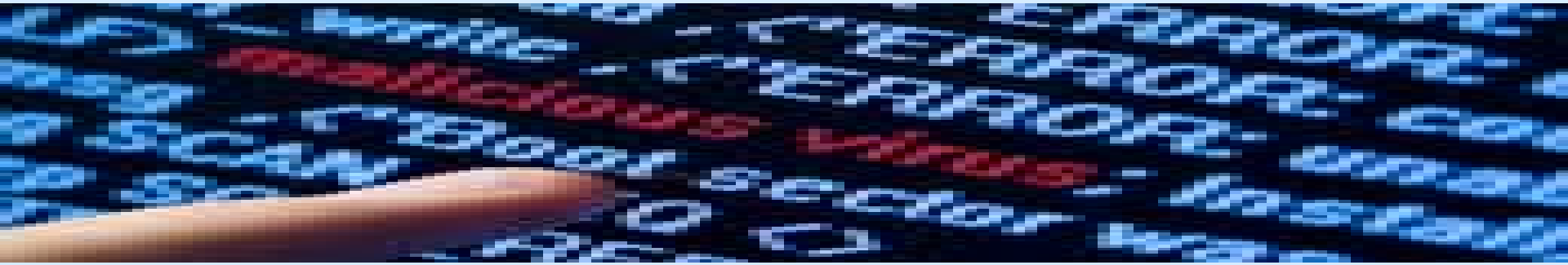
Managing Cyber C2 Challenges: Uncertainty, Acquisition, Material

International Command and Control Research and Technology Symposium

June 22, 2010



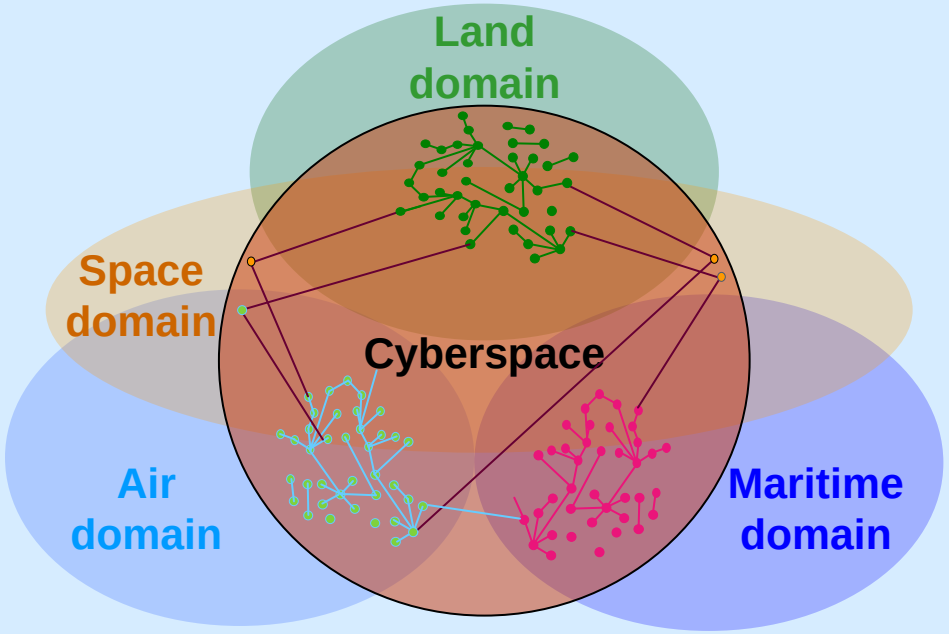
Panel Participants

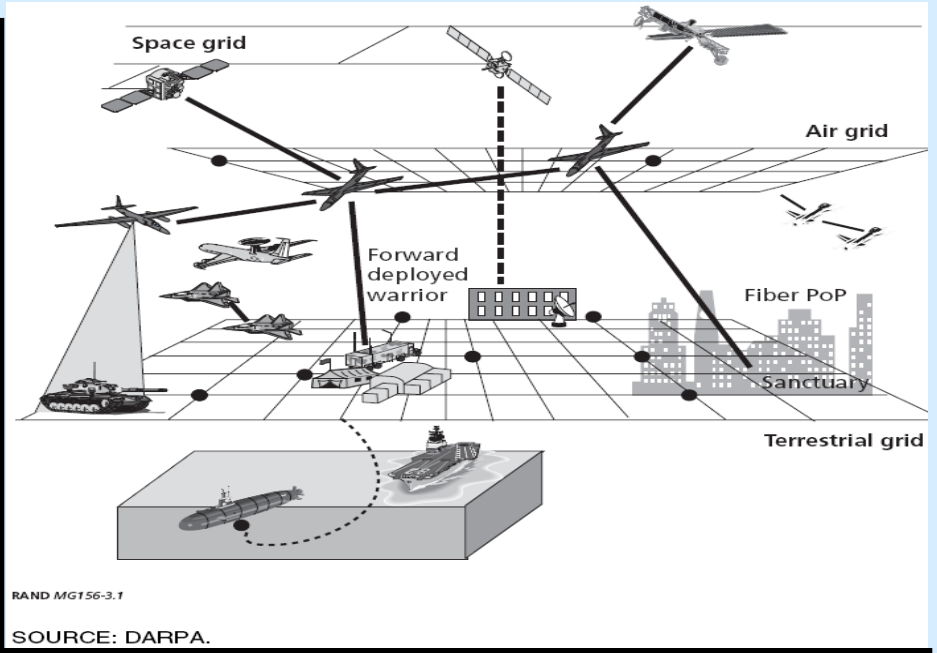
Dr. Isaac Porche, Senior Engineer, RAND

Richard Mesic, Senior Policy Analyst, RAND

Dr. Elliot Axelband, Senior Engineer, RAND

Cyberspace Facilitates Command and Control Across the Traditional Domains





SOURCE: DARPA.

Challenges:

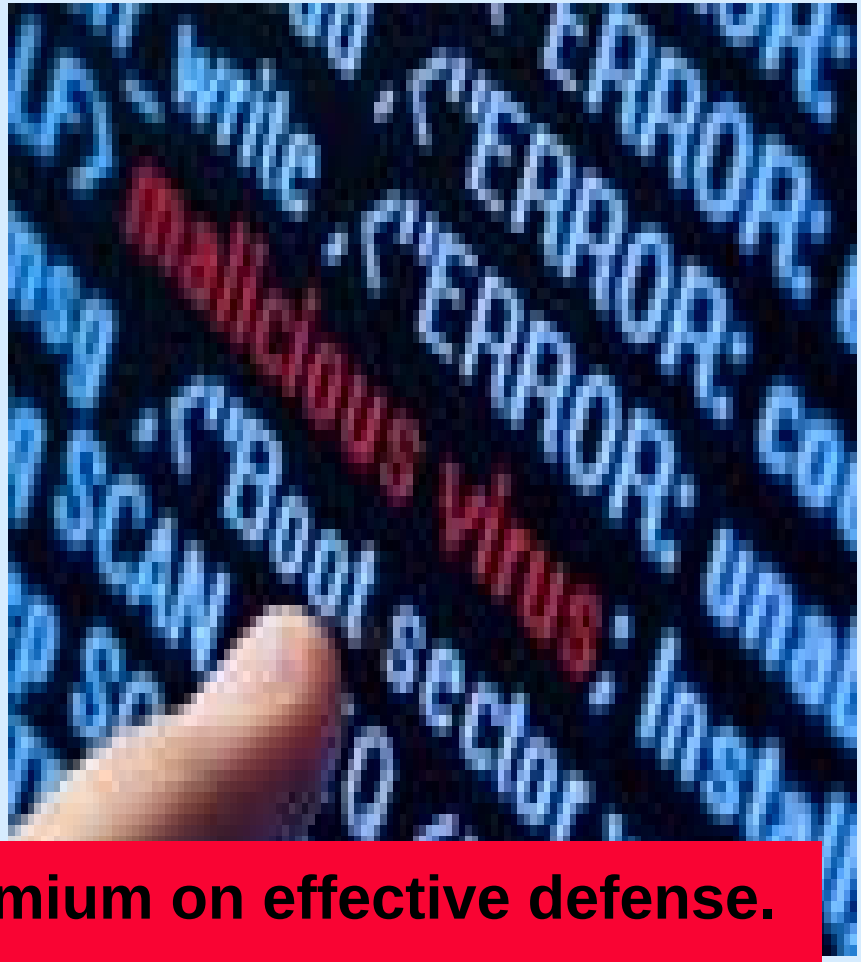
- Constantly growing in size and complexity
- Man-made
- Uncertainty abounds
  - about terms and roles, and
  - about actors, e.g., anonymity.

Enabling properties:

- Access to information, Situational awareness
- Synchronized operations,

Numerous Threats Exist but the Source/Agents Can Be Difficult to Identify

- **External threats**
- **Internal Errors**
  - **Operators slow to recognize threats**
  - **Operators mistake problems for normal system activity**
  - **Security specialists fail to realize and communicate how large a problem may be**



These challenges place a premium on effective defense.

To Manage These Challenges, We Need to Consider:

- **What kinds of operational certainties and uncertainties effect cyberwarfare and security**
- **What software, IT, and hardware is needed and can be acquired to secure cyber operations**
- **The trade-off between security and information sharing**

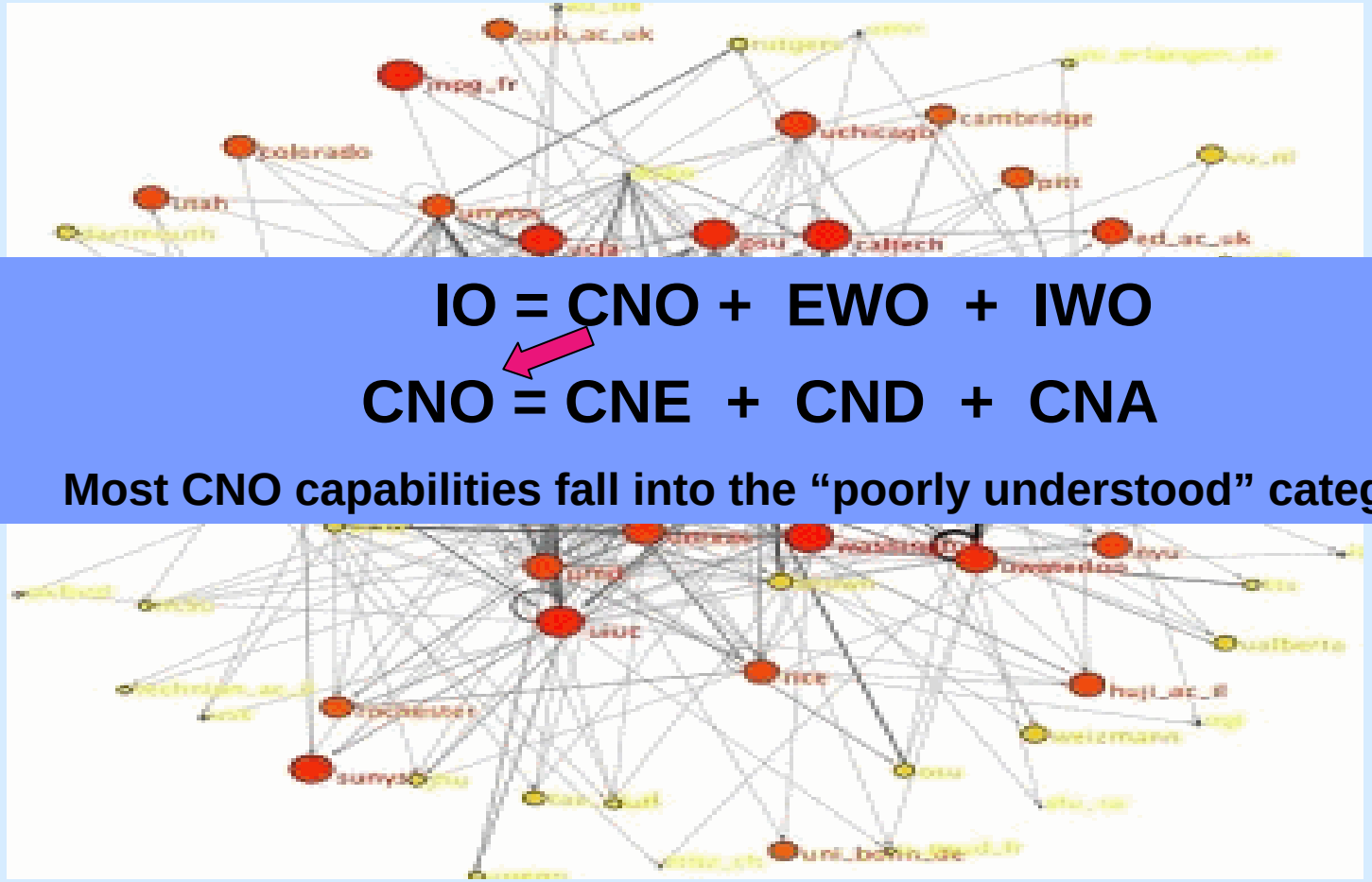
To Manage These Challenges, We Need to Consider:

- **What kinds of operational certainties and uncertainties effect cyberwarfare and security (Richard Mesic)**

- **What software, IT, and hardware is needed and can be acquired to secure cyber operations**

- **The trade-off between security and information sharing**

Can We Effectively and Efficiently Command and Control Systems that Are So Broad, Highly Classified, and Poorly Understood?

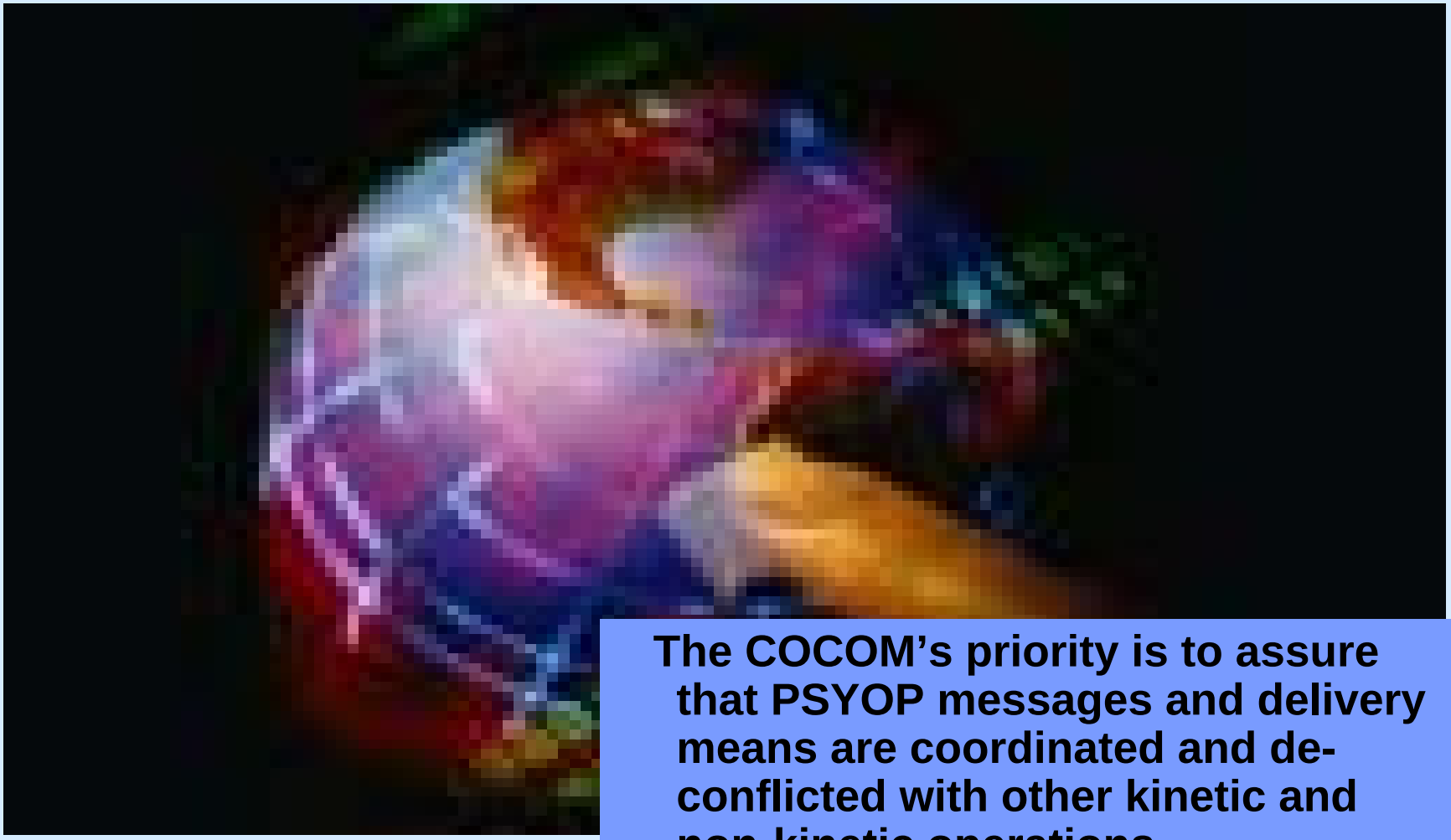


IO = CNO + EWO + IWO

CNO = CNE + CND + CNA

Most CNO capabilities fall into the “poorly understood” category

Maybe the Most Understandable Cyber Effects Are "Soft" (e.g., directed PSYOP)



The COCOM's priority is to assure that PSYOP messages and delivery means are coordinated and de-conflicted with other kinetic and non-kinetic operations.

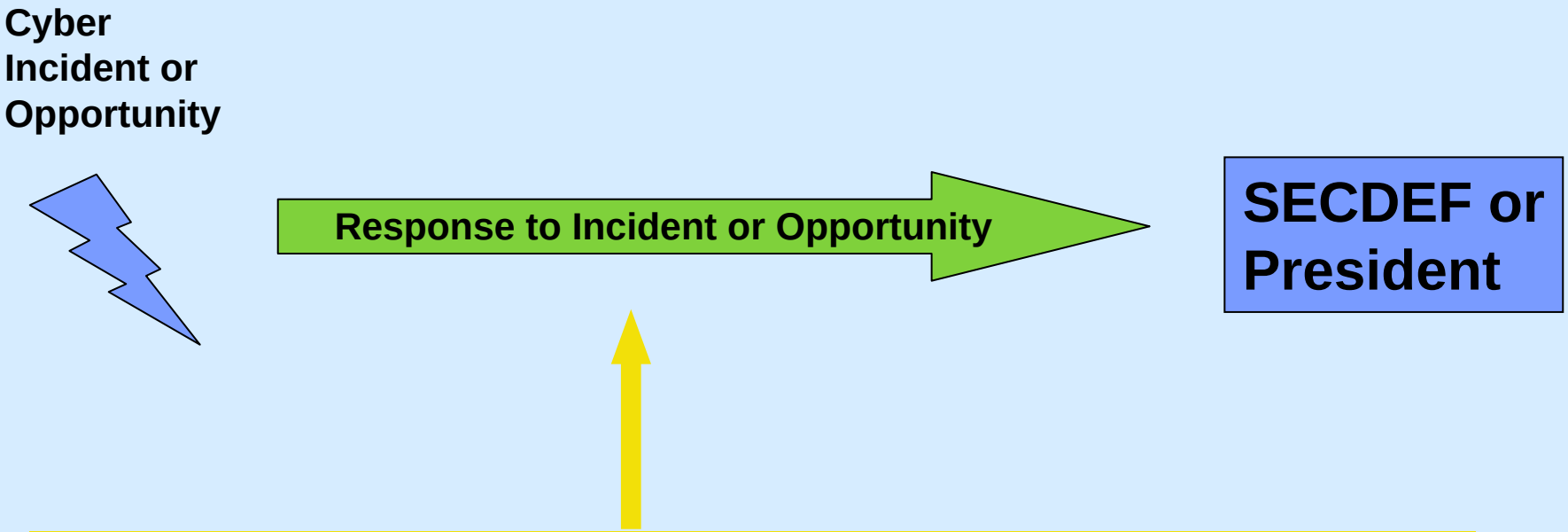
Coordinating and De-Conflicting Offensive Cyber and Non-Cyber Missions and Systems Is a C2 Challenge

- **This is due partly to the lack of cyber experience and the lack of a non-kinetic "JMEM"**
- **The challenge is particularly severe with respect to estimating and controlling cyber collateral damage**
- **Integrating kinetic and non-kinetic (eg., cyber) capabilities is a C2 challenge that seems to default to a C2 focus on kinetic missions and systems…with non-kinetic capabilities in a supporting (bonus) role**

Cyber Blurs Distinctions Between Combatants and Non-Combatants

- **The extension of the LOAC to cyberspace is still a work in progress.**
- **For now, the cyber commander's constant companion is likely to be a JAG.**

Because of Legal and Operational Uncertainties, Significant Cyber Action Is Often Approved Only at the Highest Levels of Command



Because of planning, coordination and approval time lines, lower-level commanders may be reluctant to incorporate significant cyber capabilities at the operational/tactical levels of warfare.

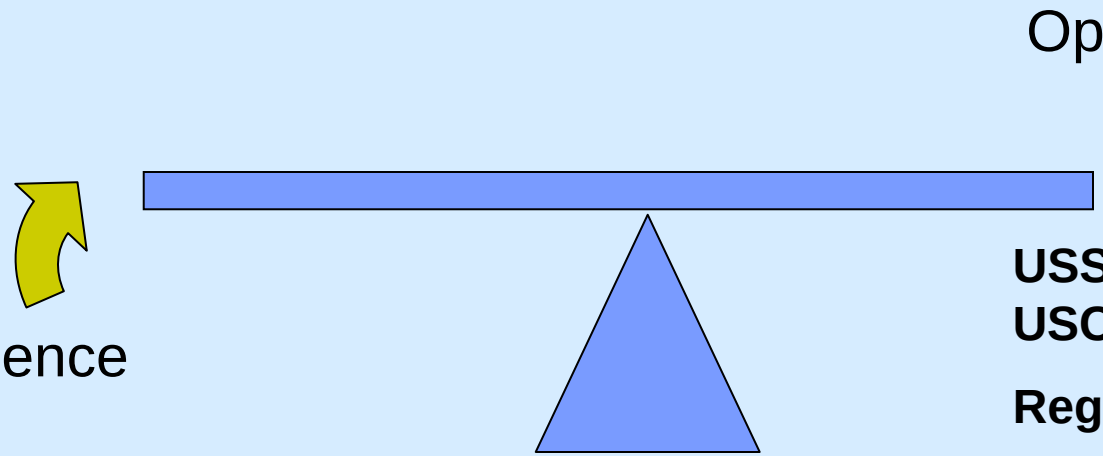
Cyber's Greatest Potential May Be in Irregular Warfare Missions and Day-to-Day Intelligence Operations and Environment-Shaping That May Require…

- **The Military to play merely a supporting role to other government entities**
- **Cyber C2 to become a matter of inter-agency cooperation, with all the associated cultural and procedural difficulties**
- **The DoD and COCOMS to be seldom given unilateral cyber C2 responsibilities and authority.**

Cyber Operational Preparation of the Environment Operates in the Seams of Title 10/50 Responsibilities and Authorities

C2 is a shared activity between the commander's intelligence and operations entities as well as organizations beyond the commanders control (e.g. NSA).

The Execution of Cyber Tools and Systems Requires Time-Sensitive Coordination



Intelligence:

NSA
CIA
Service Intelligence Organizations
Other (e.g., DHS, FBI,…)

USSTRATCOM/ USCYBERCOM

Regional COCOMs

Service Components

STO Cells . . .

This can present significant unsolved C2 challenges.

C2 Cyber Is Hindered by a Lack of Cyber-Situational Awareness

Cyber capabilities and threat, friendly, or other status are difficult to:

define

assess

visualize…

Responsibility and Authority Pose Significant Challenges to Cyber C2

- **Who owns and controls what in a landscape of dispersed "net-centric" ownership?**
  - **Commercial systems and providers (US and other)**
  - **Service-specific systems**
  - **Allies . . .**
- **How will actions - even purely defensive ones - in one area of cyber space effect others?**

To Manage These Challenges, We Need to Consider:

- **What kinds of operational certainties and uncertainties effect cyberwarfare and security**
- **What software, IT, and hardware is needed and can be acquired to secure cyber operations (Elliot Axelband)**
- **The trade-off between security and information sharing**

What Is to Be Acquired in Order to Perform Optimally in the Cyber-Landscape?

- **Software?**
- **IT?**
- **Hardware?**
- **Cyber/EW?**

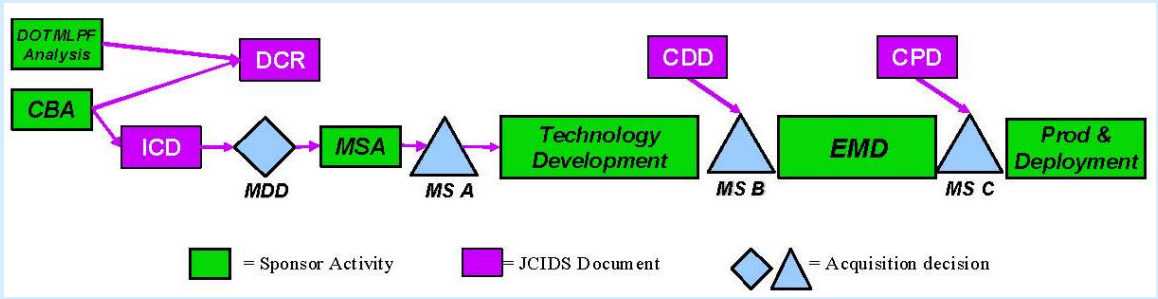
It Depends on What Is the Envisioned Life-Cycle?, AF Tentative Plans

- **Real Time - Hrs/Weeks**
  - **Software/IT**
- **Rapid - Weeks Months**
  - **Software/IT**
  - **COTS/GOTS, Mods**
- **Enduring - Years**
  - **PEOs/PMs**
  - **JCIDS/5000 Process**
  - **SW/IT/HW**

Work at the shop or floor level with with industry poised to react

"Big Safari"- like A new AFMC Cyber Safari

Expedite using existing Contract Vehicles



" We believe that existing DoD series and FARS provide you most to the flexibility you need..".
" I don't think there needs to be any change in acquisition laws or rules"
" It may require a change in the way our contracting officers look at the existing rules."
General Lord as quoted in *Inside the Air Force,* 091218.

How Does Acquisition Fit in With Current US DoD Policies?

- **USSOCOM Enablers**
- **US Army - ONS;**
- **US Navy - UON;**
- **US Marines; UUNS,**
- **US Air Force - CCD,**
- **US DoD - JUONS**

What Is Everyone Saying About Cyber Acquisition? - DSB and others

- **DSB, 3/09 Task Force**
  - **Focus - Business Systems, Information Infrastructure, C2, ISR, Embedded IT in Weapon Systems, and IT upgrades to fielded systems**
  - **JCIDS conventional process too cumbersome - retain for efforts with significant scientific, engineering, hardware development and the integration of complex systems only**
  - **New Acquisition Policy for IT needed, and workforce trained for it**
  - **Acquisition Policy Recommended that produces first increment of capability in 3 1/2 years and subsequent increments in 18 months or less**
  - **USD (AT&L) with VCS should lead this effort with support from CIO, PA&E, DDR&E, OT&E, Controller, Users and others**

What Is Everyone Saying About Cyber Acquisition? - NRC - 2010

- **Focus - Software in COTs Computers not embedded in Weapon Systems**
- **Conclusions DoD IT Acquisition too lengthy vs. Commercial Systems developed using Agile Methods**
  - **Less Oversight, Less Paper, Less Process Focus, More Product Focus**
  - **Develop Pieces**
  - **Test Frequently with Users**
  - **Aggregate pieces to get not all of the capabilities you require but better customer satisfaction**
- **Presenters Comments**
  - **Generally speaking we are talking about more than COTS computers not embedded in Weapon Systems**
  - **Agile methods are experimental**
  - **This approach would require heavy experimentation/prototyping**

What Is Everyone Saying About Cyber Acquisition? - Congress

- **WSARA - 2009**
  - **Establishes new organizations and their roles and responsibilities, and modifies those of existing organizations**
  - **Complicates DoD acquisition for major weapon systems, its focus so as to improve its operation - On time delivery within budget of acquired products and services that provide their intended capabilities**
  - **DoD implementation complicates JCIDS**
- **HASC Panel on Acquisition Reform, March - 2009**
  - **Directs the implementation of an alternate process for IT Acquisition**
- **IMPROVE - April 2010**
  - **Expands WSARA to all of acquisition, but does not discuss urgent acquisitions**
  - **Adds complications such as requirement for tracking performance using new metrics, and expanding the charters of the WSARA organizations**
  - **Requires changes to JCIDS to make it more rigorous and less cumbersome**
  - **Charters GAO to report on applicability of changes made to JROC to other acquisitions including information technology**
  - **Certification and training required required for acquisition personnel with emphasis on the acquisition of services, information technology, and rapid acquisitions.**

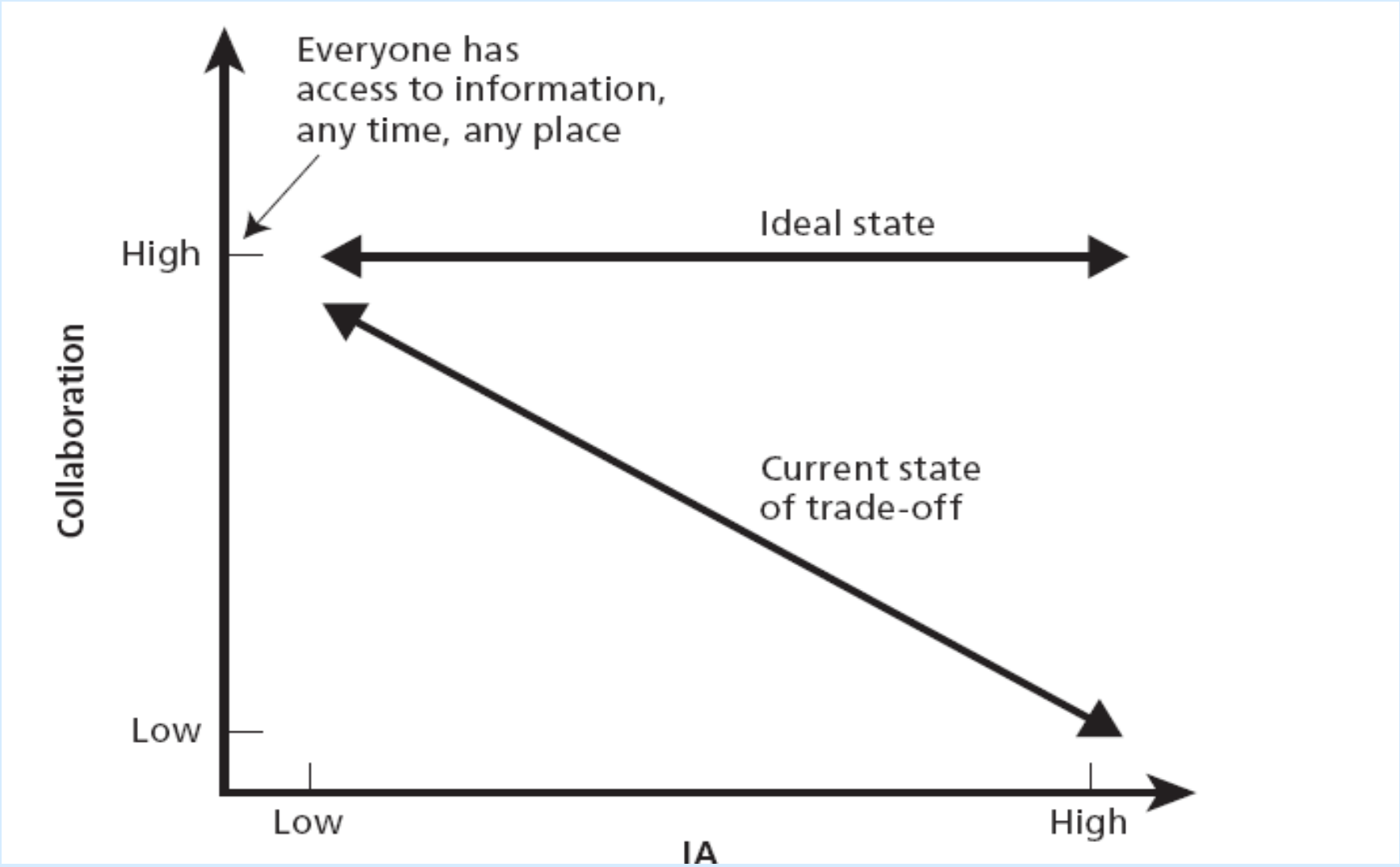
Convergence of Traditionally Distinct Areas

- **Wired and Wireless**
- **Cyber and Electronics**

To Manage These Challenges, We Need to Consider:

- **What kinds of operational certainties and uncertainties effect cyberwarfare and security**
- **What software, IT, and hardware is needed and can be acquired to secure cyber operations**
- **The trade-off between security and information sharing (Isaac Porche)**

Today, There Exists Inherent Trade-offs Between Sharing Information and Protecting/Assuring It



There Are Multiple Reasons for the Trade-Offs

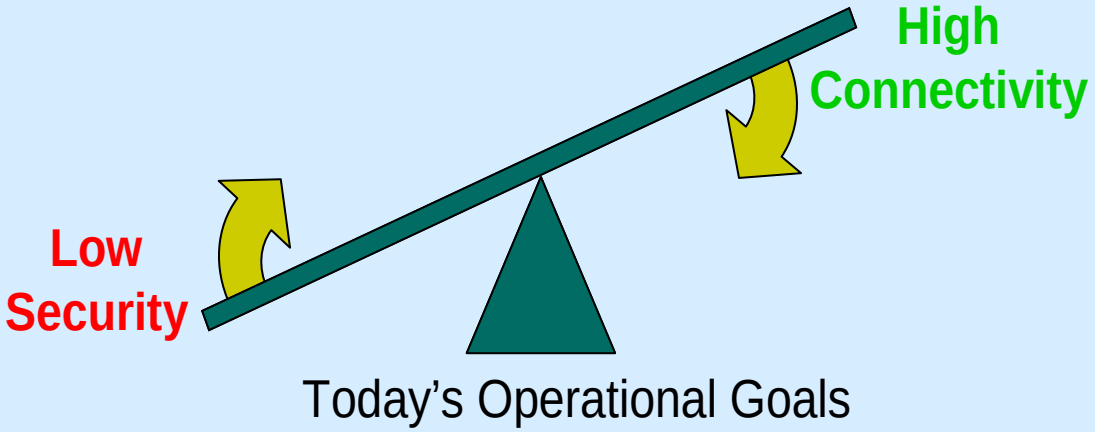
- **Culture**: CISO vs. CIO mindset
- **In wireless medium, disbenefits to ubiquitous connectivity persist** (Joe and Porche, 2004)

  e.g., throughput penalty
- **Ubiquitous or increased connectivity adds to complexity**, and "*Complexity is the worst enemy of security*"

  From: Schneier, *Secrets and Lies*, 2000, P.354
- **Access to information is equated to access to the network** (9/11 Commission report, p 418, Markel Report)

This does NOT have to be the case

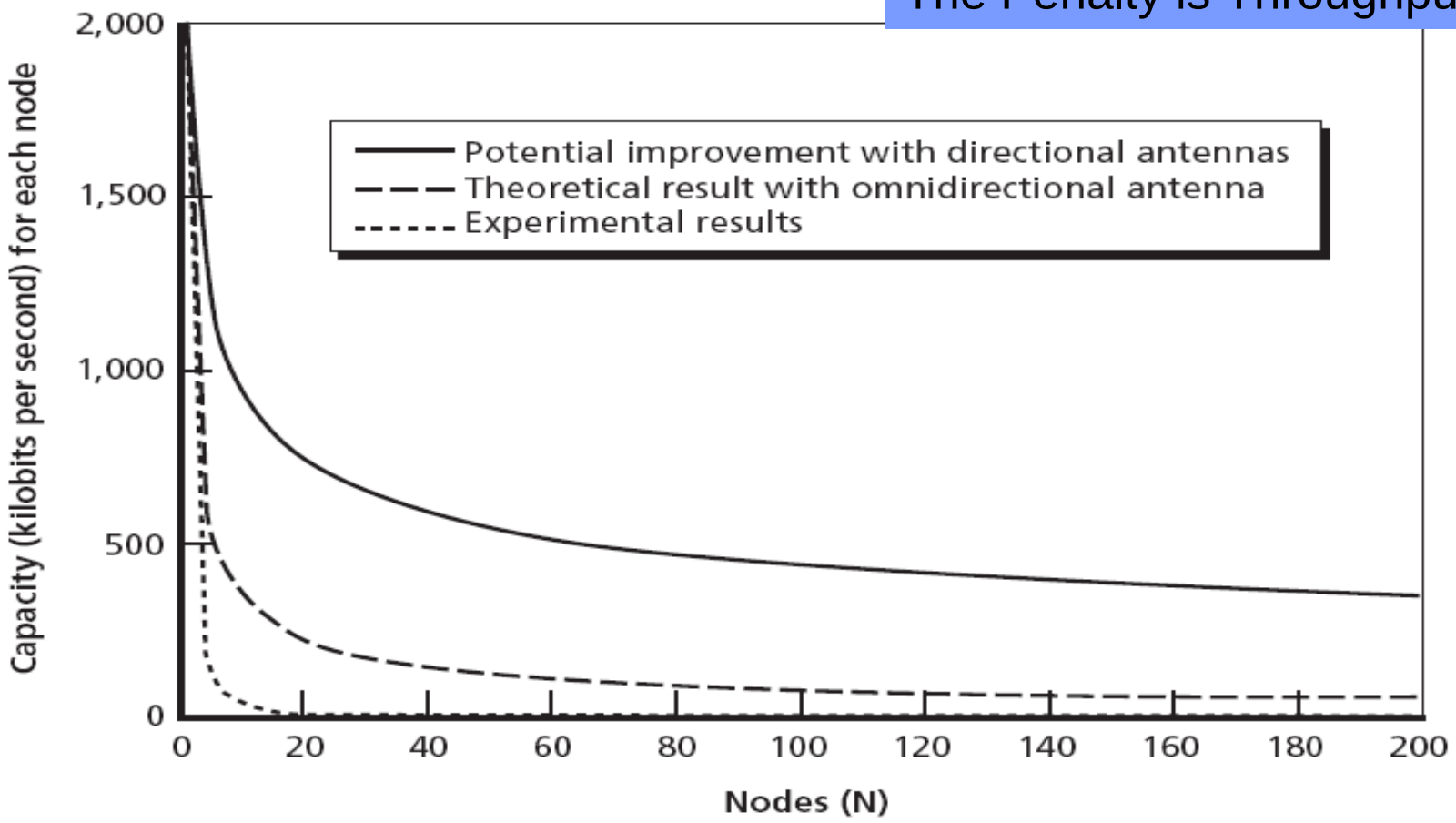
Cultural/Operational Preferences: "Keep the Net Up"



- **CIO focus = Security**
- **CISO focus = Connectivity**

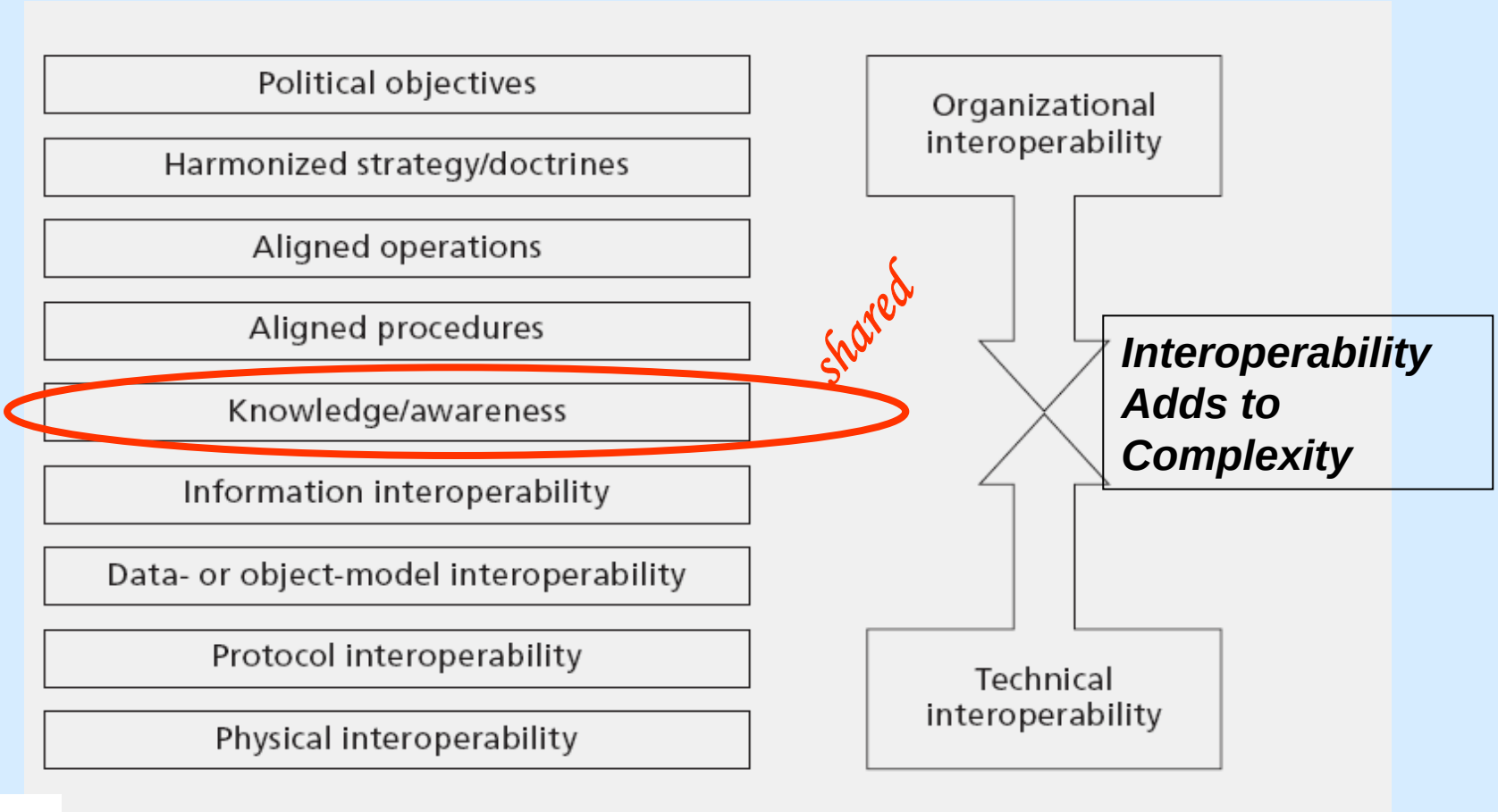
Connectivity Challenges for OTM: Wireless Networks Don't Scale Well

The Penalty is Throughput



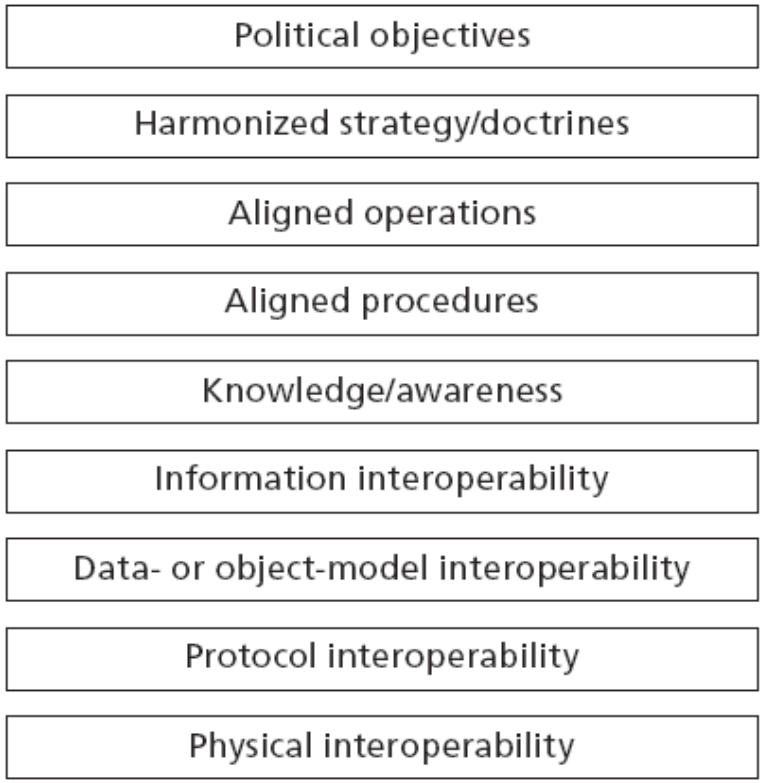
Ref: Joe and Porche, 2004

Meaningfully Increased Connectivity Requires Interoperability



Interoperability is Lacking at Many Layers/Levels

Lack of Interoperability is a Security Feature

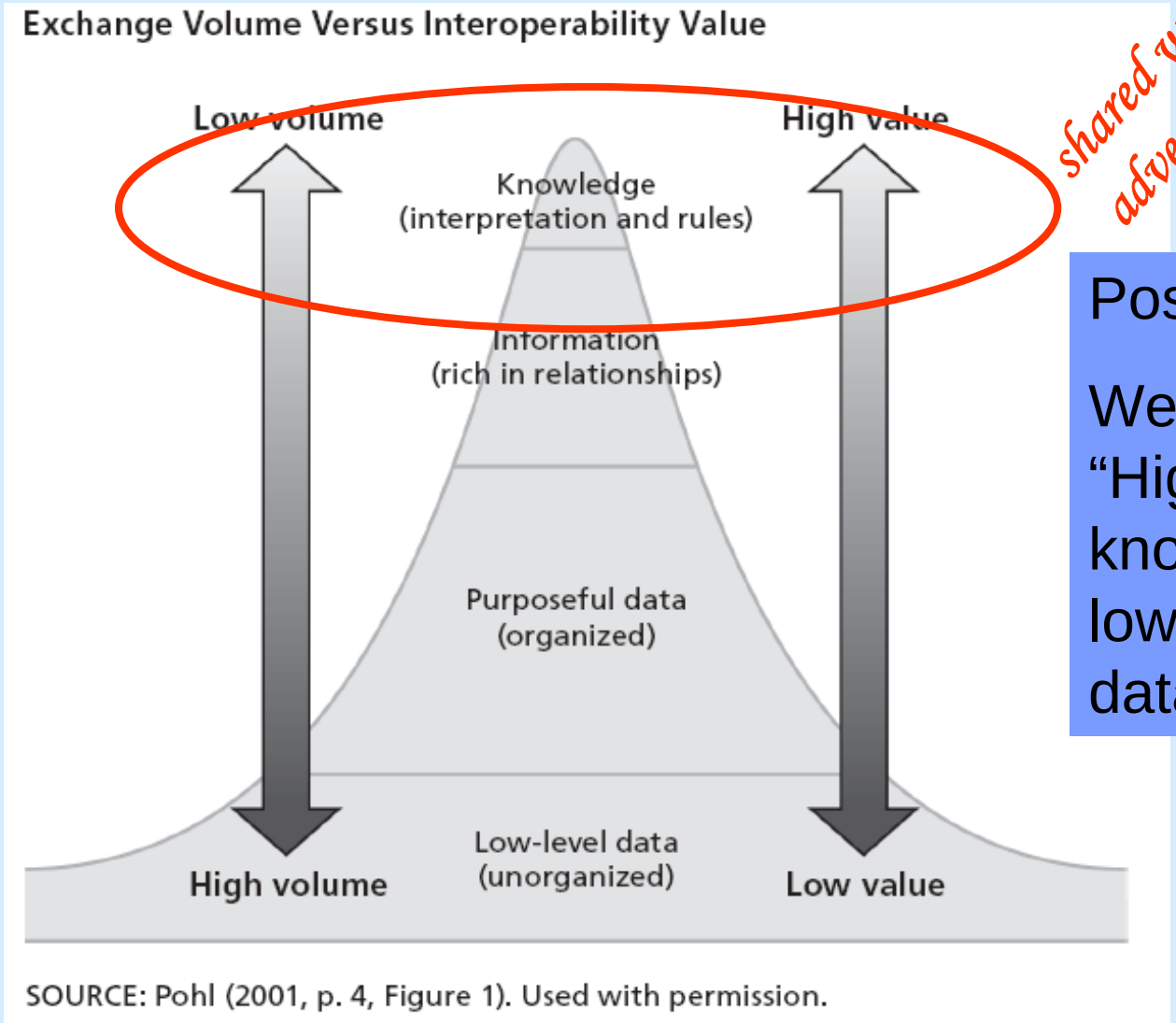


Tolk and Muguira (2003).

Open Question:

What happens when/if interoperability is fixed before we can protect our networks and repositories from compromise ?

Lack of Interoperability is a Security Feature (cont.)

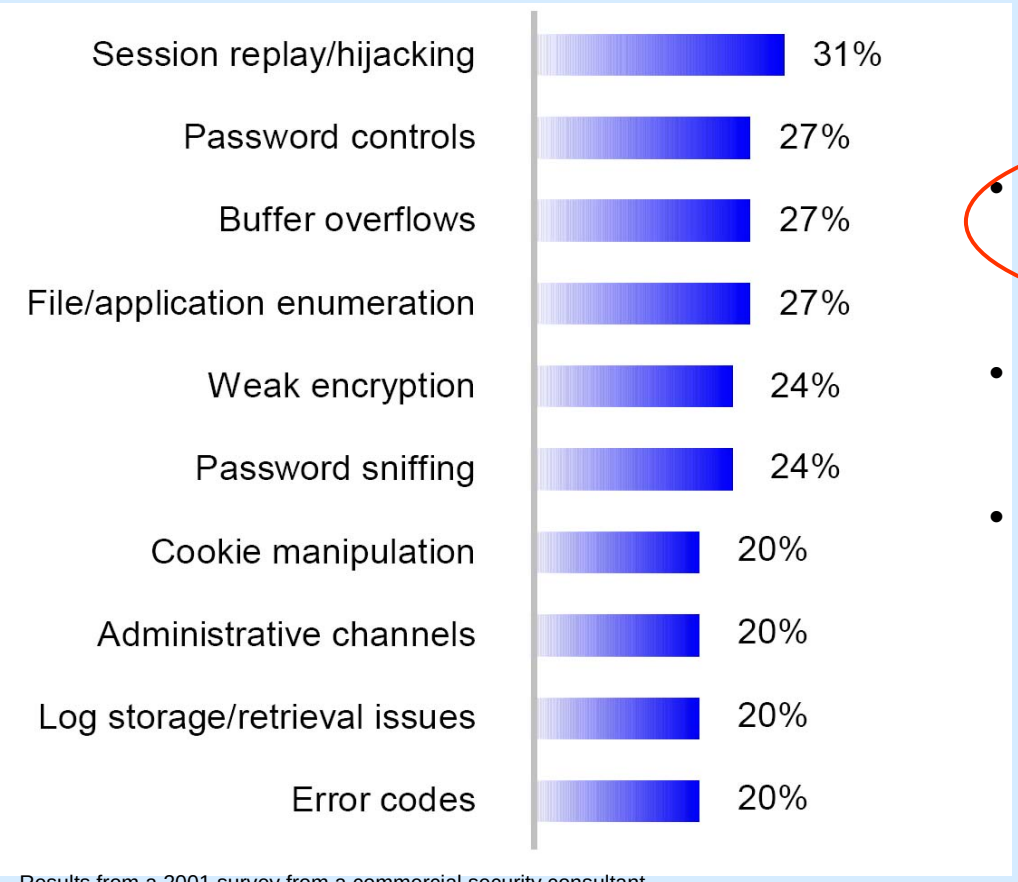


SOURCE: Pohl (2001, p. 4, Figure 1). Used with permission.

Possible Answer:

We could lose more "High value" knowledge (instead of lower valued info and data).

COTS Applications are Sources of Vulnerability



Results from a 2001 survey from a commercial security consultant

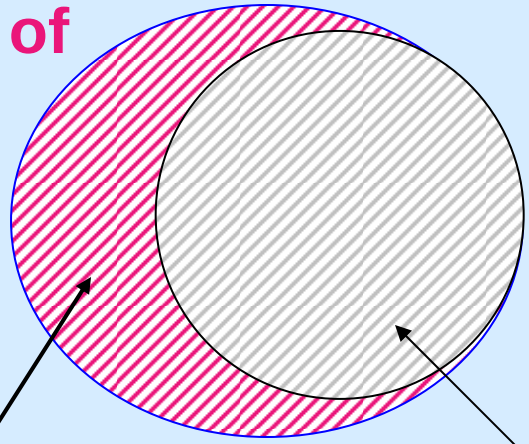
This is why COTS reliance is troubling

- Companies treat security as a "penetrate and patch" activity done *after* the application is deployed.
- Application security flaws are generally introduced early in the design cycle.
- Typical COTS applications may be "at serious risk."

*Source: Jaquith, Andrew, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, 2002.

Application Complexity is a Particular Culprit

The Crescent of Vulnerability



System functionality

Anticipated & Modeled functionality

Service Oriented Architectures (SOA) promise unanticipated functionality – which the commercial world has found to be a source of vulnerability

*The "Farewell Dossier" Example: A Reminder on the Threat from Malicious Code**

- Trojan horse was inserted into Canadian software designed for control of natural gas pipelines
- Software was "allowed" to be stolen and used by the Soviets with explosive results

Source: https://www.cia.gov/csi/studies/96unclass/farewell.htm

Reed, Thomas, *At the Abyss: An Insider's History of the Cold War*, Random House, 2004

Access to Information is Equated to Access to the Network

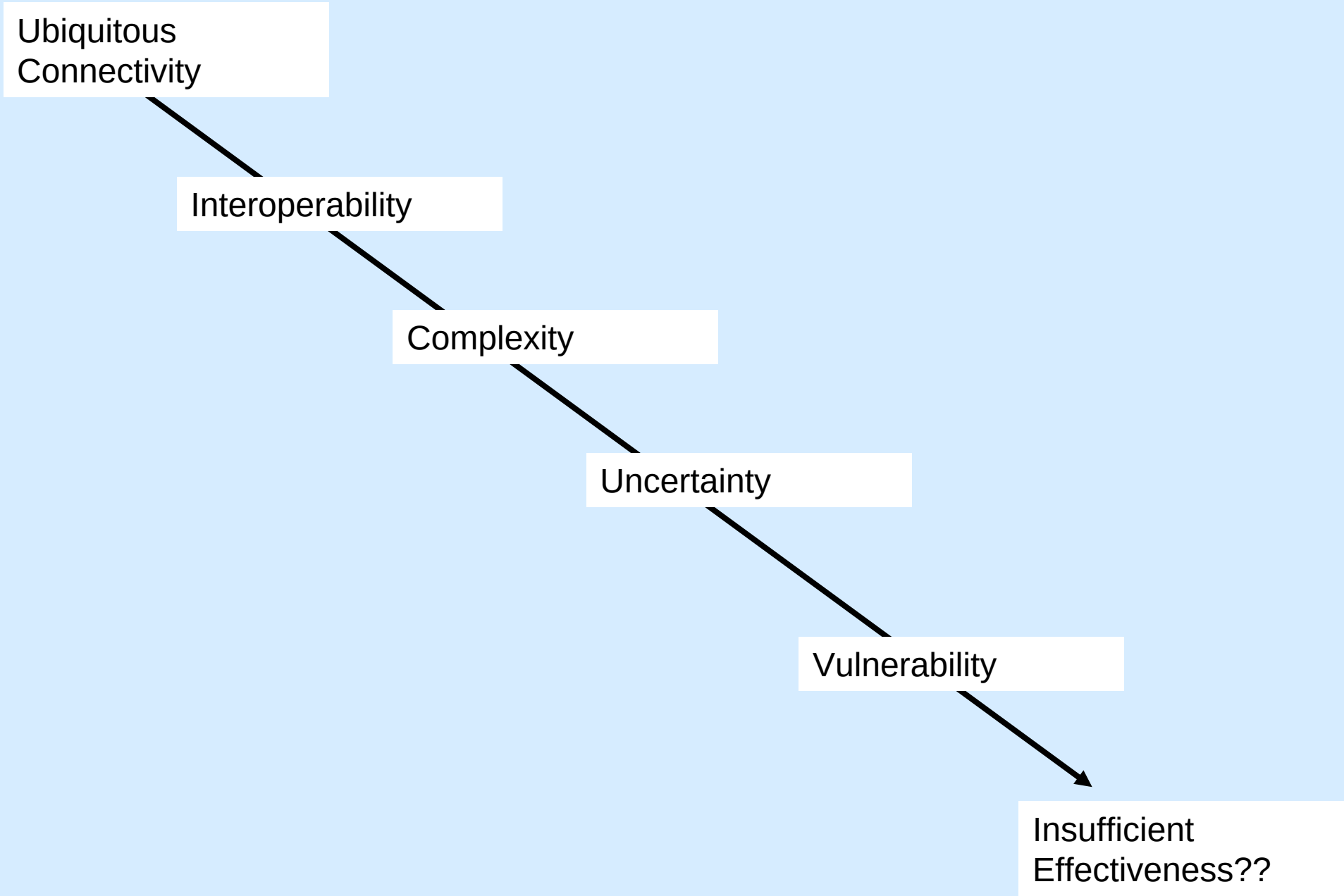
Today's [USG] information systems are air-gapped

- *Quoting: "Many critical [USG] information repositories are not compatible with the analytic tools, and many still are air-gapped and not accessible online to analysts." (Markel Report, P. 22)*

Fixing the Trade-off May Involve...

1. New systems that control access to the data, not access to the whole network (9/11 Commission report, p 418)
   - "Transactional access control" techniques
     - e.g., RAdAC
2. Philosophical shift from "need to share" vs. "need to know"
   - Includes revisiting what information has to be secured
3. Quantitative/Analytic network design tools that can model both user behaviors and network performance
4. Robust IA and CND

Are We Headed Down This Path?



Questions and Comments

References

- Aviation Week, 100329 and 100524
- DSB, Task Force on the Acquisition of Information Technology, 3/09
- F-18 G Picture, http://www.boeing.com/companyoffices/gallery/images/military/ea18g/C22-658-19.html
- Ittig, Kristen, Ronald A. Schecter, and Suzanne Sivertsen, “House Armed Services Committee Unanimously Approves Defense Acquisition Reform”, April 2010, Arnold and Porter, LLP, Advisory
- Giffin, R. E., and D. J. Reid, “A Woven Web of Guesses, Canto One: Network Centric Warfare and the Myth of the New Economy,” 8th International Command and Control Research Symposium, Washington, D.C., C4ISR Cooperative, Research Program (CCRP), 2003.
- Gilder, George, “Metcalfe’s Law and Legacy,” Forbes ASAP, September 13, 1993.
- Government Accountability Office (GAO), Recent Campaigns Benefited from Improved Communications and Technology, but Barriers to Continued Progress Remain, GAO-04-547, June 2004.
- HASC Panel on Acquisition Reform, March - 2009
- JCIDS Summary View, DAU Repository, https-//acc.dau.mil/ as of 100512
- Joe, Leland and Isaac Porche, Future Army Bandwidth Needs and Capabilities, Santa Monica, Calif.: RAND Corporation, MG-156-A, 2004, available at http://www.rand.org/pubs/monographs/MG156/index.html
- Inside the Air Force, 12/18/2009, “AFMC Building an Acquisition Plan for Cyber Purchases”
- Markle Foundation, Creating a Trusted Network for Homeland Security, New York, 2003. As of October 25, 2007: http://www.markle.org/downloadable_assets/nstf_report2_full_report.pdf
- National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States, Washington, D.C.: U.S. Government Printing Office, 2004. As of December 26, 2007: http://www.gpoaccess.gov/911/
- NRC, Report re Achieving Effective Acquisition of DoD IT, 2010
- Porche, Isaac, and Bradley Wilson, The Impact of the Network on Warfighter Effectiveness, Santa Monica, Calif.: RAND Corporation, TR-329-A, 2006, available at www.rand.org/pubs/technical_reports/TR329/
- RAND Arroyo Center, A Campaign Quality Army: Annual Report 2005, available at www.rand.org/pubs/annual_reports/2006/RAND_AR7110.pdf
- Tolk, Andreas, “Beyond Technical Interoperability: Introducing a Reference Model for Measures of Merit