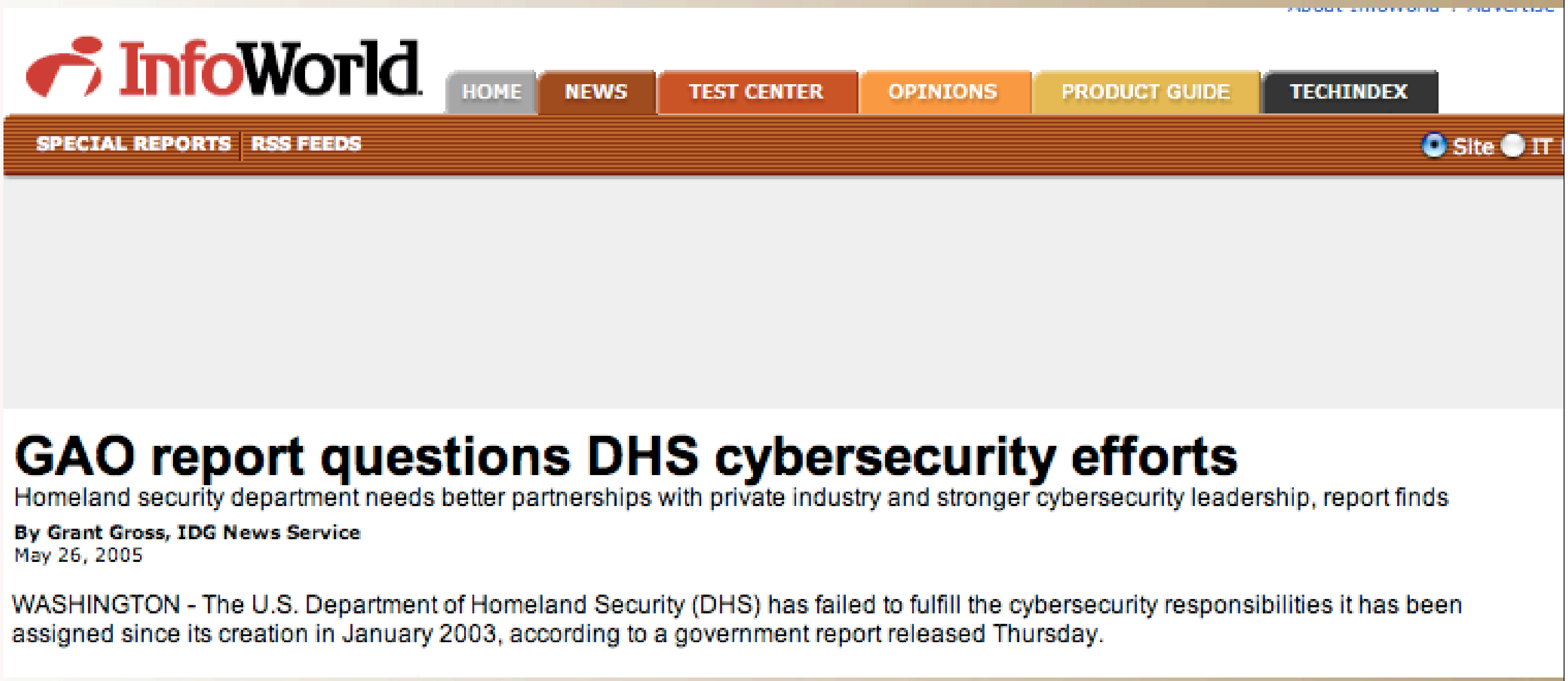
Hacker uses Sony's anticopy software to install PC virus

The Stinx-E trojan has been sent out in a mass e-mail

Law Enforcement?

- Limited tools
- Limited personnel
- Overemphasis on anti-terrorism
- International issues
- Limited prosecution

DHS?



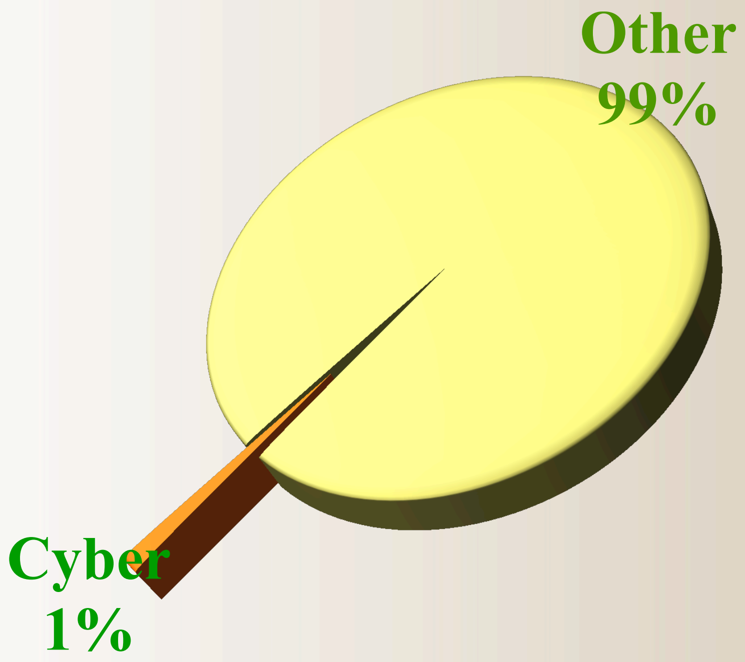
GAO report questions DHS cybersecurity efforts

Homeland security department needs better partnerships with private industry and stronger cybersecurity leadership, report finds

By Grant Gross, IDG News Service
May 26, 2005

WASHINGTON - The U.S. Department of Homeland Security (DHS) has failed to fulfill the cybersecurity responsibilities it has been assigned since its creation in January 2003, according to a government report released Thursday.

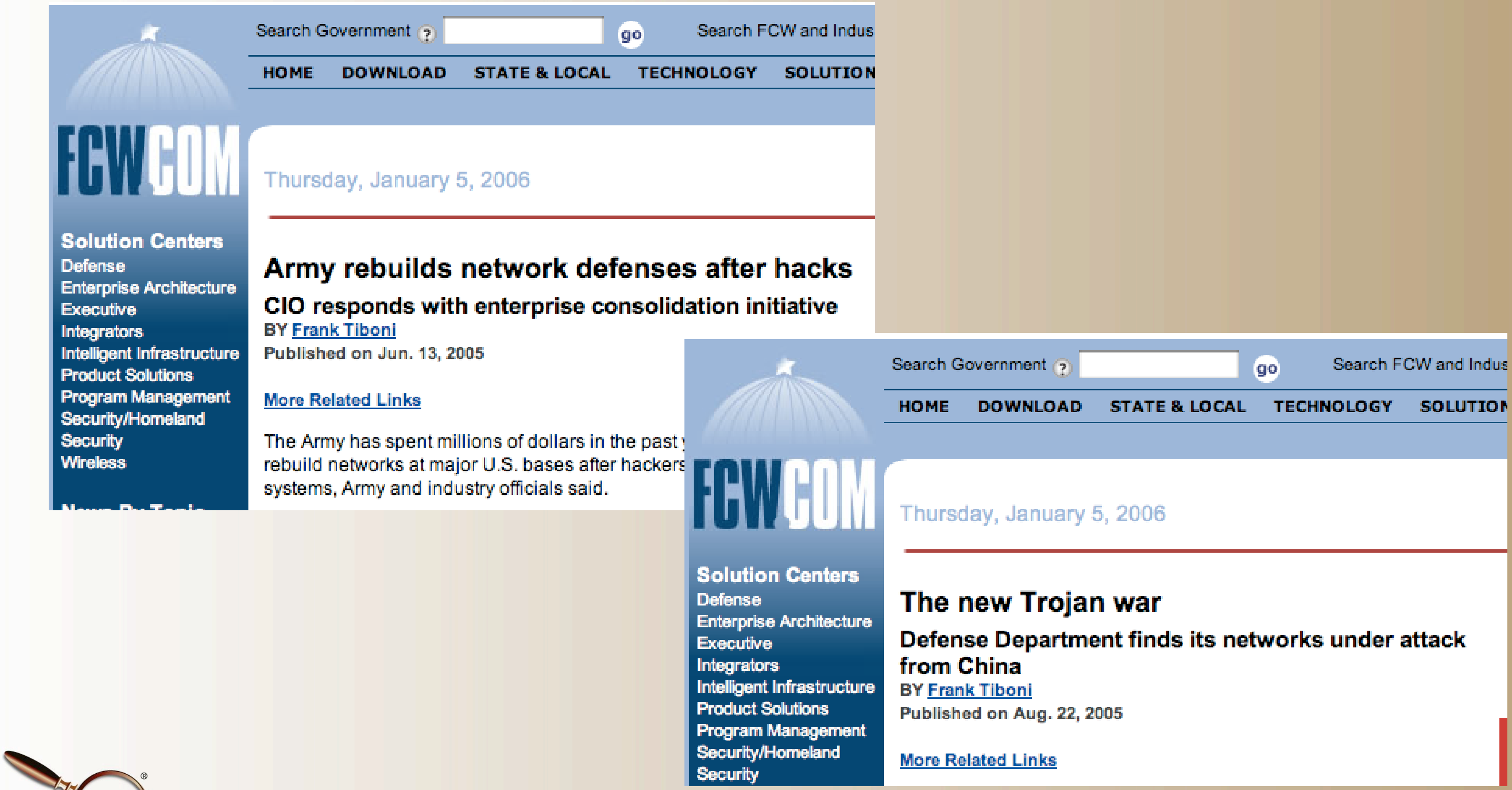
For example: DHS Attention



Research budget of $1.3 Billion

More is likely being spent to prevent you from taking nail clippers onboard airplanes than is being spent on Cyber Security.

How about the Dept. of Defense?



Thursday, January 5, 2006

Army rebuilds network defenses after hacks

CIO responds with enterprise consolidation initiative

BY Frank Tiboni

Published on Jun. 13, 2005

More Related Links

The Army has spent millions of dollars in the past y rebuild networks at major U.S. bases after hackers systems, Army and industry officials said.

Thursday, January 5, 2006

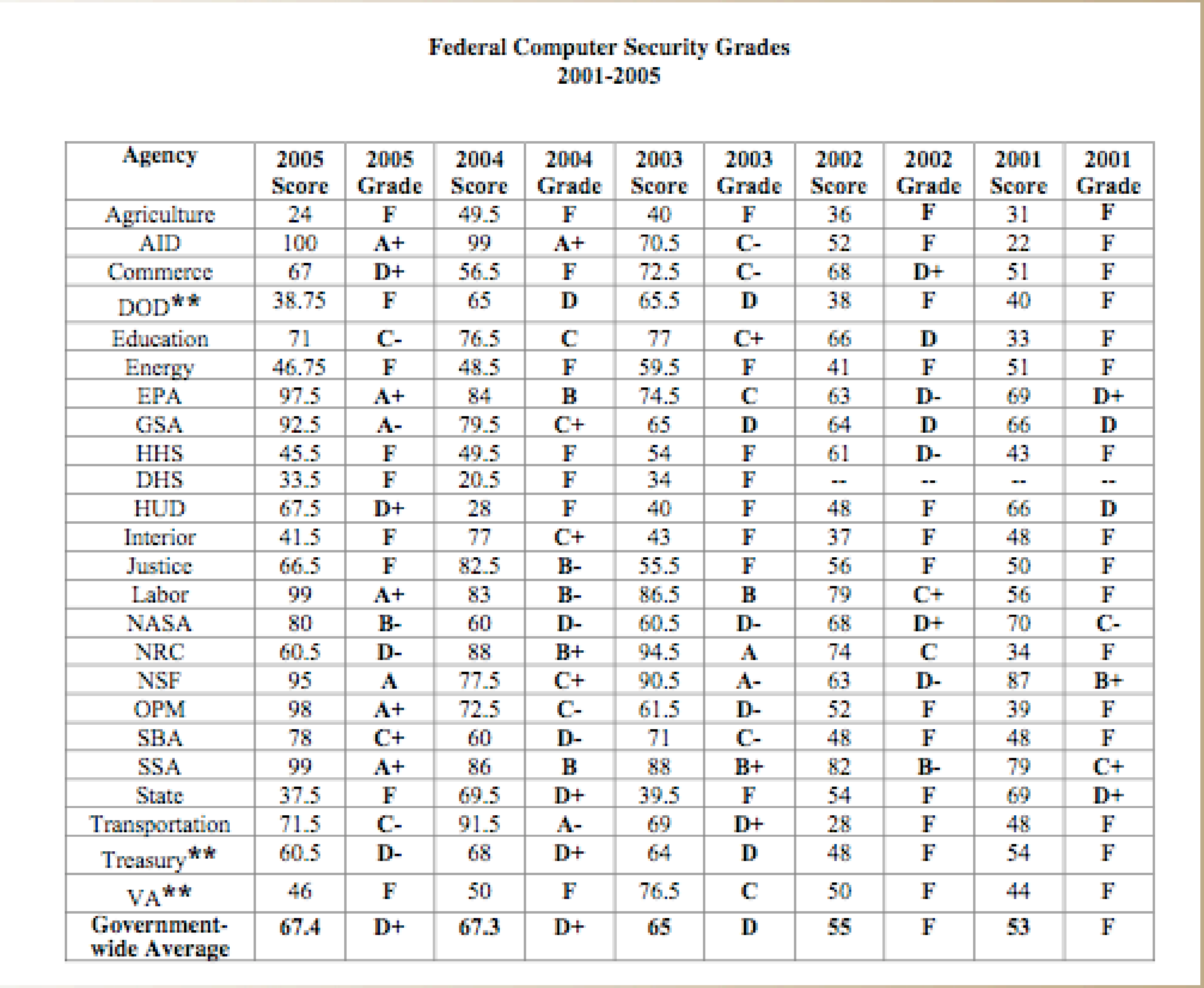
The new Trojan war

Defense Department finds its networks under attack from China

BY Frank Tiboni

Published on Aug. 22, 2005

More Related Links

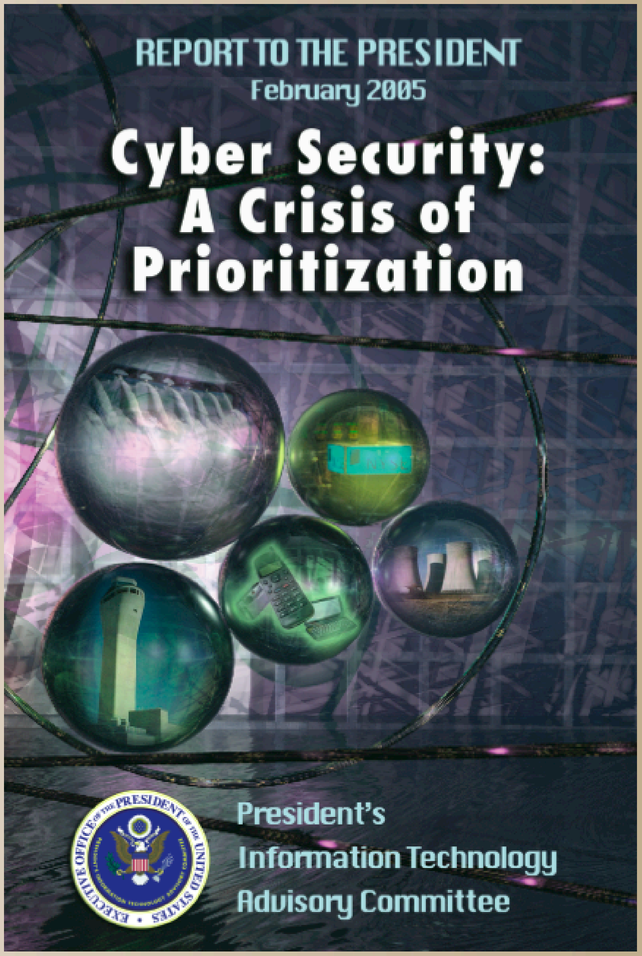


Federal Computer Security Grades
2001-2005

Agency	2005 Score	2005 Grade	2004 Score	2004 Grade	2003 Score	2003 Grade	2002 Score	2002 Grade	2001 Score	2001 Grade
Agriculture	24	F	49.5	F	40	F	36	F	31	F
AID	100	A+	99	A+	70.5	C-	52	F	22	F
Commerce	67	D+	56.5	F	72.5	C-	68	D+	51	F
DOD**	38.75	F	65	D	65.5	D	38	F	40	F
Education	71	C-	76.5	C	77	C+	66	D	33	F
Energy	46.75	F	48.5	F	59.5	F	41	F	51	F
EPA	97.5	A+	84	B	74.5	C	63	D-	69	D+
GSA	92.5	A-	79.5	C+	65	D	64	D	66	D
HHS	45.5	F	49.5	F	54	F	61	D-	43	F
DHS	33.5	F	20.5	F	34	F	--	--	--	--
HUD	67.5	D+	28	F	40	F	48	F	66	D
Interior	41.5	F	77	C+	43	F	37	F	48	F
Justice	66.5	F	82.5	B-	55.5	F	56	F	50	F
Labor	99	A+	83	B-	86.5	B	79	C+	56	F
NASA	80	B-	60	D-	60.5	D-	68	D+	70	C-
NRC	60.5	D-	88	B+	94.5	A	74	C	34	F
NSF	95	A	77.5	C+	90.5	A-	63	D-	87	B+
OPM	98	A+	72.5	C-	61.5	D-	52	F	39	F
SBA	78	C+	60	D-	71	C-	48	F	48	F
SSA	99	A+	86	B	88	B+	82	B-	79	C+
State	37.5	F	69.5	D+	39.5	F	54	F	69	D+
Transportation	71.5	C-	91.5	A-	69	D+	28	F	48	F
Treasury**	60.5	D-	68	D+	64	D	48	F	54	F
VA**	46	F	50	F	76.5	C	50	F	44	F
Government-wide Average	**67.4**	**D+**	**67.3**	**D+**	**65**	**D**	**55**	**F**	**53**	**F**

Don’t They Know?

- Reported to President Bush in 2/05
- Results:
  - Committee dissolved
  - Most of the recommendations ignored
  - Funding actually cut



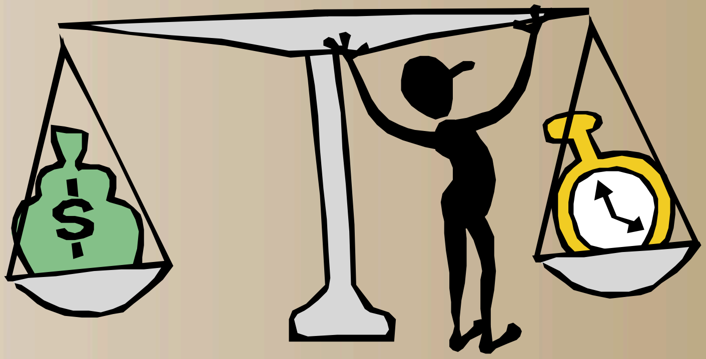
REPORT TO THE PRESIDENT
February 2005

Cyber Security: A Crisis of Prioritization

President’s Information Technology Advisory Committee

Need Balance in Research

- What are the systems after next?
- Need to grow the talent pool
- Need *significant* investment in R&D with longer focus
- Need investment in law enforcement
  - Includes reporting



Current research

Mostly focused on fixing the past, on MilSec or on IP rights

- Fixes for Windows, Linux, TCP/IP v4 ...

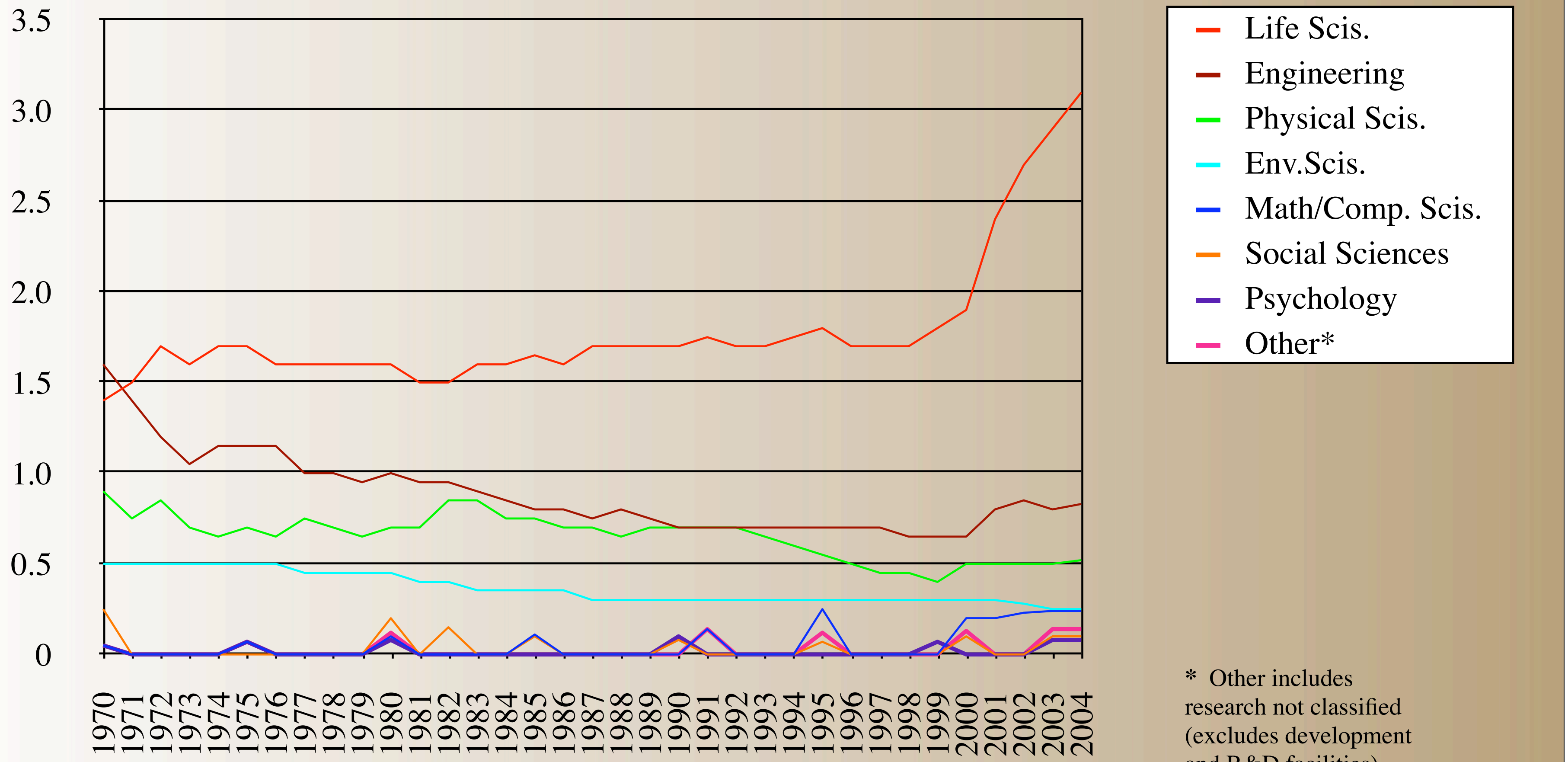
There is far more needed:

Malware, program flaws, privacy mechanisms, authentication, forensics, protocols, MLS design, intrusion detection and prevention, covert channels, crypto, digital cash, datamining, cyber terrorism, security architecture, residues, data pedigree, self-checking code, DRM, ...

PURDUE
UNIVERSITY

Federal Research Funding Share of GDP: 1970-2004

(obligations; ratio x 1000)



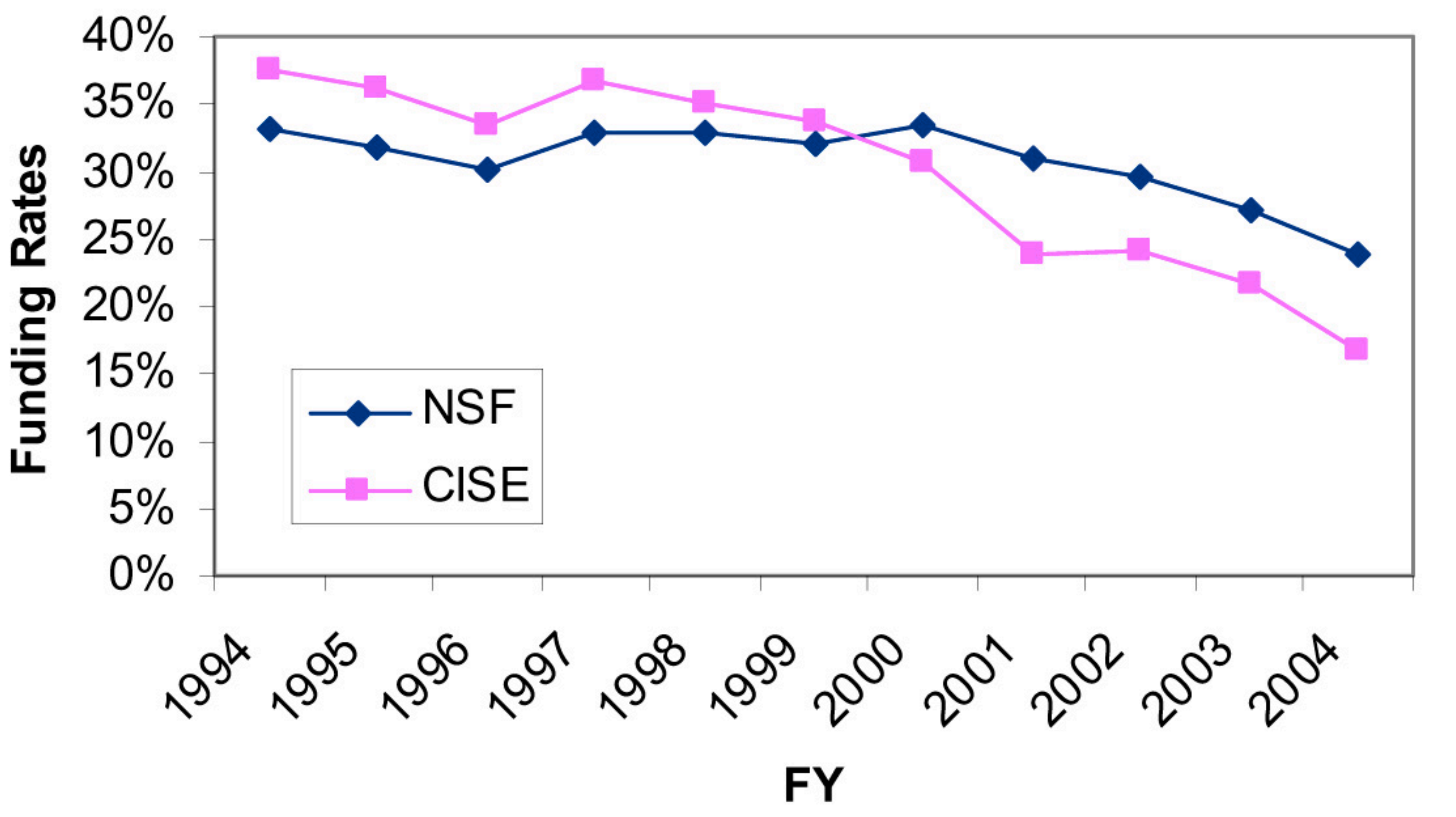
* Other includes research not classified (excludes development and R&D facilities)

Sources: AAAS, NSF *Federal Funds for Research and Development FY2001-4*

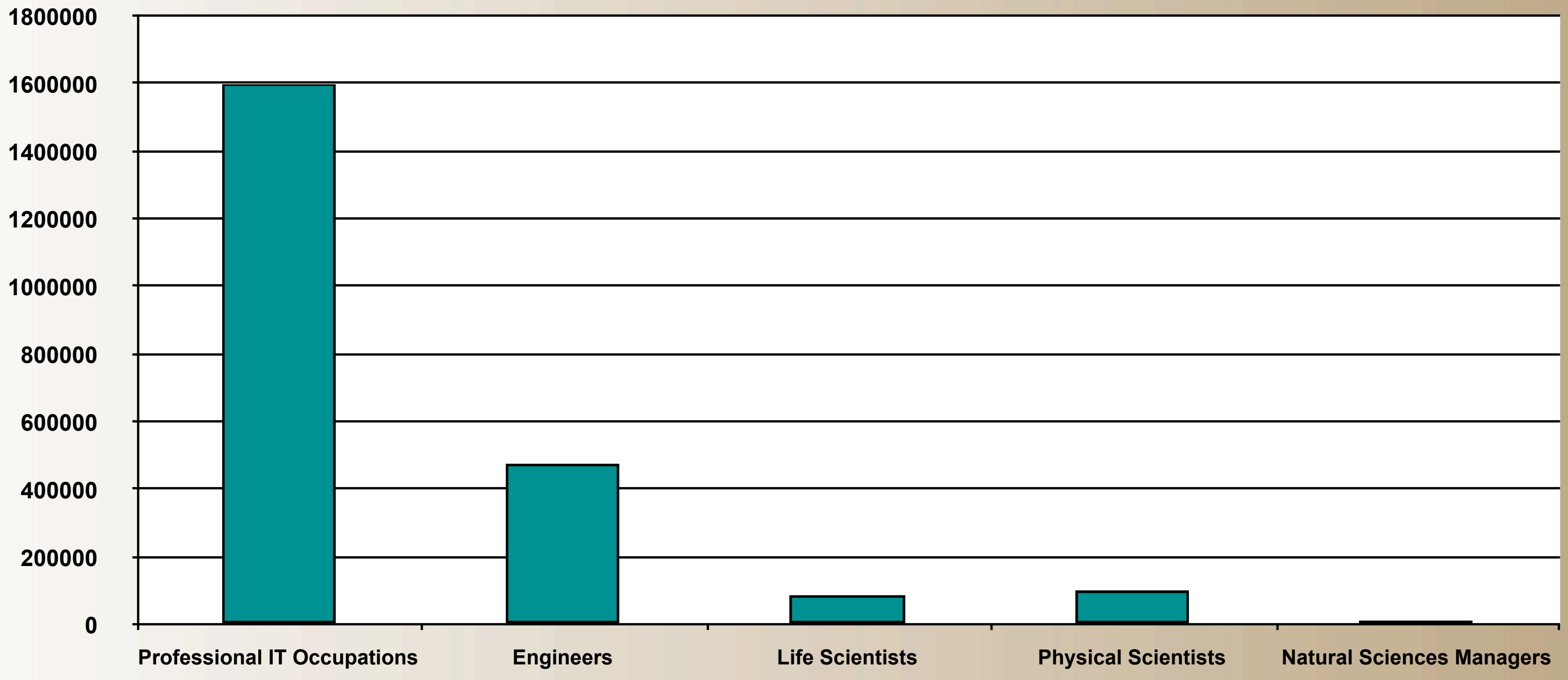
CERIAS®

http://www.cerias.purdue.edu

NSF and CISE Funding Rate Trends

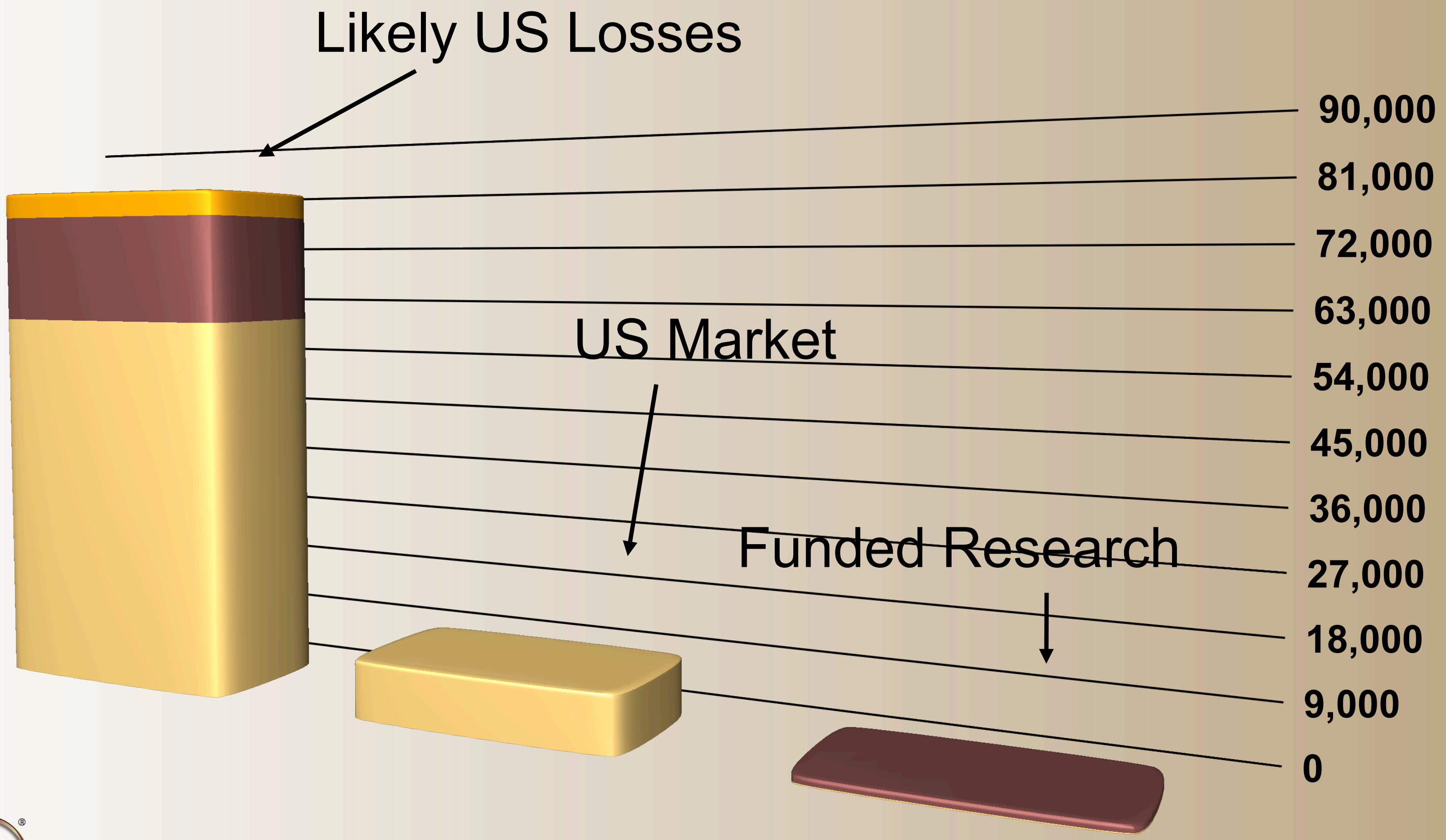


IT, Science and Engineering Occupational Projections, 2002-2012

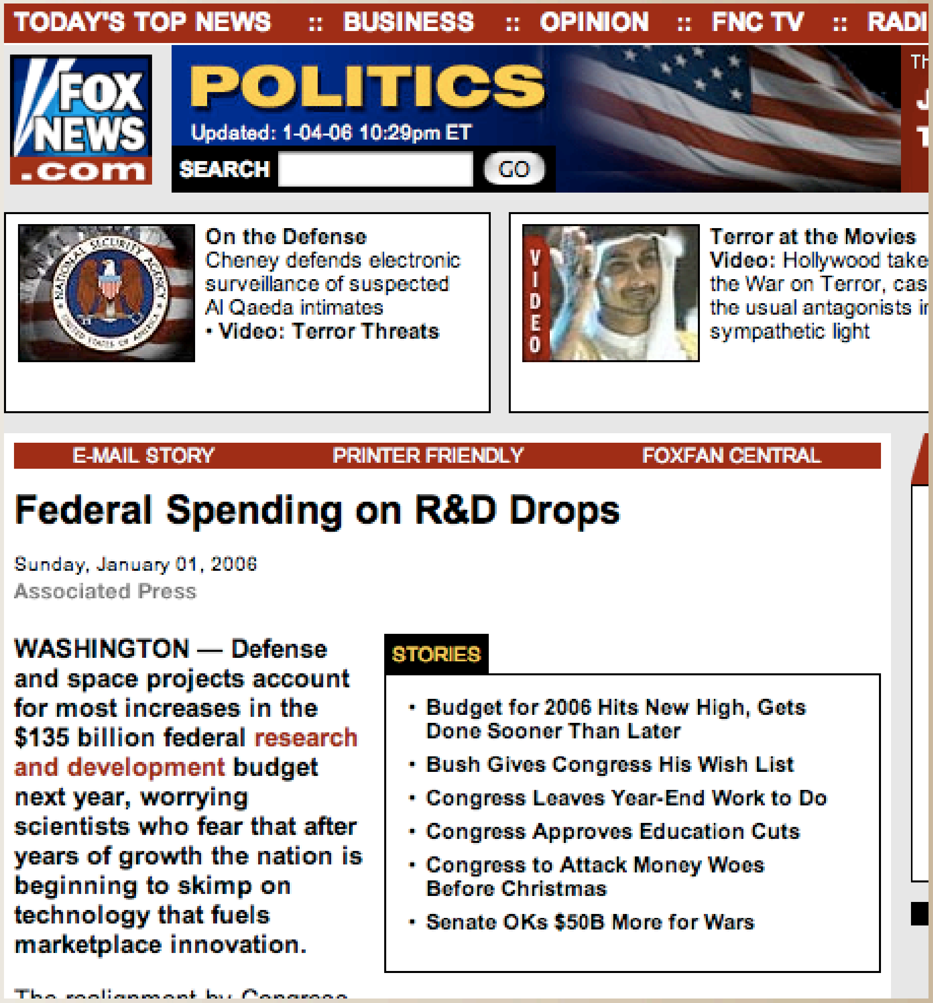


John Sargent, Senior Policy Analyst, U.S. Department of Commerce, presented to the Computing Research Association, 2/2004

Funding out-of-balance



What is Congress Doing?



Updated: 1-04-06 10:29pm ET

On the Defense
Cheney defends electronic surveillance of suspected Al Qaeda intimates
- Video: Terror Threats

Terror at the Movies
Video: Hollywood take the War on Terror, cas the usual antagonists i sympathetic light

Federal Spending on R&D Drops

Sunday, January 01, 2006
Associated Press

WASHINGTON — Defense and space projects account for most increases in the $135 billion federal research and development budget next year, worrying scientists who fear that after years of growth the nation is beginning to skimp on technology that fuels marketplace innovation.

The realignment by Congress

STORIES

- Budget for 2006 Hits New High, Gets Done Sooner Than Later
- Bush Gives Congress His Wish List
- Congress Leaves Year-End Work to Do
- Congress Approves Education Cuts
- Congress to Attack Money Woes Before Christmas
- Senate OKs $50B More for Wars

Not to Mention Things Such as the DMCA….

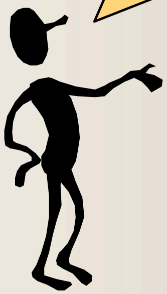
Original had copyrighted cartoon. Reproduction would not be fair use.

Dire, but not Hopeless

- Small, but growing number of dedicated researchers
- Active, concerned professional & commercial associations
  - E.g. CSIA
- Increasing public awareness that there is a problem
- President’s ACI….if it happens

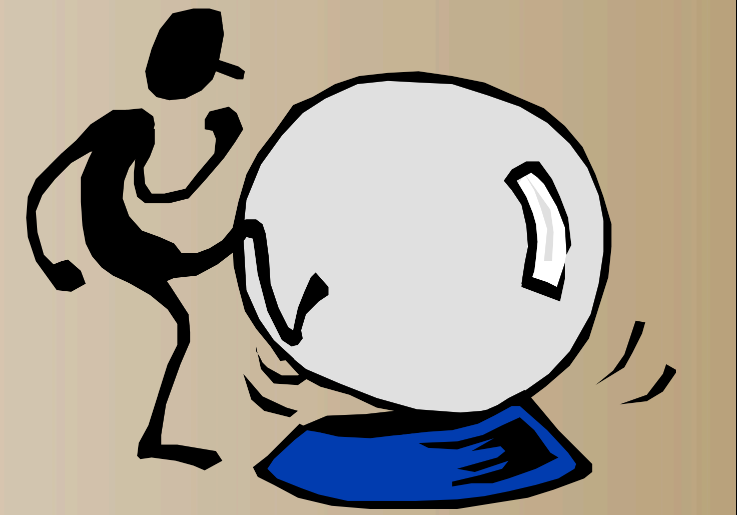
Perhaps, most of all…

Original had copyrighted cartoon. Reproduction would not be fair use.



The Future Does *Not* Need to Look Like the Present

- Change requires
  - Will
  - Investment
  - People
- Need a total approach
- Build <u>trust</u>
  - More than simply security



Thank you!

For more information

- PITAC

  www.nitrd.gov/pitac/reports
- CERIAS

  www.cerias.purdue.edu/
- USACM

  www.acm.org/usacm/
- CRA Grand Challenges

  www.cra.org/Activities/grand.challenges/security