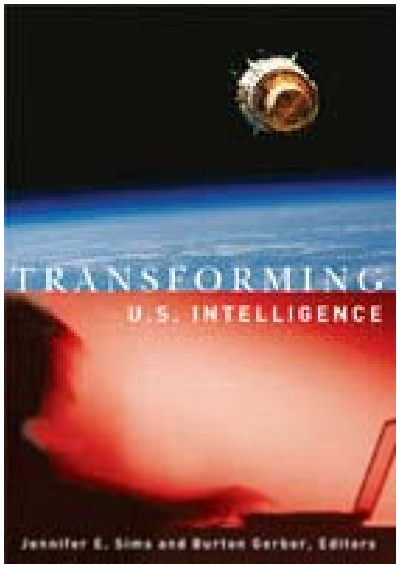
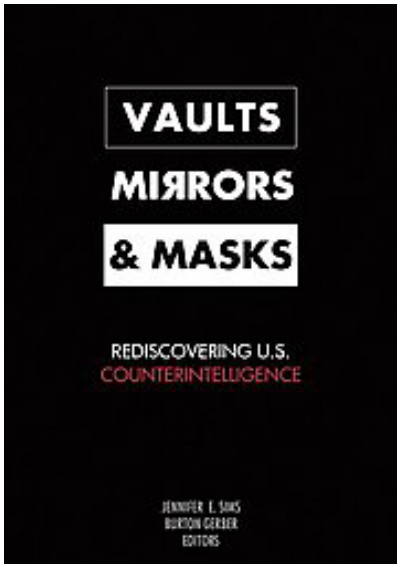
Rethinking the Foundations Seminar



4 MARCH 2009

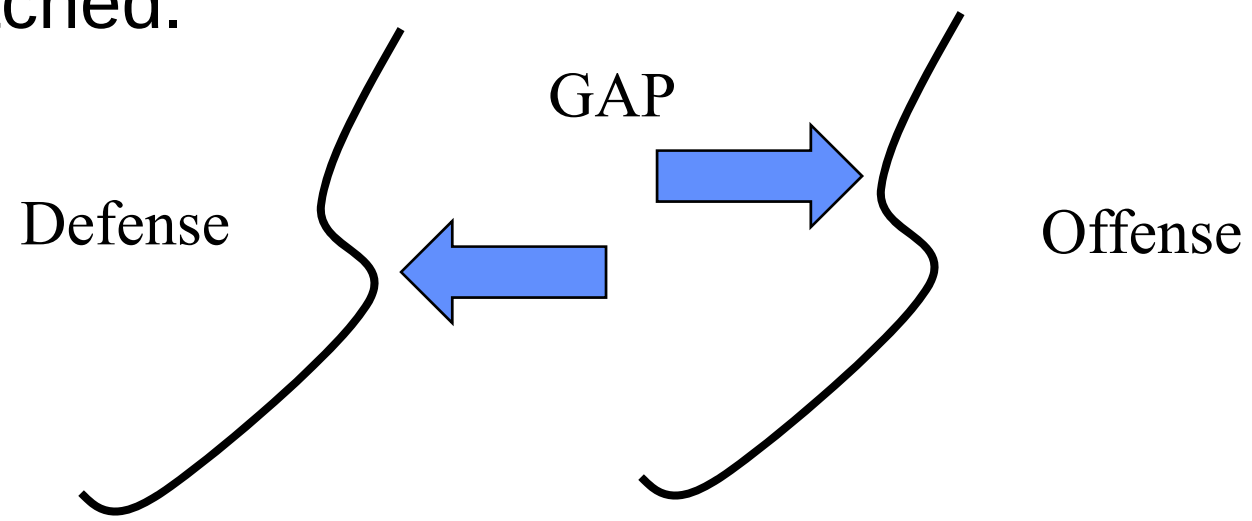
Jim Gosler

The Digital Dimension



Information Assurance Challenge

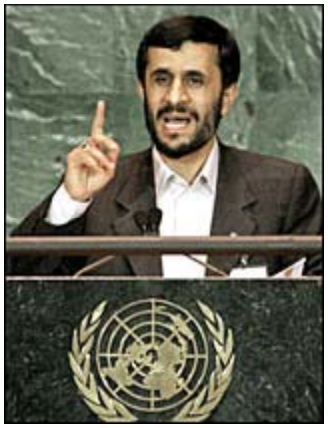
Assertion: Against a sophisticated (average) adversary, the current state-of-art in Information Assurance is significantly out matched.



National Security Imperative

ADM Bill Studeman
Former DDCI
Former Director of NSA
Commissioner on the WMD Commission
Member of SNL Intelligence Advisory Panel

"May be the biggest single problem [the Information Assurance challenge] facing DOD and the national security establishment today."



Mahmoud Ahmadinejad
President of Iran

"Surely we are not naive about the United States' ... intention to flex its muscles," a statement from Tehran read by Mr. Vaidi said. "But we also see the bone fractures underneath."

Myth or Insanity?

Gen James Cartwright

"Myth: Systems we have today are not subject to attack."

DSB meeting May 18, 2006

USS Stark FFG-31
17 MAY 1987

Insanity: We are designing and implementing mission critical systems today as if they will be operating in an adversary-free environment.

Adversarial Innovation

The Offensive Advantage

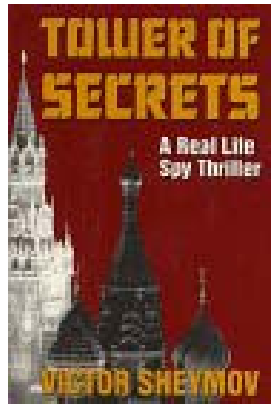
The offense has the ability to choose the time, the place and the method of attack. When they are working at their best, they see the target from a systems perspective and work as a collaborative team. They will attack at the target's weakest point.

The defense must be strong enough to withstand the strength of the offense at its weakest point

…..a daunting challenge!!!!!

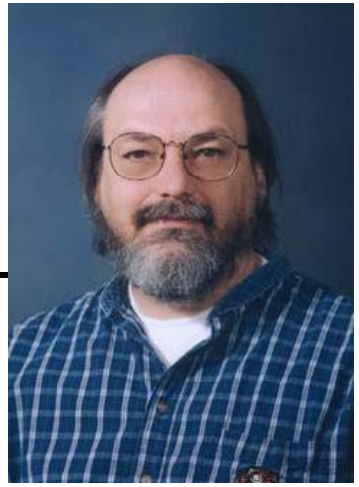
…Small Error Leading to a Big Loss

Victor Sheymov



Trust and Complexity

"You can't evaluate yourself out of this problem."



- **1984 Ken Thompson – Bell Labs**
  - **"Reflections of Trusting Trust"**
    - "The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code."

- **2005 Jim Gosler – Sandia Labs**
  - **"Transforming Intelligence: The Digital Dimension"**
    - "Thompson's insight was progressive, the situation he described is even worse today. You may not even be able to trust code that you totally created yourself! …while he might have complete confidence in his software design and implementation, including its binary representation, he would most likely have no confidence in the fidelity of the hardware platform on which the software is executing."

IT Trends Yesterday - Today

Early 80's

- Intel 8088
  - 29,000 Transistors
  - 4.77 MHZ
  - 3 micron Tech

- Disk Drive
  - 10MB 5.25"

- DOS
  - 100K Bytes

Today

- Intel
  - 1,000,000,000 Transistors
  - 3,600 MHZ
  - .032 micron Tech
- Disk Drive
  - 1,500,000MB 3.5"
- Windows 2000
  - 1-2,000,000K Bytes

Who or What has access to our SECRETS?

People

- Background Investigations
  - Polygraphs
    - Financial Disclosure
      - U.S. Citizens
        - Physical Security

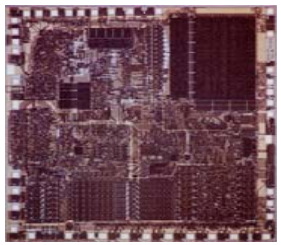
Life Cycle

- Design
  - Development
    - Test
      - Production
        - Distribution

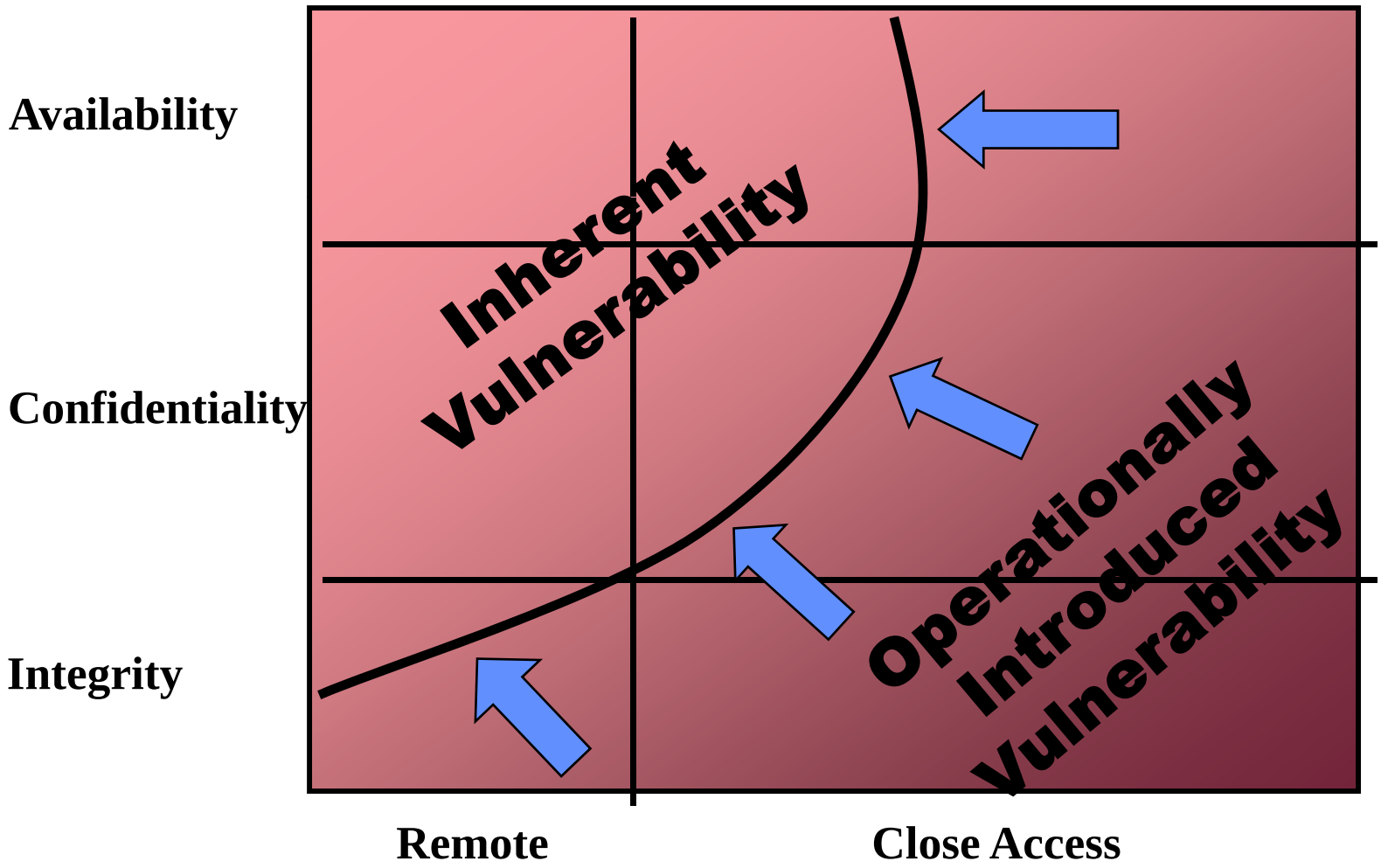
??????

Technology

- Microprocessors
- Firmware
- Circuit Boards
- Power Supplies
- Peripheral Devices
- Mass Storage Devices
- Firewalls
- Antivirus Software
- Operating Systems
- Application Software



The Domain of Vulnerability



Characteristics of Sophisticated Offensive Organization

- Worldwide Presence
- Significant Resources
- Internal Legal Protection
- Mature Operational Tradecraft
- Diverse Network of Trusted Partners
- Diverse Network of Untrusted Partners
- Worldwide Secure Comms and Logistics
- Integration of Human and Technical Ops
- Effective Security Program
- Mid-Point Collection
- Integration of Offensive and Defensive Elements

So What! Risk Management Very Hard!!

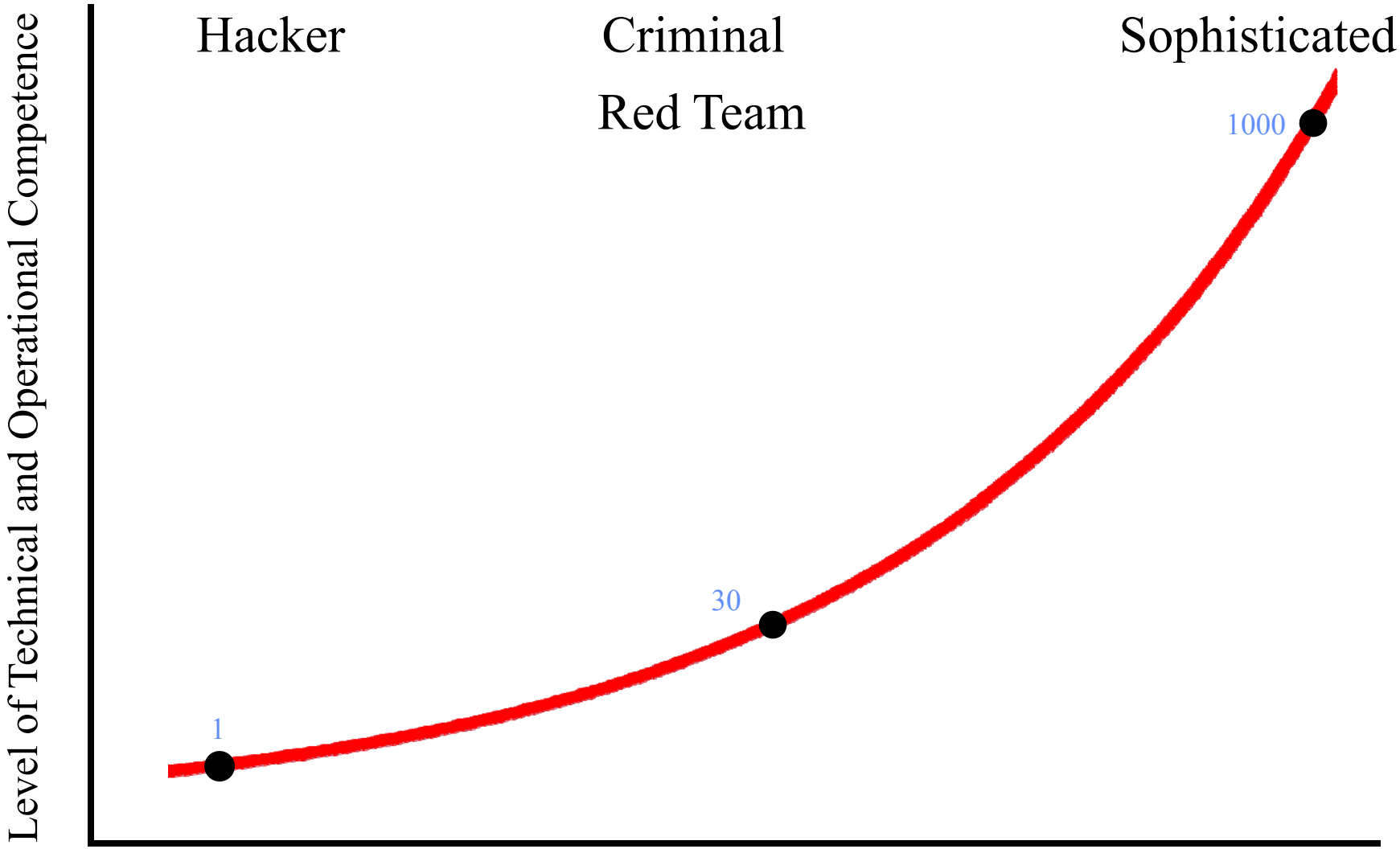
- Software Development → Foreign
- Microelectronic Fabrication → Foreign
- Brain Trust → Foreign
- Complexity Increasing Exponentially
- Defensive Measures Losing Ground Rapidly
- US Dependence Growing Dramatically
- US Conventional Military Dominance Drives Adversary to Asymmetric Approach
- Offensive Capability well within Reach of Enemy
- Impact of Defensive Failure Growing Dramatically
- Access + Tech Capability + Vulnerability + Weak Defenses +High Dependence =

VERY BAD NEWS

The 30th Annual
ACM-ICPC World Finals
Sponsored by IBM
San Antonio, Texas
12-Apr-06

Rank	Name	Solved	Rank	Name	Solved
1	Saratov State University	6	19	Kyoto University	3
2	Jagiellonian University - Krakow	6	19	Lund University	3
3	Altai State Technical University	5	19	National Taiwan University	3
4	University of Twente	5	19	Petrozavodsk State University	3
5	Shanghai Jiao Tong University	5	19	Pontificia Universidade Católica do Rio de Janeiro	3
6	St. Petersburg State University	5	19	Seoul National University	3
7	Warsaw University	5	19	Simon Fraser University	3
8	Massachusetts Institute of Technology	5	19	Sofia University	3
9	Moscow State University	5	19	South Ural State University	3
10	Ufa State Technical University of Aviation	5	19	St Petersburg Institute of Fine Mechanics & Optics	3
11	University of Alberta	4	19	Taras Shevchenko Kyiv University	3
12	University of Waterloo	4	19	Technische Universität München	3
13	Instituto Tecnologico de Aeronautica	4	19	The University of Hong Kong	3
13	Korea Advanced Institute of S & T	4	19	Tsinghua University	3
13	Peking University	4	19	University of Science and Technology of China	3
13	Sharif University of Technology	4	19	University of Tokyo	3
13	University of British Columbia	4	19	University of Toronto	3
13	Zhejiang University	4	19	Zhongshan (Sun Yat-sen) University	3
19	Information & Communications University	3	39	Bangladesh University of Engineering & Technology	2
19	KTH - Royal Institute of Technology	3	39	California Institute of Technology	2

Classes of Adversary

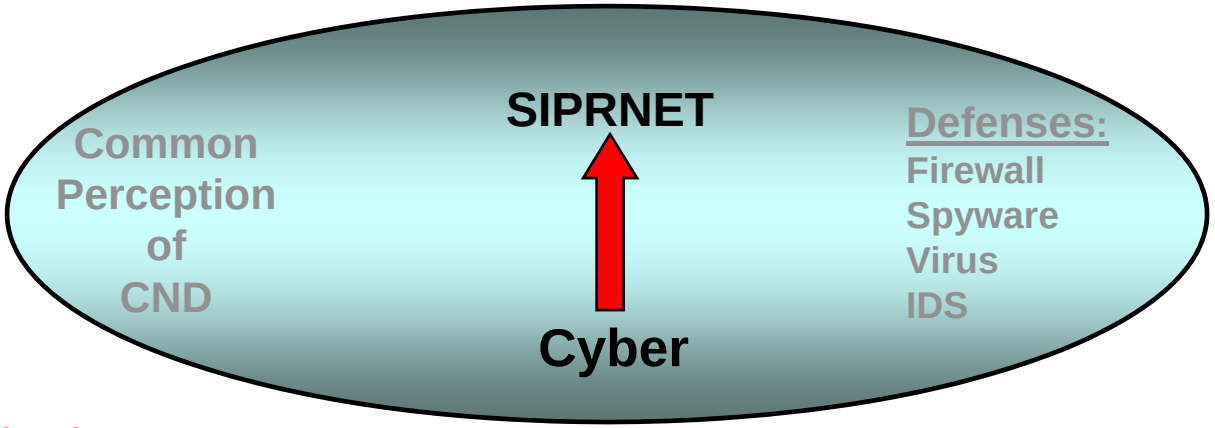


The Ambiguity of Computer Network Defense

Microelectronics and Software

Satellite	SCADA	Weapons	Network	C^2	Logistics	Switches

Targets



Offensive Methods

Entry	Human	Sigint	ClanTech	Cyber	Special	Liaison	Deception	Cover Company

Time, Place, Combination of Methods, and Secrecy

Project GUNMAN

- Congressman Henry Hyde 1990 testimony
- Soviet operation targeting typewriters
- Discovered in 1984 in US Embassy Moscow
- Typewriters bugged in shipping channel
- Captured all keystrokes and transmitted to nearby listening post
- VERY sophisticated adversary!!

Elements of a Successful Defensive Strategy

- Decrease inherent vulnerabilities within hardware and software
- Increase difficulty of an adversary introducing vulnerabilities thru life-cycle
- Increase our ability to deeply evaluate critical components
- Decrease unneeded functionality in critical components/systems
- Increase the cost and uncertainty to an adversary
- Decrease the adversaries confidence that an asymmetric IO strategy will be broadly effective
- Increase the coupling of offensive and defensive elements
- Increase US insight into the offensive IO capabilities and intentions of our adversaries
- Increase the probability of detecting a component behaving badly
- Increase the probability of attributing the bad behavior to the adversary
- Increase the consequences to the attacker for its bad behavior
- Decrease the impact of a defensive failure

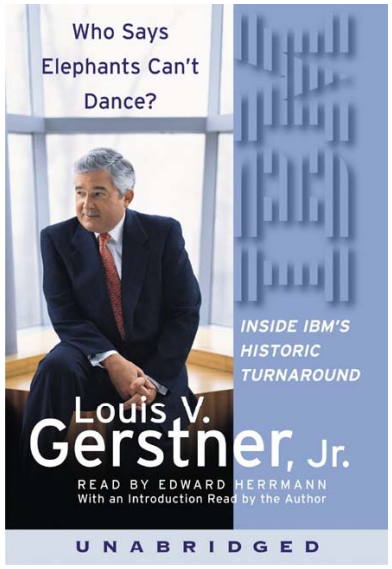
The Innovative Application of Offensive Capabilities to Support Defensive Objectives.

Necessary Conditions for Effective Risk Management

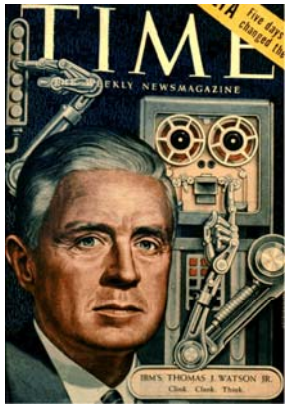
- Defense Must Understand the Full Spectrum Approach
- Understanding Must Permeate Defensive Culture
- "Seniors in Denial" Addressed – Never Been in This Foxhole – GEN Carns Story
- Defensive Elements Must Work as Integrated Team (CI, Physical, Personnel, Cyber, Acquisition,..)
- Move Well Beyond Compliance Based Security
- Address Rewards and Incentives Issues
- Develop and Maintain World-Class Workforce
- Innovative Use of Offensive Capabilities to Support Defensive Objectives
- Address Policy Issues that Arise – US Persons, Privacy,..
- Understand This Will be Never Ending – Dynamic – Not Static
- Understand Difference Between Act-of-God and Malicious Adversary
- Tailored Solutions to Address: Confidentiality, Integrity and Availability Challenges

Culture VERY Hard to Change!

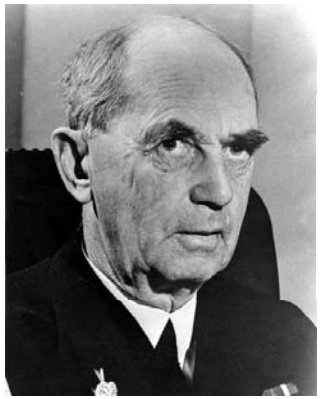
"Successful institutions almost always develop strong cultures that reinforce those elements that make the institution great. They reflect the environment from which they emerged. When that environment shifts, it is very hard for the culture to change. In fact, it becomes an enormous impediment to the institution's ability to adapt."



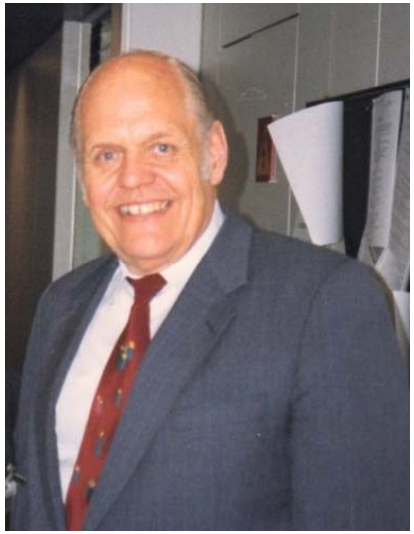
Bright Men Can Sometimes Be Somewhat Short-Sighted



"I think there is a world market for maybe five computers." – Thomas Watson, chairman of IBM, 1943



"The bomb will never go off. I speak as an expert in explosives." Admiral William Leahy, US Atomic Bomb Project



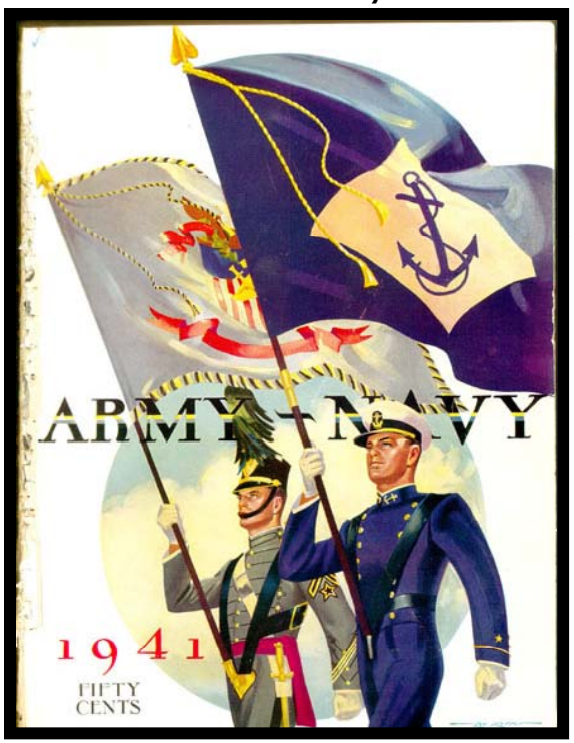
"There is no reason anyone would want a computer in their home." ? Ken Olson, president, chairman and founder of Digital Equipment Corp.,1977

"640K ought to be enough for anybody." Bill Gates, 1981

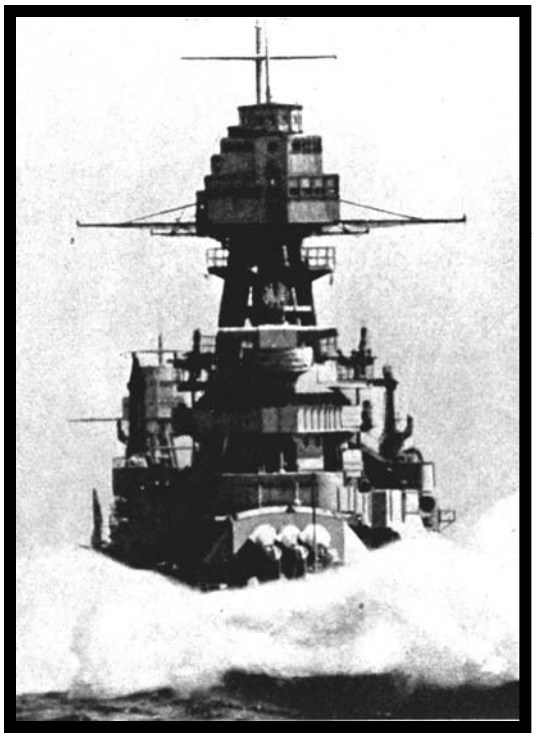
Army – Navy Football Game
Philadelphia

Navy 14 – Army 6

November 29, 1941



U.S.S. Arizona



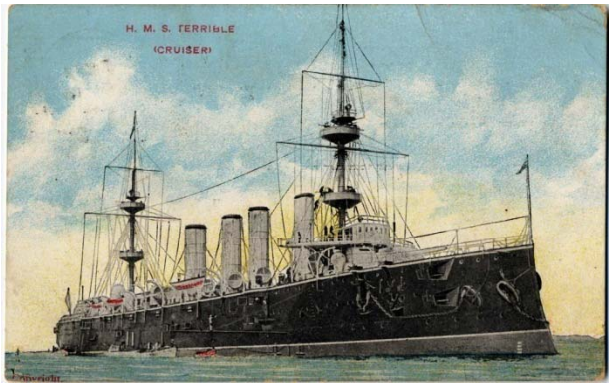
"It is significant that despite the claims of air enthusiasts no battleship has yet been sunk by bombs."

LT Sims' Frustration

"I am perfectly willing that those holding views differing from mine should continue to live, but with every fibre of my being I loathe indirection and shiftiness, and where it occurs in high place, and is used to save face at the expense of the vital interests of our great service, I want that man's blood and I will have it no matter what it costs me personally."

William S. Sims

Sir Percy Scott



H.M.S. Terrible

Elting Morison: Gunfire at Sea: A Case Study of Innovation

Jim Gosler

Observations

- NO short term answer. Technology alone will never be sufficient.
- NO informed National Defensive Strategy – *getting a lot better!*
- NO Belly Button in charge, responsible, accountable across the full threat spectrum
- Insufficient coupling between US offensive and defensive activities
- Little effort focused on development of a National technical cadre. Deep, broad, sustainable….Experts!
- Intelligence Community not sufficiently engage in the collection, analysis and reporting on this issue.
- IC reporting, in general, not actionable from defensive perspective.
- Senior decision makers lack insight into the criticality and complexity of this issue – Risk Management difficult.
- Principal adversaries of the US understand and are acting upon the asymmetric opportunities in this area.
- Probability of detection, probability of attribution, impact of defensive failure and consequence to the attacker are way out of balance.

Never underestimate the motivation, patience, and creativity of an adversary!

- **They play strength to weakness**
- **They develop surprising partners**
- **They change the rules**
- **They see offense as a systems challenge**
- **They attack against a defense that is naïve, arrogant, unbalanced and fragmented**

  - ♦ We are critically dependent on advanced technology for most every aspect of U.S. National Security. Trust in these systems is very hard to measure or guarantee. The consequences of misplaced trust in this arena is growing and alarming!

We can work a lot harder at what we are doing and not make much of a difference!