TRANSFORMING NATIONAL SECURITY SEMINAR SERIES

Cyberpower and National Security

A National Defense University and Forces Transformation and Resources Seminar
Marshall Hall Room 155, Fort Lesley J. McNair, Washington, DC 20319
April 30-May 1, 2008

DAY 1 – April 30, 2008

0800 **Opening: General James Cartwright,** Vice Chairman of the Joint Chiefs of Staff

0830 **Towards a Preliminary Theory of Cyberpower: Dr. Stuart Starr** – Senior Research Fellow, CTNSP, NDU

0900 **Cyber Future**
White House Perspective: **Mr. Leon Fuerth**, Research Professor, Elliot School of International Affairs, GWU
Policy Issues: **Dr. David Clark** – Senior Research Scientist, MIT Computer Science and Artificial Intelligence Laboratory; **Marjory Blumenthal** – Associate Provost, Georgetown University

1000 **Plenary: Representative Adam Smith, D-WA**

1030 **Break**

1045 **Cyber Security: Key Steps for the Future**
Protecting Critical Infrastructure: **Mr. William D. O'Neil,** Consultant
Defending Cyberspace: **Mr. Andy Purdy, Esq., CISSP**, Executive Advisory Board, BigFix, Inc.; President, DRA Enterprises, Inc.; Partner, Allenbaugh Samini, LLP

1145 **Lunch Speaker – Ms. Melissa Hathaway,** Cyber Coordination Executive, Office of the Director of National Intelligence and Director of the Joint Interagency Cyber Task Force

1300 **Deterrence and Response**
Policy Issues: **Dr. Richard Kugler,** Consultant and former Distinguished Research Fellow, CTNSP, NDU
Legal Issues: **Mr. Thomas Wingfield,** Associate Professor, US Army Command and General Staff College

1400 **International Issues**
Moderator: **Dr. Hans Binnendijk**, Director, CTNSP, NDU
NATO: **Mr. Mark Hall**, Director, Information Assurance Policy and Strategy Office of the Assistant Secretary of Defense
Governance: **Mr. Hal Kwalwasser,** Independent Consultant

1530 Break

1545 Cyber and Irregular Challenges (1)
Terrorists: **Dr. Irving Lachow**, Senior Research Professor, IRMC, NDU
Criminals: **Dr. Clay Wilson**, Research Specialist, Congressional Research Service

1700 End Day One

DAY 2 – May 1, 2008

0815 Cyber and Irregular Challenges (2)
SSTR: **Mr. Larry Wentz,** Senior Research Fellow, CTNSP, NDU
HA/DR: **Dr. Linton Wells,** Distinguished Research Fellow, CTNSP, NDU

0930 Cyber and State Perspectives
USG Risks: **Dr. Martin Libicki,** Senior Management Scientist, RAND
Near Peers: **Mr. Timothy Thomas,** Senior Analyst, Foreign Military Studies Office, Fort Leavenworth

1100 Break

1115 DOD Perspectives
ASD-NII: **Mr. Robert Lentz,** Deputy Assistant Secretary of Defense for Information and Identity Assurance
Joint Staff J-5: **Captain Daryl Caudle, USN**
Services: **Dr. Daniel Kuehl,** Director, Information Operations Program, IRMC, NDU

1230 Lunch and Conclusions
Lessons Learned: **The Honorable Franklin D. Kramer,** Independent Consultant and former Assistant Secretary of Defense for International Security Affairs

1400 End Day Two

Towards a (Preliminary) Theory of Cyberpower

Dr. Stuart Starr
Center for Technology and National Security Policy (CTNSP)
National Defense University (NDU)

April 30, 2008

Objective, Approach

- Objective
  - "… there is a compelling need for a **comprehensive, robust and articulate cyber power theory** that describes, explains and predicts how our nation should best use cyber power in support of US national and security interests" (2006 QDR)
- Approach
  - Multiple workshops were convened to develop the chapters of a book
  - This was complemented by three efforts; we
    - Drew insights from observations of events, experiments, and trends
    - Built on prior national security methods, frameworks, theories, tools, data, and studies
    - Formulated and hypothesized new methods, frameworks, theories, and tools to deal with unexplained trends, issues

Why a Theory?

- A Theory of Cyberpower will serve to
  - Define
  - Categorize
  - Explain
  - Connect
  - Anticipate
- However, as a caveat, any preliminary theory of cyberpower will
  - **Not** be complete
  - Be, at least, somewhat **wrong**

Cyber Theory Challenges

- Timeframe: several decades
- Discipline: subsumes multiple disciplines (e.g., hard and soft sciences, professions), most of whom can not communicate effectively
- Definitions: most basic terms are still contentious
- Categorize: no agreed upon taxonomy
- Explain, anticipate
  - The field is changing exponentially (in the midst of “a tipping point”)
  - Little or no agreement on key frameworks
  - Ability to explain is limited, particularly for social science aspects
  - Reliable prediction is infeasible
- Connect: A holistic perspective has not yet been created

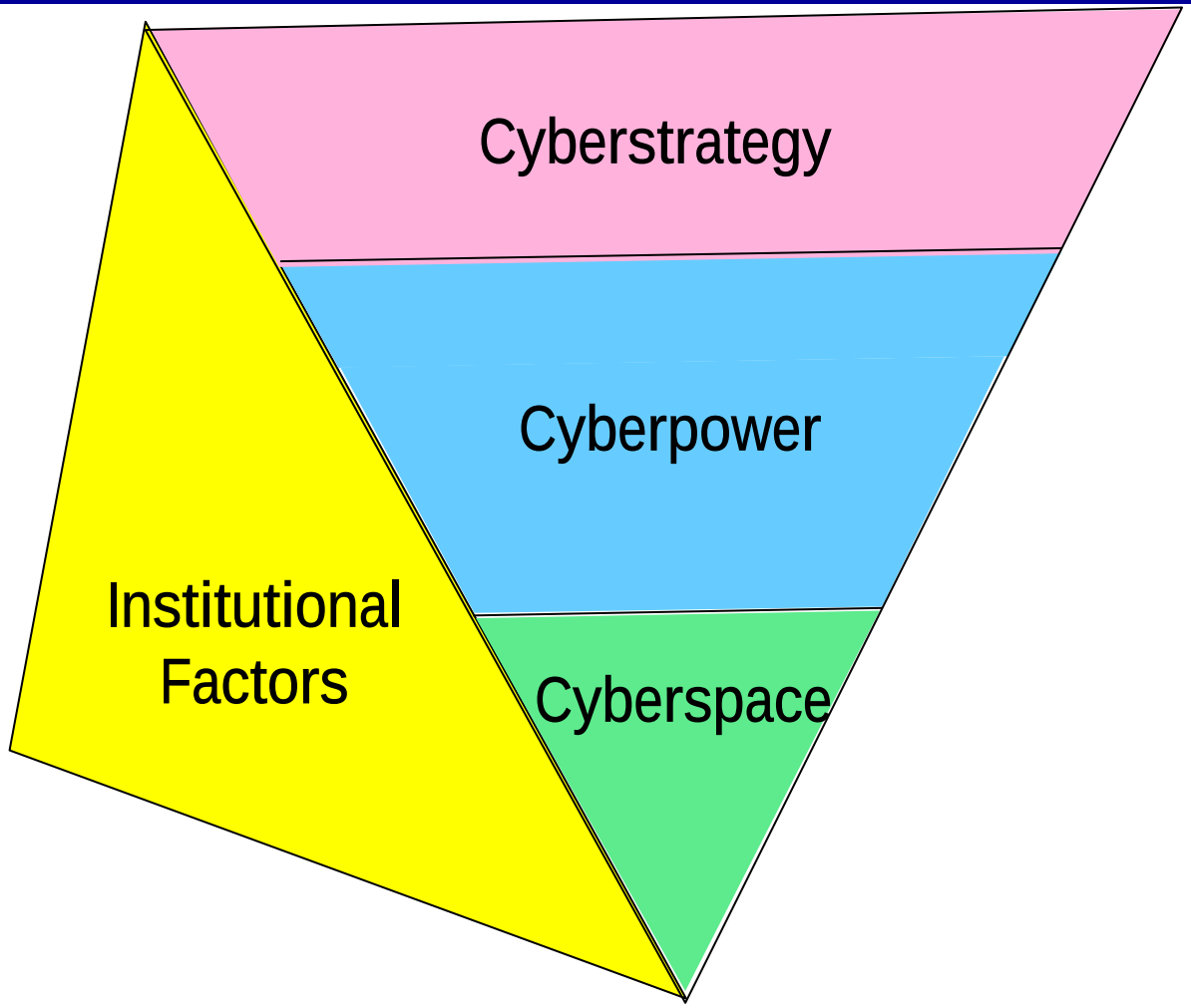
Cyberspace is Changing *Rapidly*

A Theory Will Serve to *Define*…

- Cyberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and internetted information systems and their associated infrastructures."
- **Cyberpower** is the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power
- **Cyberstrategy** is the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power

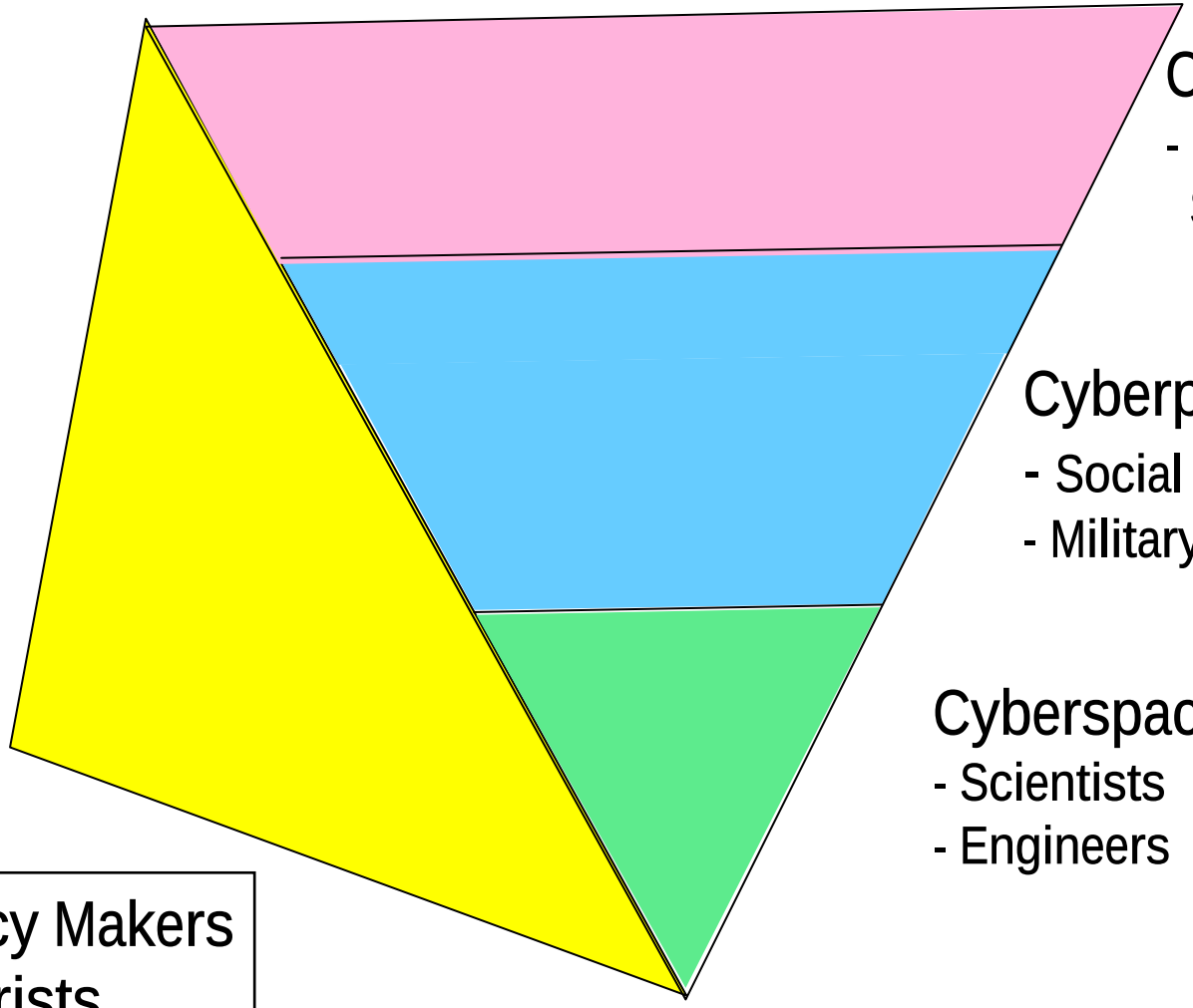
Source: Dan Kuehl

A Theory Should Serve to *Categorize (Classes)*



"All models are wrong; some are useful" George Box

A Theory Should Serve to *Categorize (Intellectual Capital)*



Cyberstrategy:
- Interdisciplinary SMEs

Cyberpower:
- Social Scientists
- Military Analysts

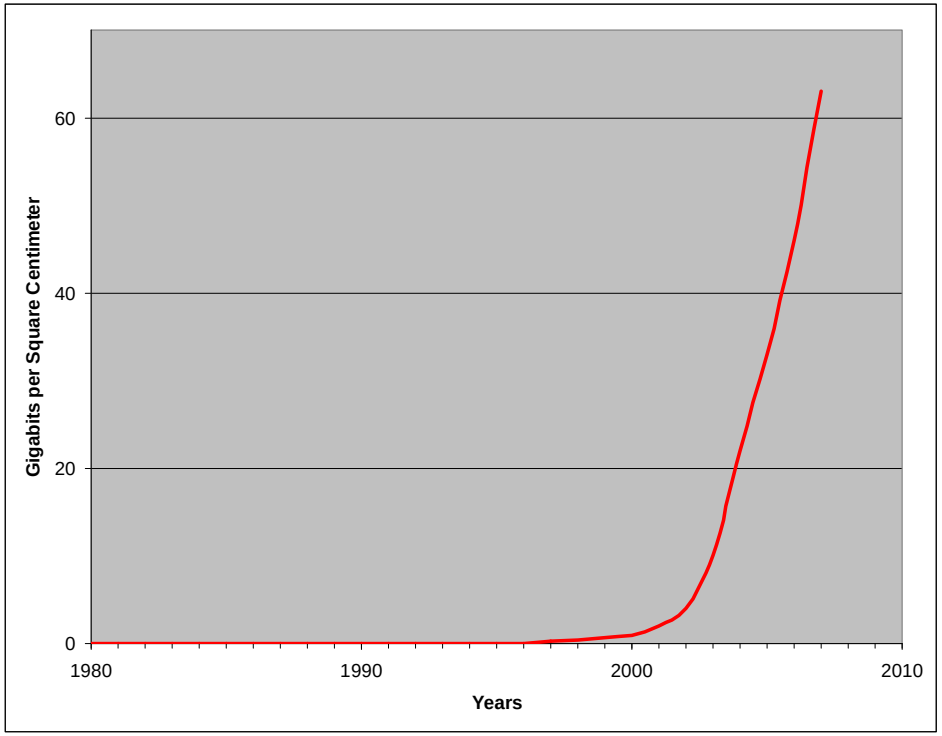
Cyberspace:
- Scientists
- Engineers

Institutional Factors:
- Lawyers
- Industry
- Civil Liberties

Users: Policy Makers
Other: Futurists

A Theory Will Serve to *Explain*: Cyberspace (1 of 2)

- Cyberspace "rules of thumb"; e.g.,
  - Moore's Law (e.g., design of micro-electronics)
  - Proliferation of IP addresses (in transitioning from IPv4 to IPv6)
  - Increase in hard drive capacity (2007 Nobel Prize in Physics)



Introduction of Giant-Magnetoresistance Drives
(Gigabits/cm^2 vs. Time)

A Theory Will Serve to *Explain*: Cyberspace (2 of 2)

- Strawman "principles of conflict"
  - The offensive has the advantage; e.g.,
    - "Target rich" environment (difficult for defense to prioritize, defend selected targets) (Will O'Neill)
    - Challenges of attribution (Ed Skoudis)
  - If cyberspace is to be more resistant to attack, it may require a new architecture that has "designed in" security (Marjory Blumenthal, Dave Clark)
  - It will be a challenge to transition from the current legacy system to a more secure objective system

A Theory Will Serve to *Explain*: Cyberpower

- "Rules of Thumb" for Cyberpower
  - Regard "Metcalfe's Law" as a myth (i.e., "value" varies as N^2)
- Selected observations on military effectiveness
  - (Greg Rattray) Studies of prior military theories (e.g., Mahan and Sea Power) have served to identify
    - Key factors of cyberpower
    - The need for risk assessments
  - In net-centric operations (NCO), the network helps, but it is not clear in what way (Martin Libicki)
  - "I-Power" can be the basis for enhanced performance in SSTR and HA/DR operations (Larry Wentz, Lin Wells)
- Selected observations on Information operations (Frank Kramer, Larry Wentz, Stuart Starr)
  - Based on operational objectives, there is a need for changes in Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, and Facilities (DOTMLPF)
  - "New media" have the potential to revolutionize strategic communication

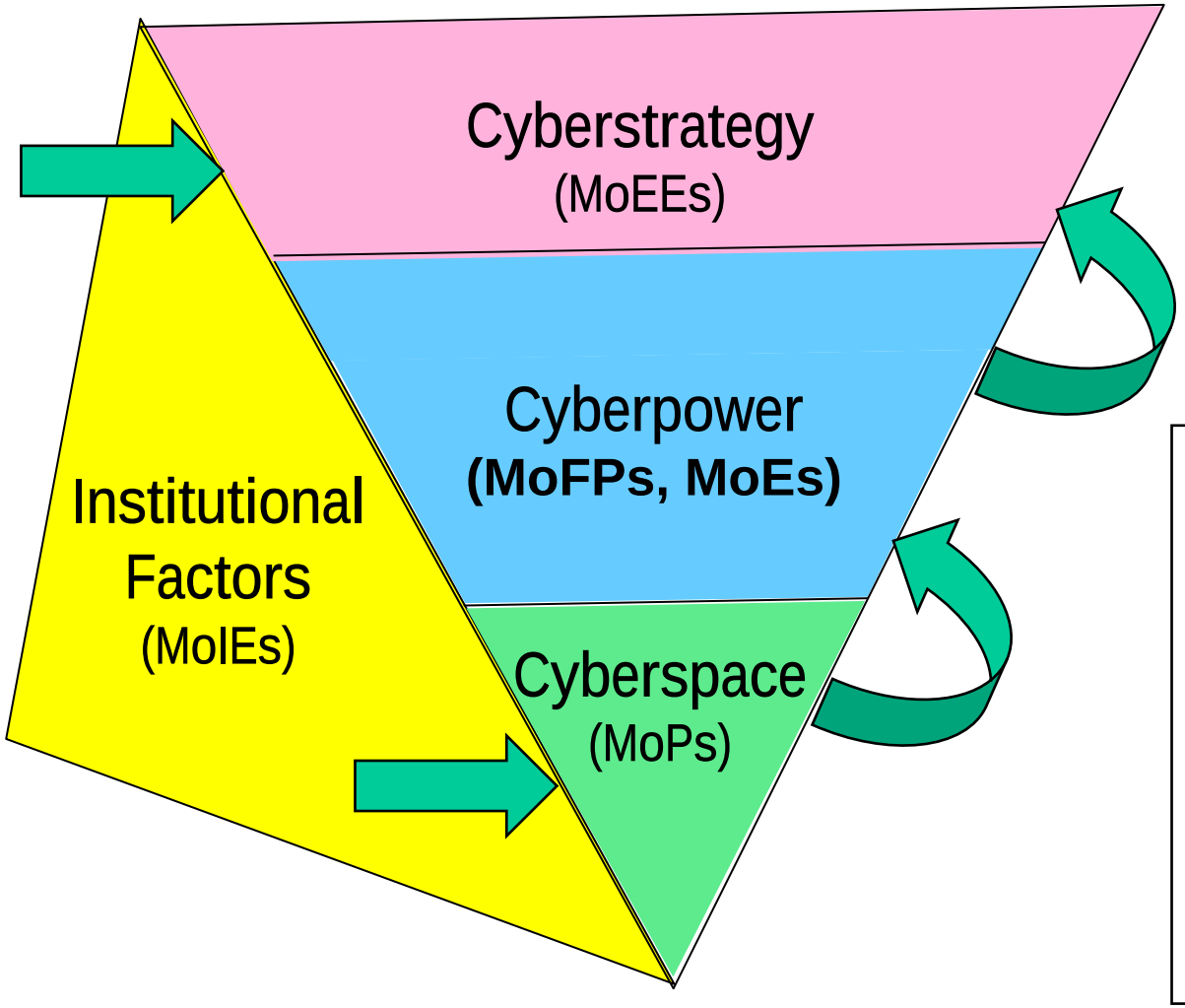
A Theory Will Serve to *Explain*: Cyberstrategy

- The “low end” users (e.g., individuals, hacktivists, terrorists (Irv Lachow), trans-national criminals (Clay Wilson)) have enhanced their power considerably through recent cyberspace trends
- Potential near-peer adversaries are aggressively exploring options to exploit attributes of cyberspace (e.g., exfiltration of data; implementation of innovative cyber strategems) (Tim Thomas)
- In light of the 2007 attack against Estonia, NATO is rethinking its cyber policy (e.g., Bucharest communique, creation of a Cyber Defense Management Authority) (Hans Binnendijk, Mark Hall)
- A theory of “cyber-deterrence” is beginning to emerge, drawing on all levers of power (Richard Kugler)

A Theory Will Serve to *Explain*: Institutional Factors

- Given the complexity of the governance mechanisms, one should seek *influence* over cyberspace vice *governance* (Hal Kwalwasser)
- The legal community has just begun to address the key cyber issues that must be resolved during the next decade (Tom Wingfield) ; e.g.,
  - What is an act of (cyber)war?
  - What is an appropriate response to a “cyber attack”?
- Guidance and procedures are required to address the issues of risk management and sharing of cyber information between the USG and industry (Andy Purdy)
- There is a need for a framework and enhanced dialogue between champions of civil liberties and proponents of enhanced cyber security to establish an adequate balance

A Theory Should Serve to *Connect*



Legend:

MoPs: Measures of Performance

MoFPs: Measures of Functional Performance

MoEs: Measures of Effectiveness

MoEE: Measures of Entity Empowerment

MoIE: Measures of Institutional Effectiveness

A Theory Will Serve to *Anticipate*: Policy Recommendations

Category	Area/ Recommendations
Cyberspace	• Security/ USG should adopt "differentiated security" approach • Resources/ Establish national Cyber Labs; substantially increase R&D funding for governmental agencies; enhance private sector activities
Cyberpower	• NCO/ Address risks (e.g., exercise against highly capable cyber-warriors) • Computer Network Attack (CNA)/ Review definitions, classification level, integration into operations • Influence Ops/ Adopt a holistic, multi-disciplinary, interagency approach • Stability, Security, Transition, Reconstruction (SSTR)/ Adopt I-Power approach
Cyberstrategy	• Organization/ Create a new, interagency Cyber Policy Council (Leon Fuerth) • Deterrence/ USG should adopt a much more robust deterrence policy (e.g., generate capabilities; undertake political action) • Espionage/ Conduct policy-legal review
Institutional	• Governance/ Develop strategy for Internet *influence* • Legal/ Clarify definitions, reconcile international and sovereign law • Critical Infrastructure Protection/ Implement effective public-private partnership

Frank Kramer, Bob Lentz, CAPT Daryl Caudle

A Theory of Cyberpower: Residual Challenges

Area	Assessment	Residual Challenges
Define	Green-Amber	• Rationalize key definitions (e.g., cyber; domain; information operations)
Categorize	Green-Amber	• Develop a family of frameworks to address various policy issues
Explain	Green-Amber	• Address a variety of topics that have not been treated in the book (e.g., civil liberties; diplomatic, economic issues)
Connect	Red	• Develop appropriate Measures of Merit (MoMs) and explore their linkages
Anticipate	Red-Amber	• Improve assessments of highly non-linear trends

Summary

- The CTNSP Team has
  - Developed a **preliminary** theory of cyberpower
  - Generated a book on the subject that consists of approximately thirty chapters
  - Identified many key cyber policy issues and formulated preliminary recommendations
- However,
  - Considerable effort is required to enhance the evolving theory of cyber
  - Many of the key policy issues require additional analyses

The Future of the Internet and Cyberpower

Marjory S. Blumenthal

David D. Clark

April-May 2008

Whence the Future?

- Yes, technology change, and also . . .
- Decisions and interactions of many
  - Researchers/innovators
  - Investors, evolving industries
  - Gov't entities at all levels—and many nations
  - Individual and organizational users of all kinds
- In a key of C: conditions for connectivity, content, cognition, choice, credibility ➔ *cyberpower*

Internet as Platform for Cspace

- Cspace as sequence of platforms, emergent
  - Wireless, SCADA, and more + the Internet
  - Computing is evolving—the PC no longer rules
  - The Internet is evolving—it is not static
    - It may become less general or general in different way
    - Alternatives mean different things for security, management, and economics
- Policy leverage over the Internet is limited
  - Too many aspects are changing together
  - Points of control are few and often indirect

Information and User Experience

- More ways of collecting, finding, and transmitting more kinds of information
  - Sensors, Google, blogging, personalized content.
  - Blind you, lie to you, induce hallucinations—trust is key
- Focus on info substructure—servers as sources:
  - Where are they located? Who controls the servers and what they do?
  - More in-region variation in user experience
- Augmented reality creates new venues
  - Do new venues generate/reinforce new allegiances?
- Digital divide: Who goes to cyber, how?
  - What happens to the others?

Security Challenges

- Theme for the conference—our key points:
  - Communication is risky, do it w/o full trust
  - Trust for collective action, collaborative
  - Balance of mechanisms in net and in device
  - Need not standardize fully
    - Opportunities for national variation
  - Designs vary re opportunities for different actors to exercise control or power
  - Shifting power balance between citizen + state

Private Sector Investment

- They who pay . . .
- Will the Internet be open?
- Who is (in) the Internet industry?
- What about advertising?
- What options do consumers have?
  - Who owns and controls in-home devices?
- Where is or can be Internet regulation?
  - Law enforcement, nat'l sec/emerg prep, governance, ...
- Gov't-targeted promotion of investment?
- By-country and international action

Research Health/Character

- Basic research is at risk—it can be a tough policy sell, esp. when funds are scarce
- Industrial labs have limits—gov't funding of academic research promotes creativity
- Planning international cyberspace research is difficult
  - Collaboration v. competition
- Key research topics are forks in the road—security, provenance, identity, location awareness, open sensor networks, . . .

Questions

- What is a “good” cyberpower outcome? How can agreement across sectors and at least some nations be fostered?
- How can the US Government—itself having competing interests—promote more secure Internet architecture design and deployment?
- How can national security entities coordinate more effectively with commercial and non-profit members of the Internet community to promote favorable cybersecurity outcomes?

Infrastructure & Cyberpower

Will O'Neil
http://www.analysis.williamdoneil.com/
w.d.oneil@pobox.com

30 April 2008

Infrastructure & Cyberpower

- Counter cyberattack *against* infrastructure
- Infrastructure *for* cyberpower

Introduction/Overview

- Networks and infrastructures
- Electric grid – most central infrastructure
- Other infrastructures
- Policy issues

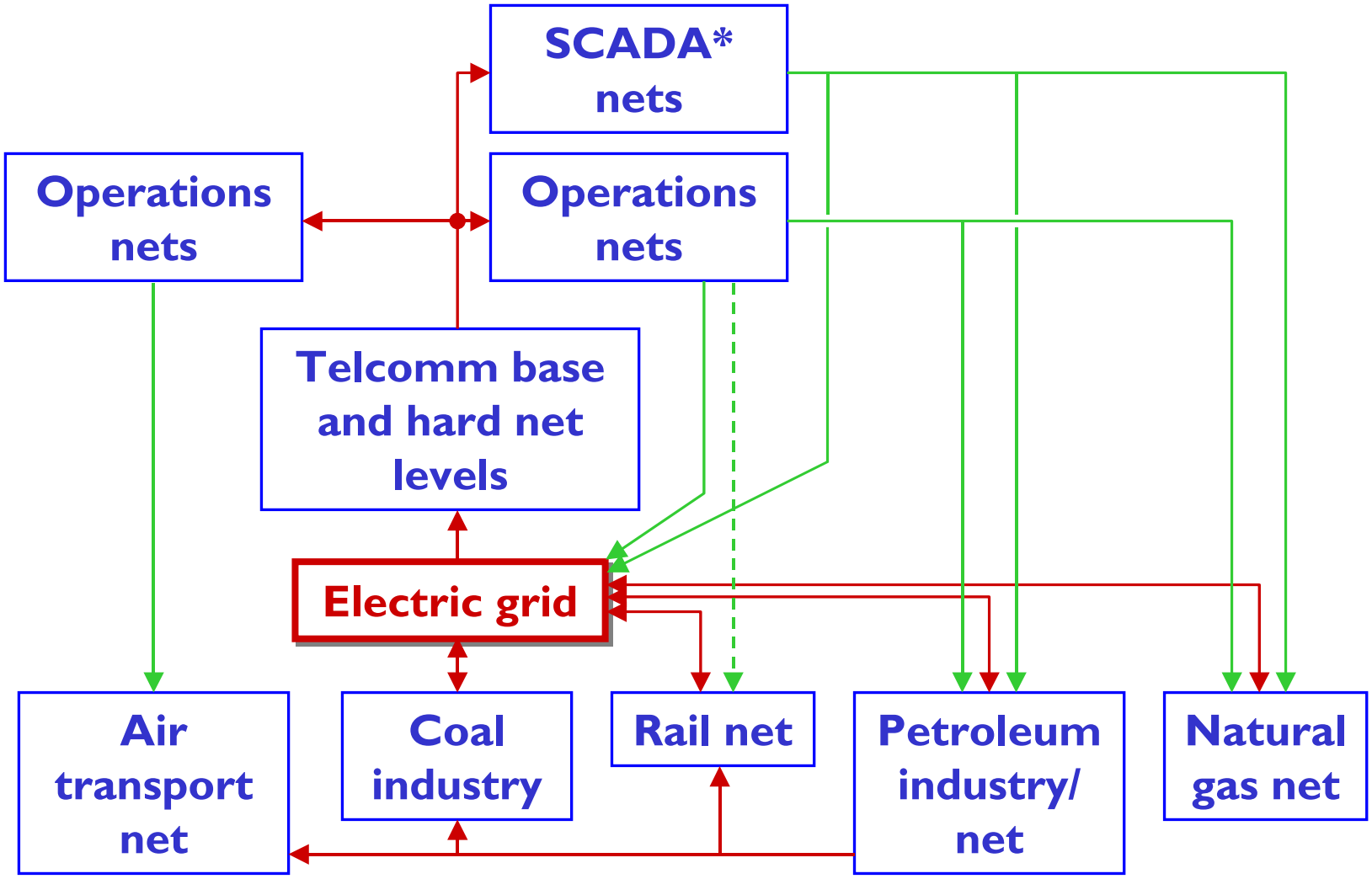
Infrastructure : Network

- Almost always
- Network properties make a difference

Q: Does networking favor survivability or vulnerability?

A: It all depends…

Selected Dependencies



* Supervisory Control and Data Acquisition

Controls

- System isolation & “shorts”
- Complexity & automaticity
  - Time constants
- Authority to do harm?
- Hackattacks
  - Nuisance, not menace (so far)

Controls threats

- Short-term system outage
  - Take system down as part of coordinated attack plan
- Disable protective function
  - In coordination with physical attacks to stress system
  - Could greatly increase damage, lengthen recovery

Controls attacks most potent *in conjunction with* physical attacks

In the Near Term

- Cautious steps toward reliability requirements
  - North American Electric Reliability Corp. (NERC) designated U.S. Electric Reliability Orgn (ERO)
  - Under Fed'l Energy Regulatory Commission (FERC) authority
  - Hope to expand continent-wide
- Emphasis on tight operating standards & training
  - Grid expansion urged
- Divided, overlapping responsibilities remain
  - FERC, DoE, DHS, States

Infrastructure Policy Issues

National security not unique

- Threats/ Challenges
- Authority/ Incentive
- Knowledge

Cyber Issues
Infrastructure

- Physical threats primary
- Cybersec important adjunct
  - Threat synergies

Summary/Overview

- Networks and infrastructures
- Electric grid – most central infrastructure
- Other infrastructures
- Policy issues

“Lessons from Defending Cyberspace”

Andy Purdy, Esq., CISSP
President, DRA Enterprises, Inc.
BigFix Executive Advisory Board
Allenbaugh Samini, LLP

Public Policy Challenge

- Nation is dependent on cyber for national security, economic well-being, public safety, and law enforcement
- Risk is real but not visible and obvious
- Authority and control is spread among multiple entities in the public and private sectors
- Cyber is international
- Individuals and organizations are reactive and tactical
- We do not learn lessons from the past

Threat versus Risk

- Traditional model has been to react to known or perceived threats
  - “Threat” - intent and capability of malicious actors
- Key lesson we must learn and operationalize is to use a risk management approach at the organizational, national, and international levels
  - “Risk” - threat, vulnerabilities, and consequences

What is our operating premise?

- Will it take a cyber calamity to drive an effective approach?
- What can we expect to happen if there is a cyber disaster?
- How can we use that reality to drive action?

What is missing?

- What do we need to worry about and what do we need to do about it?

What do we need?

- Need a public-private strategic approach to collaboration and information sharing to set requirements for action that can be tracked and measured
  - Risk assessment - assess and mitigate risk,
  - Common operating picture - build capability for situational awareness/ability to detect, analyze, respond and recover
  - Research and development – develop and implement a national cyber R&D plan

www.andypurdy.com

Andy Purdy

President, DRA Enterprises, Inc.

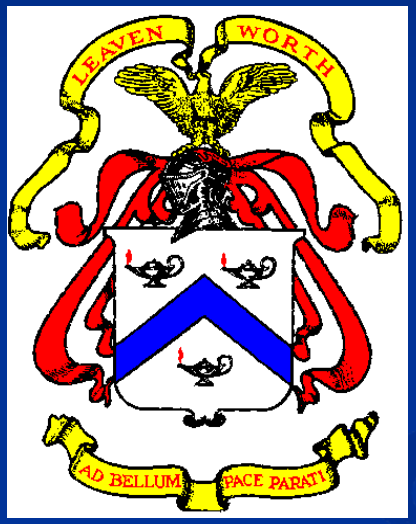
BigFix, Inc. Executive Advisory Board

Andy.Purdy@andypurdy.com

Allenbaugh Samini, LLP

www.alsalaw.com

War and Peace (Abridged): Information Operations and International Law



Thomas C. Wingfield, Esq.
Associate Professor
U.S. Army Command and General Staff College
Fort Belvoir, Virginia

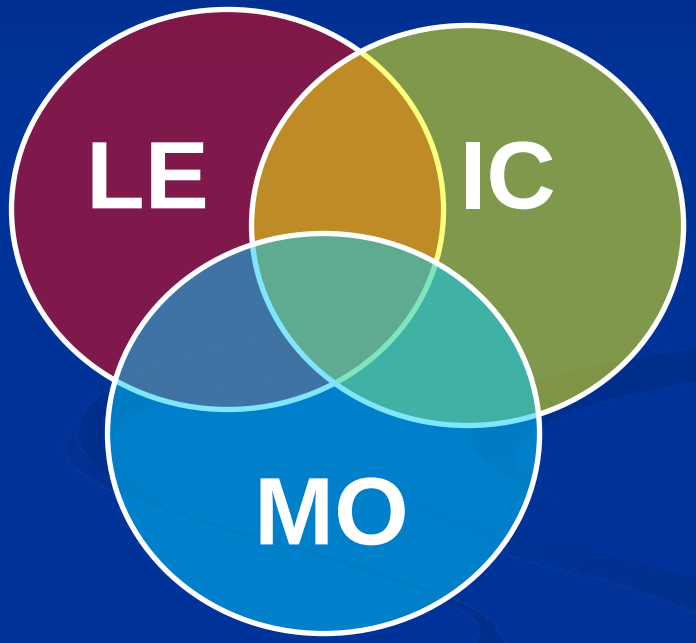
April 30, 2008

Overview

- Three Regimes
- Levels of Law
- Peacetime Rules
- Transition to War
- Wartime Rules

Three Regimes

- Law Enforcement
  - Title 18
- Intelligence Collection
  - Title 50
- Military Operations
  - Title 10



Levels of Law

- Domestic
  - Federal
  - State
- International
  - Treaty
  - Customary
- Foreign Domestic
  - Target Country
  - Third Country

Jus ad Bellum

- Criteria for self-defense
  - Necessity
    - Exhausting all reasonable peaceful alternatives before resorting to force
  - Proportionality
    - Using only that amount of force required to end the immediate threat
  - Imminency
    - Acting only when the aggressor has irrevocably committed itself to attack

Transition to War

- In peacetime, legality of self-defense is determined on an incident-by-incident basis
- During armed conflict, all combatants and military objectives become lawful targets of belligerents until effective cessation of hostilities
- How do we know when the violence is generalized enough to make the legal transition?
- Pictet Analysis (SDI)
  - Scope
  - Duration
  - Intensity

Jus in Bello

- Discrimination
- Necessity
- Proportionality
- Chivalry

Contact Information

Prof. Thomas C. Wingfield
CGSC Belvoir
Room 185
9265 Belvoir Rd.
Fort Belvoir, VA 22060

thomas.wingfield@us.army.mil

(202) 246-7002

Governance of Cyberspace

Hal Kwalwasser

THE KEY ASPECTS OF INTERNET GOVERNANCE

- Internet Governance is diffuse; many organizations make collective decisions impacting the Internet
- The private sector tends to dominate the decision-making
- The decision-making process is generally long and difficult
- Results are reflected in standards, guidance, and contracts more than in laws or treaties
- Power is generally achieved through individuals who attend meetings regularly, have expertise, and great persistence
- The structures of key organizations heavily involved in Internet Governance are evolving

- *The greatest tension in Internet Governance is the dynamic between establishing and solidifying the legitimacy of current structures and the pressure from foreign governments to increase their ability to control the decision-making process*

KEY INTERNET DECISION MAKING BODIES

- The INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN) and the INTERNET ASSIGNED NUMBERS AUTHORITY (IANA)
  - ICANN was created by the USG in 1998 to oversee the Domain Name System (DNS)
  - IANA predated ICANN but the USG assigned the performance of IANA's functions (i.e., IP addresses, root zone changes, and assignment of protocol parameters)
- THE INTERNET SOCIETY (ISOC), THE INTERNET ENGINEERING TASK FORCE (IETF), THE INTERNET ENGINEERING STEERING GROUP (IESG), and THE INTERNET ARCHITECTURE BOARD (IAB)
  - IETF is the most critical of the groups; it issues standards for voluntary compliance on core Internet operating functions
  - The World Wide Web Consortium (W3C) is not related to IOS but addresses core Web issues
- THE INTERNATIONAL TELECOMMUNICATION UNION (ITU)
  - The ITU is a UN agency that pre-dates both the UN and the Internet
  - It addresses standards and other issues of importance to the telecommunications systems that carry Internet traffic

OTHER INTERNET GOVERNANCE BODIES

- MULTINATIONAL/INTERNATIONAL GOVERNMENT ORGANIZATIONS
  - Organization for Economic Cooperation and Development (OECD)
  - Council of Europe
  - European Union/European Commission
  - United Nations (other than the ITU)

- World Intellectual Property Organization (WIPO)

- NATIONAL GOVERNMENTS

- MULTINATIONAL/INTERNATIONAL STANDARDS ORGANIZATIONS
  - Institute of Electronic and Electrical Engineers (IEEE)
  - International Electrotechnical Commission (IEC)
  - International Organization for Standardization (ISO)

CHARACTERISTICS OF INTERNET GOVERNANCE

- Not speedy
- Stress technical competence and long-term commitment
- World-wide processes, designed to incorporate broad range of views
- All bodies except ICANN and ISO require unanimity or near unanimity
- Private, chiefly commercial, interests dominate
- Governments participate on equal footing in standards bodies except ITU
- Decision-making is fairly transparent but leaders have discretion, and it is not always apparent how it is exercised
- Overlap of subject matters creates some incentive to forum shop

LEGITIMACY TESTS FOR INTERNET GOVERNANCE

- OPEN – ICANN and IETF very open; ITU open to anyone with resources to join and participate. IEEE, ISO and IEC also open
- DEMOCRATIC – ICANN and IETF highly democratic; There are issues:
  - Undue influence arising from USG-ICANN JPA
  - Relatively few people participate extensively enough to have real influence
- TRANSPARENT – Processes are generally transparent; Issues:
  - ICANN-USG JPA an issue
  - Study Group chairs discretion
  - Lack of media coverage
- DYNAMIC – Scaled well; There are issues:
  - System rests on voluntary standards
  - Lack of consensus on emerging problems, such as cyber-crime
- ADAPTABLE – Issues with emerging security problems
- ACCOUNTABLE – Easier to block policies at ICANN and IETF than to hold people accountable, but there is consensus policy generally restraining action
- EFFICIENT – Efficient enough for now; Some governments have not provided “enabling environments” for development
- EFFECTIVE – High marks, with some possible problems in the future

FUTURE CHALLENGES

- ICANN transparency
- USG-ICANN contracts
- Continued collaboration among decision-making bodies
- Continued enforcement of competition policies
- Key players must continue to focus on the overall good of the Internet
- Private sector domination will continue
- Number of key players will not grow unwieldy
- Greater international dialogue on spam and cyber-crime
- Continued widespread support for
  - Deregulation
  - Private enterprise
  - Free markets
  - Free speech
  - Participatory democracy

Cyber Terrorism:

Menace or Myth?

Irving Lachow, Ph.D.

May 1, 2008

Information Resources Management College
National Defense University

Outline

- What is Cyber Terrorism?
  - Definition
  - Cyber Terror vs. Other Cyber Threats
- Is Cyber Terrorism a Serious Problem?
- How Are Terrorist Using the Internet?
- Is Terrorist Use of the Internet a Serious Problem?
- What are US Response Options?
- Discussion

What is Cyber Terrorism?

- Definitions of terrorism:
  - State Dept: "Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience."
  - FBI: "The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."

- Definition of cyber terrorism:
  - Denning: "A computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. *The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism.* Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples... *Attacks that disrupt nonessential services or that are mainly a costly nuisance would not*."

Cyber Terrorism vs. Other Cyber Threats

	MOTIVATION	*TARGET*	*METHOD*
Cyber Terror	**Political or social change**	**Innocent victims**	**Computer-based violence or destruction**
Hacktivism	**Political or social change**	**Decision-makers or innocent victims**	**Protest via web page defacements or DDOS**
Black Hat Hacking	**Ego, personal enmity**	**Individuals, companies, governments**	**Often use malware, viruses and worms, and hacking scripts**
Cyber Crime	**Economic gain**	**Individuals, companies**	**Often use malware for fraud, ID theft; DDOS for blackmail, etc.**
Cyber Espionage	**Economic and political gain**	**Individuals, companies, governments**	**Use wide range of techniques to obtain information.**
Info War	**Political or military gain**	**Infrastructures, IT systems and data (private or public)**	**Use wide range of techniques for attack or influence operations.**

Outline

- What is Cyber Terrorism?
- *Is Cyber Terrorism a Serious Problem?*
  - *Terrorism Risk Model*
  - *Assessment of Current Risk*
  - *Assessment of Future Risk*
- How Are Terrorist Using the Internet?
- Is Terrorist Use of the Internet a Serious Problem?
- What are US Response Options?
- Discussion

Basic Cyber Security Risk Model

- Risk = Threat*Vulnerability*Consequence
  - Threat = Probability that a given attack is launched against a given target
  - Vulnerability = Probability that a given attack against a given target succeeds
  - Consequence = Expected level of damage from a successful attack against a given target
- Countermeasures can be applied against any or all of these three variables
  - Countermeasures usually described in terms of three categories: Protect, Detect, Respond
  - A given countermeasures always carries costs/risks

Risk from Cyber Terrorism Is Currently Low

- No documented cases of cyber terrorism in US or Europe
- Few indications that serious cyber terrorist threats are imminent
- Wargames by Gartner/NWC and NPS both showed that risks of cyber terror are overstated
- Most security experts agree
  - Denning, Lewis, Libicki, Kohlman, Schneier, Weimann, Winkler…
- *Why are risks lower than perceptions indicate?*

Cyber Terrorism vs. Other Attack Vectors

- Cyber Terror Challenges:
  - Nuisance attacks are easy but do not create desired effects
  - Serious attacks are difficult to do and *may* create desired effects
    - Require extensive intelligence gathering, training, and funding
    - Require different skill sets and potential reliance on outside experts
    - Prospects for success and potential outcomes are highly uncertain
  - Bottom line: costs outweigh benefits in most cases
- Explosives Work Very Well
  - Easy to do, require little training, and ops are based upon extensive knowledge base
  - Highly effective at creating terror and getting attention.
- WMD is Another Option
  - Would create tremendous sense of terror and panic
  - Would dominate news for weeks or months
  - Would be huge source of pride

Future Cyber Terrorism Risk May Be Greater

- Trends For Cyber Terror
  - Demographics
  - Growing risk of state sponsorship
  - Outsourcing to hackers and criminals
  - Increased reliance of infrastructures on Internet
  - Growth in software vulnerabilities
  - Technology trends
- Trends Against Cyber Terror
  - Increasing focus on cyber security
  - Growing resilience in infrastructures
  - Technology trends
  - Fundamental challenges remain in place

Outline

- What is Cyber Terrorism?
- Is Cyber Terrorism a Serious Problem?
- *How Are Terrorist Using the Internet?*
  - *Why the Internet?*
  - *Organizational Effectiveness*
  - *Influence Operations*
- Is Terrorist Use of the Internet a Serious Problem?
- What are US Response Options?
- Discussion

Why Do Terrorists Use the Internet?

- Rapid communications
- Low cost
- Ubiquity
- Ease of use + sophistication of tools
- Anonymity
- Social networking

How do Terrorists Use the Internet?

- Organizational effectiveness
  - Communications
  - Fundraising
  - Training
  - Command and control
  - Intelligence gathering
- Influence Operations
  - Create support in general population
  - Recruiting
  - Media relations
  - Counter propaganda

The Internet is enabling networked organizational structures that are extremely difficult to destroy.
(Starfish vs. Spider)

Outline

- What is Cyber Terrorism?
- Is Cyber Terrorism a Serious Problem?
- How Are Terrorist Using the Internet?
- *Is Terrorist Use of the Internet a Serious Problem?*
- What are US Response Options?
- Discussion

Consensus: U.S. is Losing Cyber War Against Terrorists

- Terrorist use of Internet is leading to:
  - A global ideological movement based on a set of guiding principles and beliefs
  - Effective operational structures that support local action without centralized control
  - Effective perception management campaigns that influence target audiences while undermining U.S. interests
- Secretary of Defense Rumsfeld:
  - "If I were rating, I would say we probably deserve a D or D+ as a country as how well we're doing in the battle of ideas that's taking place."
- Dr. Bruce Hoffman:
  - "…the U.S. is dangerously behind the curve in countering terrorist use of the Internet…"

Warfare in the Information Age Is a New Ball Game

- US View = Clausewitz: "War is violence to constrain the enemy to accomplish our will"
  - Information supports kinetics
  - Great for industrial age, not for information age
- Terrorist View = Sun Tzu: "To win 100 victories in battles is not the acme of skill…To subdue the enemy without fighting is the acme of skill."
  - Kinetics support information
  - Great for information age, not for industrial age
- Osama Bin Laden: "It is obvious that the media war in this century is one of the strongest methods; in fact, its ratio may reach 90% of the total preparation for the battles." (Letter to Mullah Mohammed Omar, written prior to 2002)
  - He gets it!

Examples of Terrorist Use of the Internet

- Growth in number and of sophistication of websites and videos
  - Number of web sites grew from around 12 to over 4300 in eight years (Weimann)
  - YouTube
- Evidence of Internet use for kinetic operations
  - 9/11
  - London
- Evidence of kinetic operations supporting info war
  - See videos from Iraq

Outline

- What is Cyber Terrorism?
- Is Cyber Terrorism a Serious Problem?
- How Are Terrorist Using the Internet?
- Is Terrorist Use of the Internet a Serious Problem?
- *What are US Response Options?*
  - *Cyber Terrorism*
  - *Terrorist Use of the Internet*
- Discussion

Treat Cyber Terror as “Lesser Included” Cyber Security Threat

- Focus cyber defense efforts on hacking, crime, espionage, and state-level threats
  - These efforts will also work against cyber terrorism
- Improve resilience of critical infrastructures and key resources
- Use proven counter-terrorism techniques from intelligence and law enforcement
- Explore possible role of pre-emption and deterrence

Counter TUI Via Comprehensive Strategy

- Develop high-level, coordinated strategy for countering terrorist use of the Internet
  - Current efforts are disjointed and occur mostly at operational and tactical levels
- Strategy must maximize benefits and minimize risks/costs of each layer of info environment (infrastructure, content, and cognition)
  - Where appropriate disrupt infrastructure to create fear, uncertainty, and doubt (FUD) about its reliability
  - Attack confidentiality, integrity and availability of extremist information to further increase FUD, gain intelligence and disrupt operations
  - Focus significant time, energy and resources on cognitive domain to impact terrorist decision-making, reduce terrorist influence on stakeholders, and promote US ideas

A Few Recommendations

- US alone cannot counter extremist Muslim ideology
  - Must build up and/or support networks of moderate Muslims and help spread their message
  - Use former terrorists to undermine extremist recruiting
- Need to reset terms of ideological struggle
  - Change language used to describe the players and their actions
  - Focus on things that matter to Muslim audiences (e.g., honor)
- US must adapt to fight a long-term, broad-based “war of ideas”
  - Elevate importance of information component of power in Executive
  - Develop structures, processes, incentives to better coordinate IO, PD, SC
  - Strengthen capabilities of diplomatic corps and the “non-kinetic” abilities of soldiers

Outline

- What is Cyber Terrorism?
- Is Cyber Terrorism a Serious Problem?
- How Are Terrorist Using the Internet?
- Is Terrorist Use of the Internet a Serious Problem?
- What are US Response Options?
- Discussion

Contact Information

Dr. Irv Lachow
Senior Research Professor
Information Resources Management College
National Defense University

Email: lachowi@ndu.edu
Office phone: (202) 685 - 2060
Cell phone: (202) 903 - 7722

Cybercrime Issues, National Defense University, April 2008

Clay Wilson, PhD, CISSP

Analyst, National Security and Information Technology
Congressional Research Service

Opinions expressed are those of the author, and do not necessarily reflect the views of the Congressional Research Service

Trends and Issues

- Cybercrime is now organized, with its own economic structure – suppliers, specialists, recruiters
- Cybercrime is growing in dollar amount, despite policy for cybersecurity
- Cybercriminals have low chance of receiving a penalty
- The public is easily victimized, and poorly informed about cybersecurity threats
- Cybercrime methods evolve more quickly than cybersecurity policy

Policy Questions

- How to respond to a cyberattack – military action, or law enforcement?
- Does the private sector now have a new responsibility to protect national security?
- How can government and private sector cooperate for increased cybersecurity?

Internet Crime Statistics

- GAO reports losses at $49.3 billion in 2006 for identity theft.
- The Internet Crime Complaint Center received 206,884 complaints of online fraud in 2007 - FBI and National White Collar Crime Center
- Banque de France - international credit card fraud has ranged between three and six percent of all international transactions from 2002 to 2006.
- An estimated 250,000 computers are compromised each day by botnets – RSA Conf, 2008

Measures of Cybercrime

- Number of attacks
- Amount of money or IP value stolen
- Cost of resources for recovery after attack
- Costs to Upgrade Security measures
- Organized Crime involvement
- Possible Foreign government involvement

Scope of Cybercrime

- Illegal transfer of electronic funds
- Money laundering
- Identity theft
- Copyright and Trademark violations
- Cable piracy
- Illegal sale/release of Intellectual Property
- Stealing trade secrets electronically
- Software piracy

Latest Methods

- User visits an infected Web site, malware is secretly installed on user's PC
- Spear Phishing – false email messages lure a user into installing malware.
- Botnets – infected PC receives commands from a third party
- Keystroke loggers – malware transmits passwords and account info to a third party

Edit View Favorites Tools Help
Back Search Favorites
Customize Links Free Hotmail Google Windows Windows Marketplace Windows Media CNN.com EllaZ - artful intelligence Forecasting for the Future
http://www.darkcoding.net/credit-card-numbers/

Graham King

Solvitas perambulum

Credit card numbers

Credit card numbers that conform to the Luhn formula (MOD 10 check). Usefull for testing e-commerce sites (because they should get past any pre-validation you do, and be declined at the card processor or bank stage).

In testing situations any expiry date within the next 3 years should work

Feedback forces me to clarify this: These are NOT valid credit card numbers. You can't buy anything with these. They are random numbers that happen to conform to the MOD 10 algorithm. They are a technical resource for programmers - that's all.
Information about CVV2 / CVC / etc numbers can be found here: CVV numbers. As you can see these would be very hard to calculate without the bank's keys.

A very good article about the credit card number format can be found here: Anatomy of Credit Card Numbers

Mastercard	VISA 16 digit
5413260584222277	4539822624744503
5225095384150502	4916793024237088
5122265860613935	4716555929480523
538979822664 1693	4916533057865557
5349807503642017	4 6121037150303 62

Credit Card Numbers
Looking For Credit Card Numbers? We Identify The Options.
TenaciousDeals.com

Credit Card Numbers
Find - Credit Card Numbers. Credit Card Numbers Guide.
Yourcreditcardsmatters.com

Ads by Google

Categories

- All
- Behaviour
- Credit card
- Finance
- Future of Web Apps
- History
- Ideas
- Misc
- sage
- Society
- Software

Internet

View Favorites Tools Help

Search Favorites

ustomize Links Free Hotmail Google Windows Windows Marketplace Windows Media CNN.com EllaZ - artful intelligence Forecasting for the Future

http://rapidlibrary.com/index.php?q=credit+card+full+info+hacking+url Go

Rapid Library

Rapidshare File Search:
credit card full info hacking url

Quick Search: credit card full info hacking url All files ok

New: Submit Rapidshare links to RapidLibrary

e File Search Results: 1-25 of 17396 for credit card full info hacking url

sults By: Size + - Alphabet + -

0.33M	Ebook Hacking Credit Card Version 2 .pdf download http://rapidshare.com/files/.../Ebook_Hacking_Credit_Card_Version_2.pdf Search tags: Ebook Hacking Credit Card
0.53M	Ebook Hacking Credit Card Version 3 .pdf download http://rapidshare.com/files/.../Ebook_Hacking_Credit_Card_Version_3.pdf Search tags: Ebook Hacking Credit Card
1.89M	Ebook Hacking Credit Card Version 1 .pdf download http://rapidshare.com/files/.../Ebook_Hacking_Credit_Card_Version_1.pdf

Last 10 Rapidshare searches:

» credit card full info hacking url » katie melua » freelancer » tereza cernochova » jones » pushing the senses » pcsx2 0 9 4 exe » doors » cuckold » karaoke montez de durango

We are da best?! Help us. Set our link to your site or forum!

```
<a target="_blank"
href="http://rapidl
ibrary.com">Best
Rapidshare
```

3196507 files in our database

pidlibrary.com/ Internet

Edit View Favorites Tools Help

Back Search Favorites

Customize Links Free Hotmail Google Windows Windows Marketplace Windows Media CNN.com EllaZ - artful intelligence Forecasting for the Future

http://www.youtube.com/watch?v=rQihdKttry8

Yes it's true i can really offer you

Fresh, Visa, Credit Cards

00:11 / 00:47

Share Favorite Add to Playlists Flag

Rate: 58 ratings

Views: 23,199

Comments: 0 Favorited: 19 times Honors: 0 Links: 5

Comment on this video

Post a video response

From: xxxbios
Joined: 1 year ago
Videos: 2

Subscribe

About This Video

NEW EMAIL!!!!!!!!!!!!!!!!!!!!

» REPLY_@CONSULTAN... (more)

Added: May 22, 2007

Embed customize

<object width="425" height="355"><param name="movie" value="http://

More From: xxxbios

Related Videos

Display:

Card Number
00:14 From: claudeclosky
Views: 23,273

Credit Wizard 1.0
00:28 From: knd74
Views: 19,027

Effects of crack programs and keygens on your PC
02:14 From: zwtcrack
Views: 105,027

Credit Card Generator
00:37 From: knd74
Views: 30,706

Hacking, Cracking, Credit Cards..

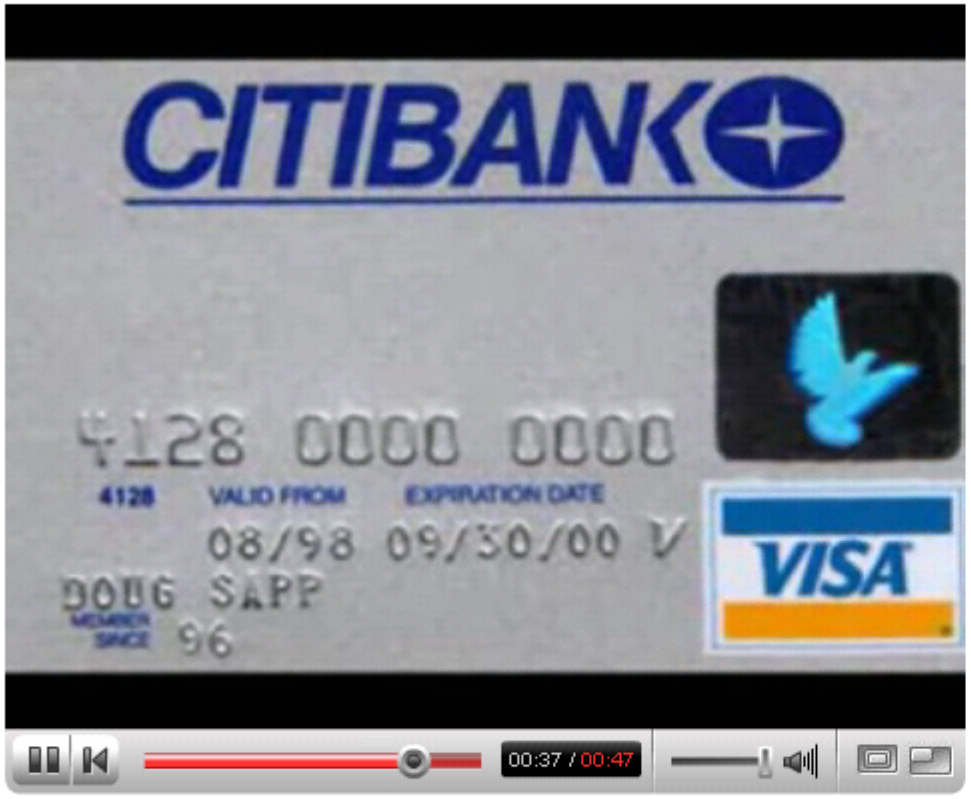
Internet

Edit View Favorites Tools Help

Back Search Favorites

Customize Links Free Hotmail Google Windows Windows Marketplace Windows Media CNN.com EllaZ - artful intelligence Forecasting for the Future

http://www.youtube.com/watch?v=rQihdKttry8



Share Favorite Add to Playlists Flag

Rate: ★★☆☆☆ 58 ratings Views: 23,199

Comments: 0 Favorited: 19 times Honors: 0 Links: 5

Comment on this video

Post a video response

From: xxxbios
Joined: 1 year ago
Videos: 2

Subscribe

About This Video

NEW EMAIL!!!!!!!!!!!!!!!!!!!

※ REPLY_@CONSULTAN... (more)

Added: May 22, 2007

Embed customize

<object width="425" height="355"><param name="movie" value="http://

More From: xxxbios

Related Videos

Display:

Card Number
00:14 From: claudeclosky
Views: 23,273

Credit Wizard 1.0
00:28 From: knd74
Views: 19,027

Effects of crack programs and keygens on your PC
02:14 From: zwtcrack
Views: 105,027

Credit Card Generator
00:37 From: knd74
Views: 30,706

Hacking, Cracking, Credit Cards..

one Internet

Edit View Favorites Tools Help
Back Search Favorites
Customize Links Free Hotmail Google Windows Windows Marketplace Windows Media CNN.com EllaZ - artful intelligence Forecasting for the Future
http://tv.boingboing.net/2008/03/19/how-to-hack-an-rfide.html

boingboing tv

How to hack RFID-enabled credit cards for $8

POSTED ON MARCH 19, 2008 12:20 AM | PERMALINK

Internet

Cost of Recovery after Attack

- 45 million credit card numbers stolen from TJ Maxx, 2006-2008
- Recovery includes
  - Investigation
  - Improving security
  - Communication with customers
  - Future lawsuits

- Estimated Final Cost $4.5 billion in 2008

Advantages of Cybercrime

- Anonymity - only 5 % of cybercriminals are caught and convicted
- Can cross borders instantly
- Automated and remotely controlled
- Soft targets -- Poorly educated public
- Technology services can be rented
- Inadequate e-crime laws in some countries

Policy for Cybersecurity

- **Federal Computer Fraud and Abuse statute**
  - Merges elements of espionage and computer abuse
- **The USA PATRIOT Act**
  - enlarges the definition of Federal crimes of Terrorism
- **CSA of 1987**
  - NIST prepares standards for fed systems
- **IT Management Reform Act of 1996 (Clinger Cohen Act)**
  - Agencies must implement sound practices
- **OMB Circular A-130**
  - Agencies must establish security programs
- **FISMA, 2002**
  - OMB must oversee agency security practices
- **Homeland Security Act, 2002**
  - DHS established to reduce vulnerabilities
- **Cyber R&D Act, 2002**
  - DHS coordinates security R&D

Authorities that set Security Policy for Civilian Agency Systems

- **HSPD-7, 2003**
  - Lead agencies work to improve industry security
- **HSPD-12, 2004**
  - Dept of Commerce will set standards for common encrypted IDs for fed employees and contractors
- **NSPD-54/HSPD-23, 2007**
  - **AKA, *The Cyber Security Initiative***
    - DHS will reduce agency Internet portals to no more than 50
    - NSA, CIA, FBI will monitor Internet activity
    - DOD can plan attacks on adversary networks

Cybercrime successfully invades Utilities

- "We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands"
- One power outage outside the U.S. affected multiple cities
- We do not know who executed these attacks
- All involved intrusions through the Internet – CIA, Jan 2008
- A similar successful exploit was also used by consultants against the U.S. Power Grid – RSA, Apr 2008

Edit View Favorites Tools Help
Back Search Favorites
Customize Links Free Hotmail Google Windows Windows Marketplace Windows Media CNN.com EllaZ - artful intelligence Forecasting for the Future
http://www.news.com/8301-10784_3-9914896-7.html?tag=tb

ad Get more done with Windows Mobile

April 8, 2008 6:58 PM PDT

Breaking into a power station in three easy steps

Posted by Elinor Mills | 21 comments

"I will tell (you) how to break into a nuclear reactor," Ira Winkler, president of security firm ISAG said as he launched into his presentation on "How to Take Down the Power Grid" at RSA 2008 on Tuesday night.

"Frankly, it's really easy to break into the power grid," he said. "It happens all the time."

First, you set up a Web server that downloads spyware onto the computers that visit.

Second, you send an e-mail to people who work inside a power station that entices them to click on a hyperlink to the Web server with the spyware. Warning them that their human resources benefits are going to be cut and sending them to a Web site with "hr.com" in the domain would work, according to Winkler, who said he has done this several times in company-approved penetration tests.

Ad Feedback

But what helps *innovation* rise?

About News Blog

Recent posts on technology, trends, and more.

Internet

Issue - Unsecured Computers

- **“Consumers’ unsecured computers play a major role in helping cybercriminals conduct cybercrimes not only on the victim’s computer, but also against others connected to the Internet.”**

- **Ron Teixeira, executive director of the National Cyber Security Alliance NCSA 2008**

Issue – Poorly Informed Online Consumers

2008 NCSA Survey of 2,249 online consumers

- 71% are not familiar with the term “botnet”;
- 59% believe it’s unlikely that their computer could affect homeland security;
- 47% believe it’s not possible for their computer to be commandeered by hackers;
- 51% have not changed their password in the past year; and
- 48% do not know how to protect themselves from cybercriminals.
- http://www.staysafeonline.info/pdf/NSCA_quickquery_survey.pdf

New Trends in Cybercrime

- Information is now stolen as credit cards are swiped, during authorization
  - 2008 Hanaford Bros. Co supermarket chain reported theft of credit card information being transmitted from point-of-sale, during authorization.
  - Credit card info sent to third party
    - Computerworld April 2008

Trend - Peer-to-Peer BotNets
The Storm Worm

- Storm is a massive "botnet"--a collection of hundreds of thousands of hijacked computers
- Described as very professional, and still growing in 2008.
- It has *no controller* -- it functions as a peer-to-peer system where any hijacked computer can give and receive commands
- Very difficult to stop
  - Recently used to steal consumers' banking information.

Cyber Criminal Profits - James Ancheta

- 20-year-old California resident worked in an Internet cafe
- Drove a BMW and spent $600 a week on new clothes and car parts
- May have made about $60,000 over a six-month period.
- In 2006, pled guilty to four felony charges of violating United States Code Section 1030

Cyber Criminal Profits - James Ancheta

- Hosted a server and Web site that advertised rental prices and advice to other cybercriminals
- Amassed a Botnet of 40,000 infected computers
- Part of the botnet included DOD computers
- There may be hundreds of criminals like Ancheta, probably many in the United States, operating botnets that we don't yet know about. -- Cnet, Jan 2006

The new Cyber Crime Economy - Attractive to Many

An IT graduate in Romania might be able to earn $400 per month legitimately, compared to <u>several thousand dollars</u> per month in the cyber crime economy -- RSA conference, April 2008

The new Cyber Crime economy- a franchise model that scales

- Cyber criminals "have very sound business models,"
- Every task in the criminal economy has become a separate specialty.
  - Some people sell e-mail lists,
  - others sell lists of compromised IP addresses,
  - there are sellers of credit card numbers, and
  - those who sell access to bot nets.
  - Some specialize in recruiting new talent

- RSA conference, April 2008

Today's Cyber Criminal

- Today there is a booming economy for hackers for hire.
- Groups have conventions and job-posting boards just like legitimate IT contractors

Today's Cyber Criminal

Groups are well funded and are staffed with large teams who may have higher skill sets than some corporate IT departments

Today's Cyber Criminal

- Eastern Europe has emerged as a center for identity theft.
- Theft includes credit card numbers, social security numbers, and other information, such as mother's maiden names
- information is sold on the black market for a high profit

The Russian Business Network

- Launched by young computer science graduates, run by techies, not career criminals
- Top graduates from universities are recruited
- Founders discovered that it was more profitable to host illegitimate activities
- RBN might not have directly violated any laws.
- They primarily provide hosting services;
- their customers are apparently the ones violating laws; Specializes in identity theft, denial of service, phishing, computer extortion and child pornography
- The RBN is reportedly linked to around 60% of all cybercrime

The Russian Business Network

- Very professionally operated
- When they rent bots, they advertise the fact that they are checked every five minutes and that the network is 99% reliable
- They advertise that for $200 an hour you will get a good, reliably hosted botnet
- RBN also offers a safe haven for the intellectual property of cybercriminals - the spyware, trojans and botnet command and control systems.
- For a fee, allegedly, it will also launder money.
  - The Guardian, Nov 2007

Trend – Estonia: Was it Cybercrime, Cyberwarfare, or Cyberterrorism?

- Founder of Russian Business Network may be related to a high-ranking official in Russia

- The Attack on Estonia may have been coordinated by, or out-sourced to RBN.

Trend - Government-sponsored cybercriminal-attacks may increase, McAfee says Network World , 11/29/2007

- David Marcus, security research and communications manager at McAfee Avert Labs.
  - -- Predicts it will be increasingly common for governments to license cybercriminals to attack enemies -- a privatized model.

International Efforts to Control Cybercrime

- Council of Europe Cybercrime Treaty
  - Harmonizes computer crime laws for countries that ratified
  - U.S. and 15 other countries ratified in 2006

- For example -- U.S. is now obligated to investigate and monitor French Internet crimes, and vice-versa.

Policy Issue – Is Cybercrime really any different than traditional Crime?

- Is cybercrime just crime as usual, or have technology and automation magnified the effects into something that is different?
- Costs of cybercrime are passed on to consumers. Are private sector customers paying tribute to cybercriminals?
- Can government protect citizens from cybercrime?
- How to increase cooperation between the government and the private sector to reduce cybercrime?

Policy Issue – How should the Private Sector respond to Cybercrime?

- Does the private sector also now have a responsibility to protect national security through better cybersecurity?

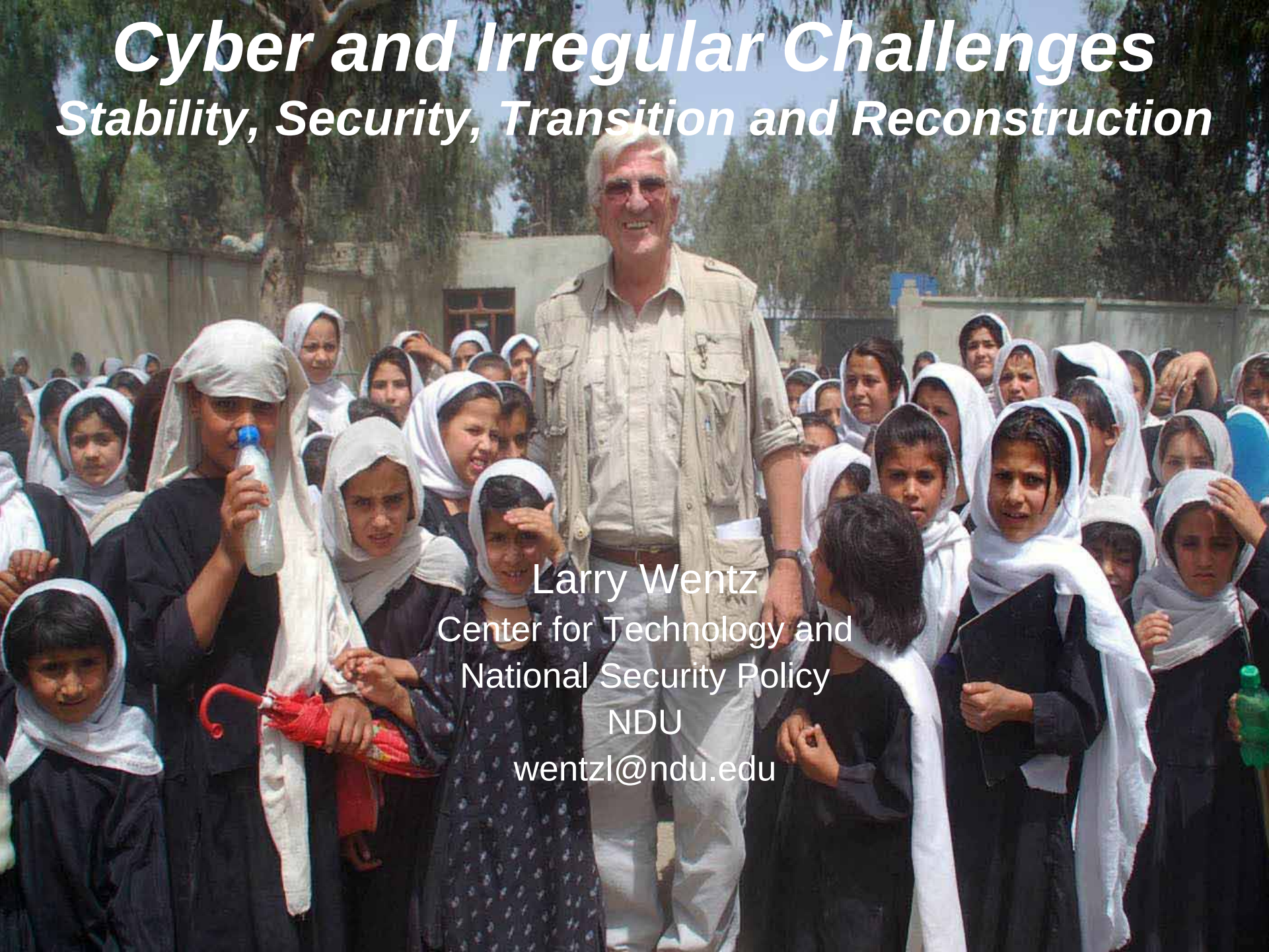
- If so, who should pay for meeting this new responsibility – the customers, or government?

Questions?

Clay Wilson, PhD, CISSP
Congressional Research Service
cwilson@crs.loc.gov
202-707-8748

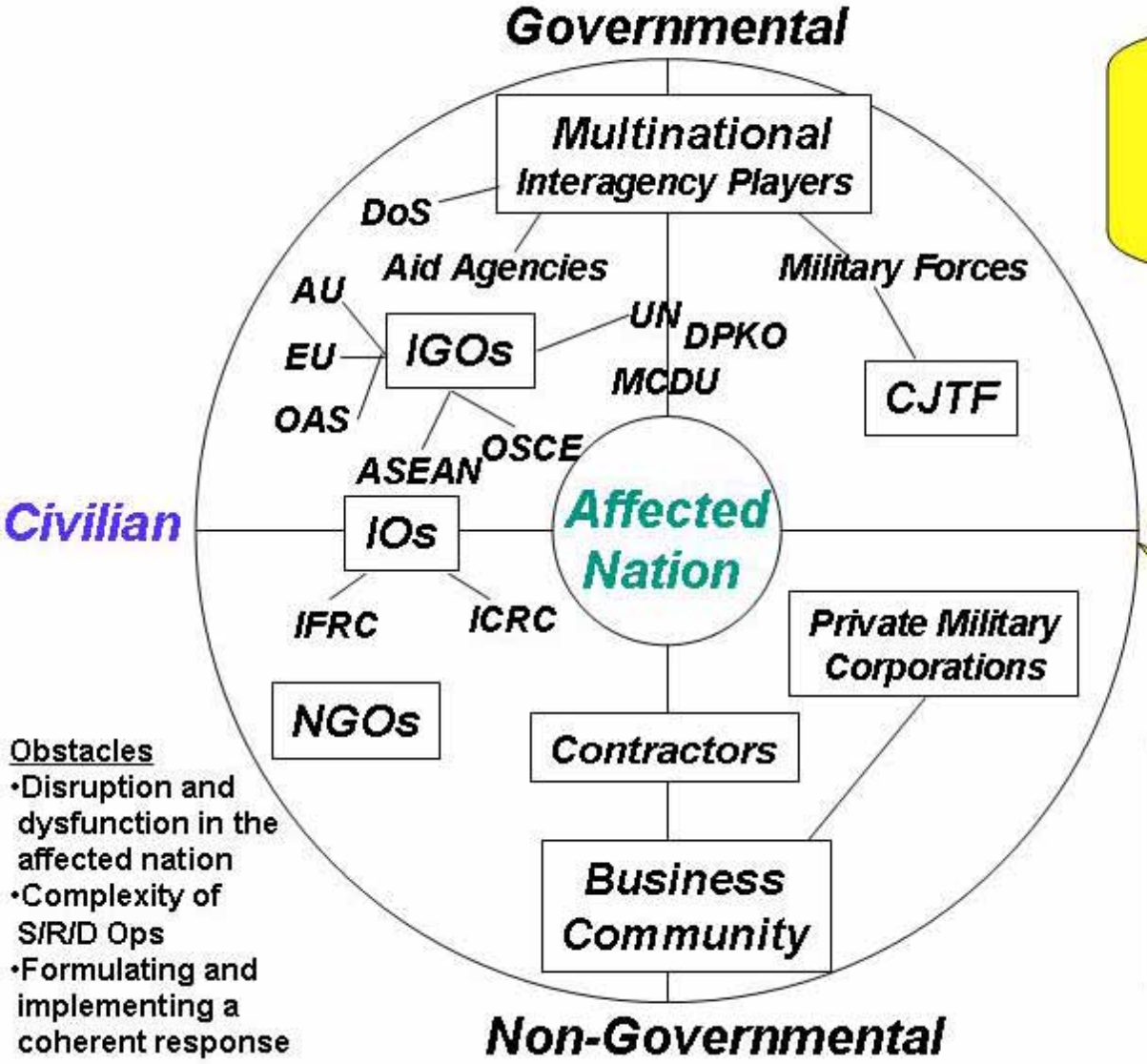
Cyber and Irregular Challenges

Stability, Security, Transition and Reconstruction



Larry Wentz
Center for Technology and
National Security Policy
NDU
wentzl@ndu.edu

SSTR is a Complex Environment



Obstacles
- Disruption and dysfunction in the affected nation
- Complexity of S/R/D Ops
- Formulating and implementing a coherent response

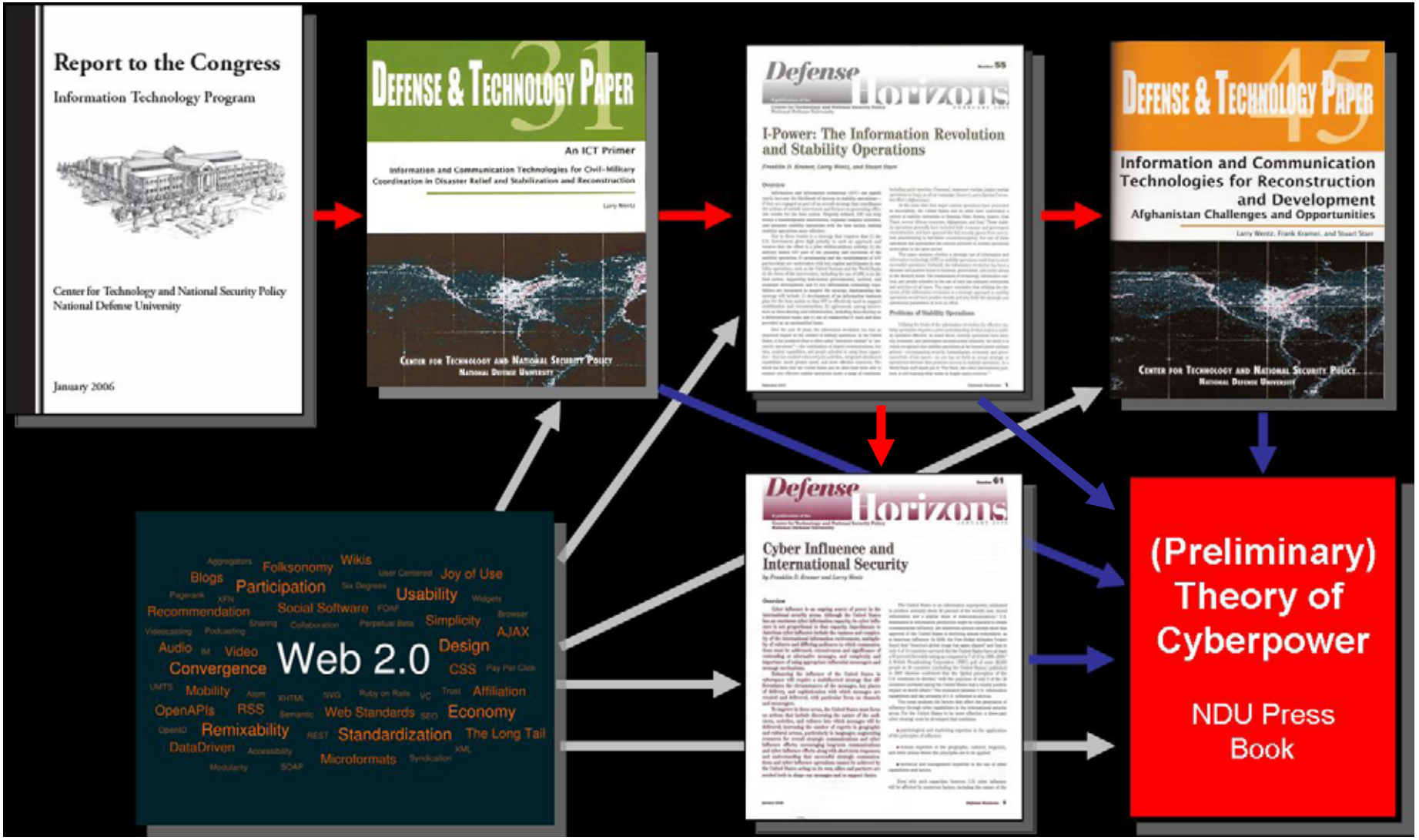
(1) Participants have different responsibilities, authorities, and capabilities and expectations and agendas

Challenge: Lack shared situation awareness and understanding of each others roles, capabilities and limitations

(2) Roles of Participants vary
- *Based on cause and urgency of operation*
- *Over time as conditions change*

NDU CTNSP: SSTR Cyber Activities

(http://www.ndu.edu/CTNSP/publications.html)

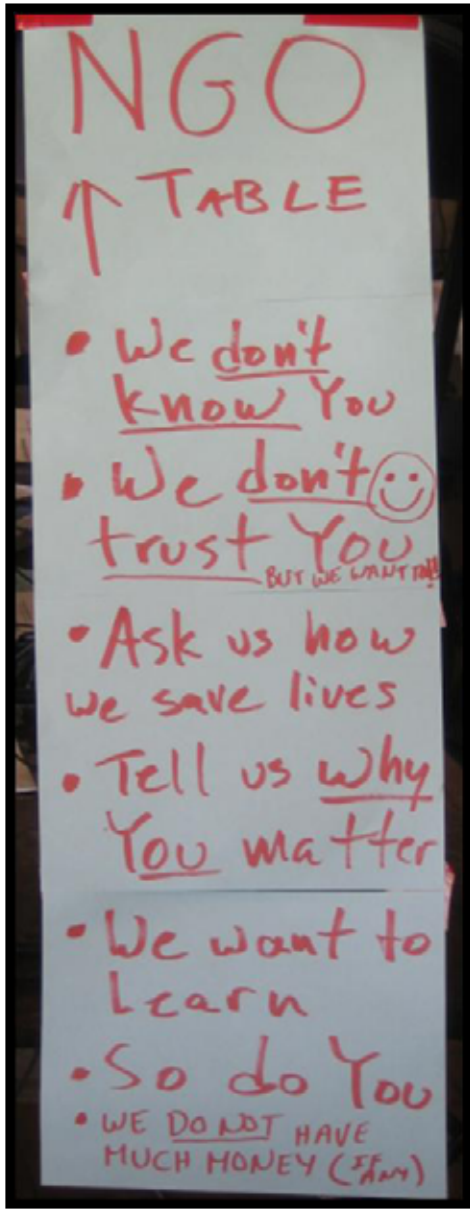


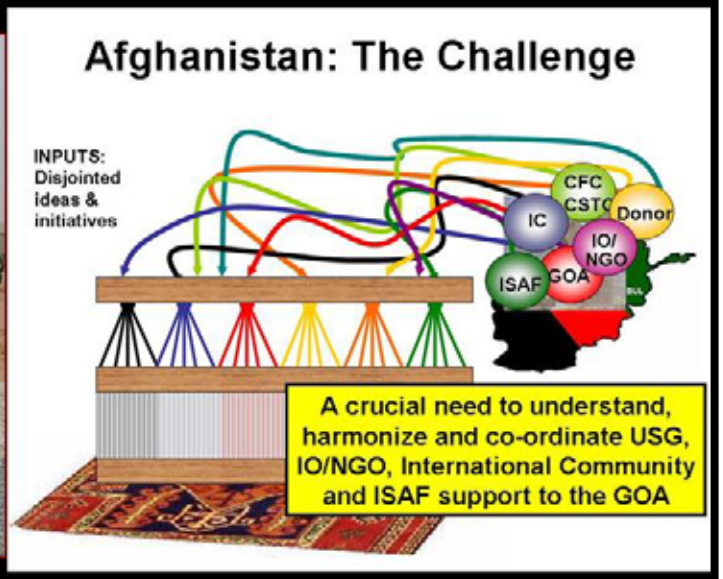
SSTR Challenges

- Understanding affected nation information culture and IT business culture
- Culture, language, policy and IT capability differences among participants including affected nation
- Common culture of trust
- Collaboration and information sharing
- Use of commercial IT and Internet including new media
- Default is to over classify information
- Coherent US Government and multinational strategy and plan focused on supporting affected nation
- Cyber an engine for economic growth, social development and enhanced governance
- Agreed metrics to quantify impact of cyber—evidence largely anecdotal

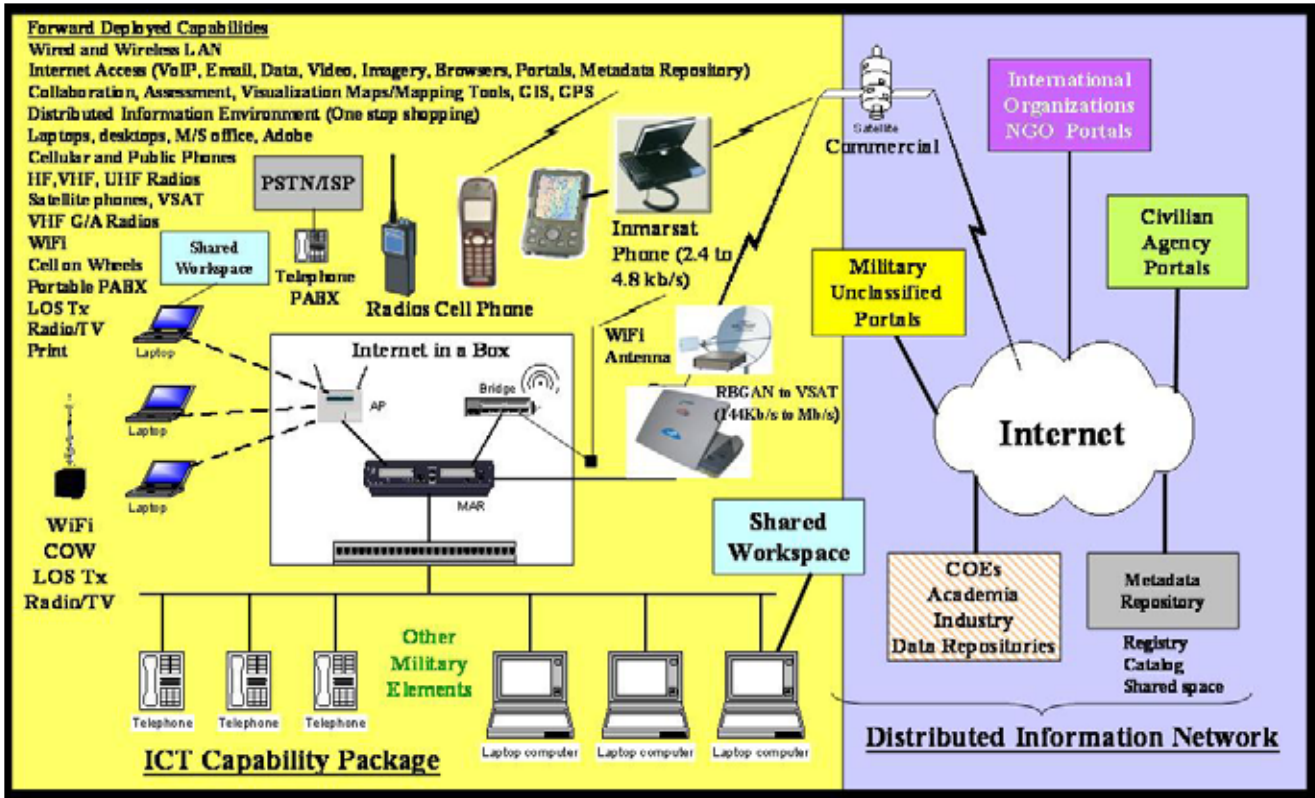
Cyber is an enabler

Real World Examples



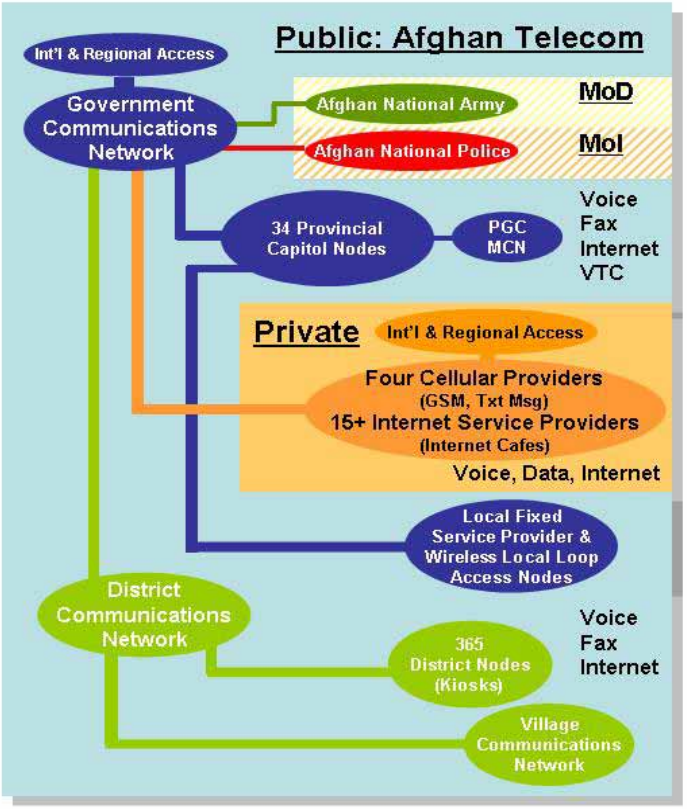


Commercial ICT Capability Packages



ICT as Sector Enabler

Emerging Afghanistan ICT



Sector Enabler Focus

Security

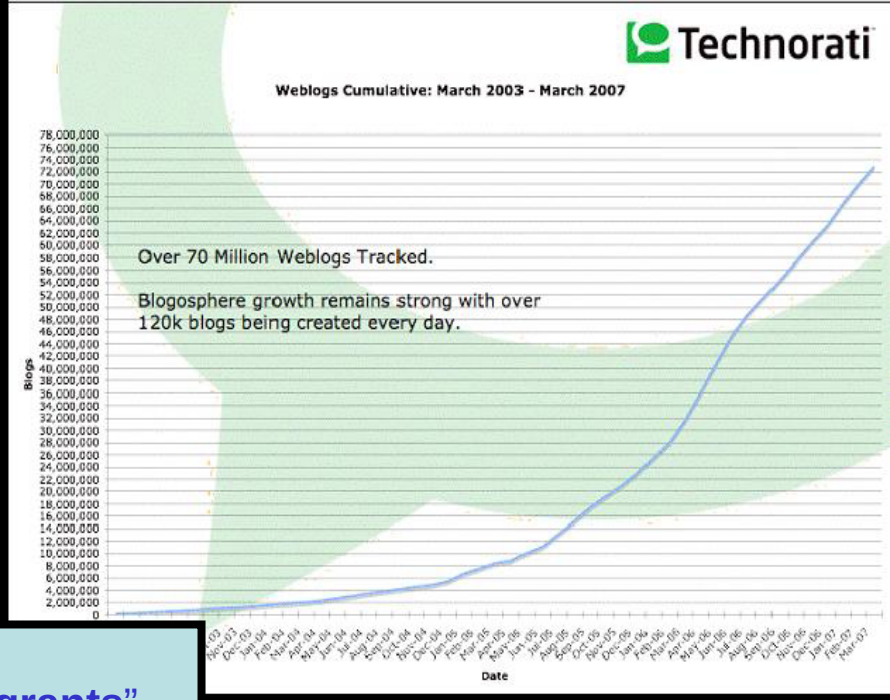
Governance

Public Access, Economic, Education, Healthcare, Governance, Security

Cellular, Internet Service Providers, VSATs
Telekiosks, Internet Cafes, Public Call Offices
Electronic Funds Transfer (e-Wallet, Internet)
Community Towers

WorldWide Mobile Phone Penetration (2006)

GSM technologies		
World	2007 3.3 billion	
Africa	208,498,137	9%
Americas	234,821,455	10%
Asia Pacific	924,047,562	39%
Europe: Eastern	349,952,186	15%
Europe: Western	444,426,302	19%
Middle East	136,649,157	6%
USA/Canada	94,365,408	



"**Digital Immigrants**"
(the over 30s)
versus
"**Digital Natives**"
(the 30 and under)

WORLD INTERNET USAGE AND POPULATIO

World Regions	Population (2007 Est.)	Population % of World	Internet Usage, Latest Data	% (Penetration)	% of World	Growth 2000-2007
Africa	941,249,130	14.2 %	44,234,240	4.7 %	3.5 %	879.8 %
Asia	3,733,783,474	56.5 %	461,703,143	12.4 %	36.6 %	303.9 %
Europe	801,821,187	12.1 %	343,787,434	42.9 %	27.2%	227.1 %
Middle East	192,755,045	2.7 %	33,510,500	17.4 %	2.7 %	920.2 %
North America	334,659,631	5.1 %	237,168,545	70.9 %	18.8%	119.4 %
Latin America/Caribbean	569,133,474	8.6 %	122,384,914	21.5 %	9.7 %	577.3 %
Oceania / Australia	33,568,225	0.5 %	19,243,921	57.3 %	1.5 %	152.6 %
WORLD TOTAL	6,606,970,166	100.0 %	1,262,032,697	19.1 %	100.0 %	249.6 %

NOTES: (1) Internet Usage and World Population Statistics are for November 30, 2007. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau . (4) Internet usage information comes from data published by Nielsen//NetRatings, by the International Telecommunications Union, by local NIC, and other reliable sources. (5) For definitions, disclaimer, and navigation help, please refer to the Site Surfing Guide, now in ten languages. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com.
Copyright © 2000 - 2008, Miniwatts Marketing Group. All rights reserved worldwide.

Legal and Doctrinal Changes

- **Baseline DoD Directive 3000.05 Task: Ensure *effective information exchange and communications* among the *DoD components, US Departments and Agencies, foreign governments and security forces, IOs, NGOs, and members of the Private Sector* (para 5.7.1).**

- **Prior to November 2006, DODD 2205.02 *Humanitarian Civic Assistance Activities* was interpreted to read that provision of ICT capacity was not an authorized activity in Security, Stability, Transition, and Reconstruction (SSTR) or Humanitarian Assistance/Disaster Relief (HA/DR) operations.**

- **Congress provided language in the conference report of the Defense authorization bill that clarified the issue: *". . .Rudimentary construction and repair of public facilities, under section 401(e)(4) of title 10, United States Code, includes information and communications technology as necessary to provide basic information and communications services."***

This now affords Combatant Commanders around the world an opportunity to provide a basic ICT capacity *and leave it behind.*

Cyber an Enabler of SSTR

- Complex multinational, multicultural and multilingual civil-military environment
  - Collaborative information environment
  - Real-time translations
  - Information classification and release
- Smart interventions
  - Enhance engagement/Phase 0
  - Coordinate intervention
  - High priority and joint civil-military activity
  - Coherent strategy focused on supporting affected nation
- Engine of economic and social growth
  - Treat as an “essential service” equivalent to roads, power, water, ..
  - Enabler of cross-sector reconstruction
    - Education, healthcare, governance (reduce corruption and enhance legitimacy)
- Policy changes support information sharing and investments in telecom and IT reconstruction
  - Information and telecom and IT crucial elements of DIME for SSTR
  - Part of planning and execution
  - Preplanning and partnerships with international and NGO participants

Challenges

- Collaborative information environment
- Leverage “The Whole of Government”
- USG organization arrangements to support planning, intervention, transition and sustainment of capabilities and services
- Language translation
- Classification and release of information
- Leverage and engagement in “New Media”
- Cyber as an “essential service” and enabler of SSTR and sector reconstruction
- Metrics for measuring effects

Questions

پولیس دتولنی خدمتگار
پولیس ترافیک درخدمت مردم
معلومات
INFORMATION
TRAFFIC
POLICE
معلومات

Challenges in Humanitarian Assistance/ Disaster Relief

Dr. Linton Wells II.

CTNSP, NDU

Challenges in Humanitarian Assistance/ Disaster Relief

- UNCLAS Information Sharing is Critical
- Comms, Lift and Power
- Prerequisites to Effective Action
  - Capability
  - Social Networks
  - Policy, Doctrine, TTP (Tactics, Techniques &
  - Procedures)
  - Resolution of Legal Issues
  - Funds for Rapid Deployment

Examples

- "Outpath"—bandwidth sharing
  - Lessons Learned from Tsunami and STAR-TIDES
- Imagery sharing in Nagahar province
  - Ad Hoc, Near-Real-Time collection
  - New classes of product: "SOIL-INT," etc
- Taking advantage of private sector innovation
- STAR-TIDES

STAR-TIDES

Sustainable Technologies, Accelerated Research
- Transportable Infrastructures for Development and Emergency Support

- Research project to help people in stressed environments through
  - Information Sharing
  - Lightweight Logistics
  - Social Networks
- Collaborative, international, largely voluntary effort: public and private organizations, academia, companies and individuals
- Emphasizes Information & Communications Technology (ICT) as critical enabler in providing reachback "knowledge on demand" and creating communities quickly
- Evolving, demonstrating and testing diverse solutions in varied scenarios
  - All results published in public domain
  - Focus is on humanitarian assistance, disaster relief, post-war stabilization and economic development

Questions for Audience

- How important is UNCLAS info sharing with civil-military mission partners?
- How can it be encouraged?
- What are the pitfalls?
- How can DoD best take advantage of private sector energy and innovation in ICT?

Cyberpower and the Modern Military

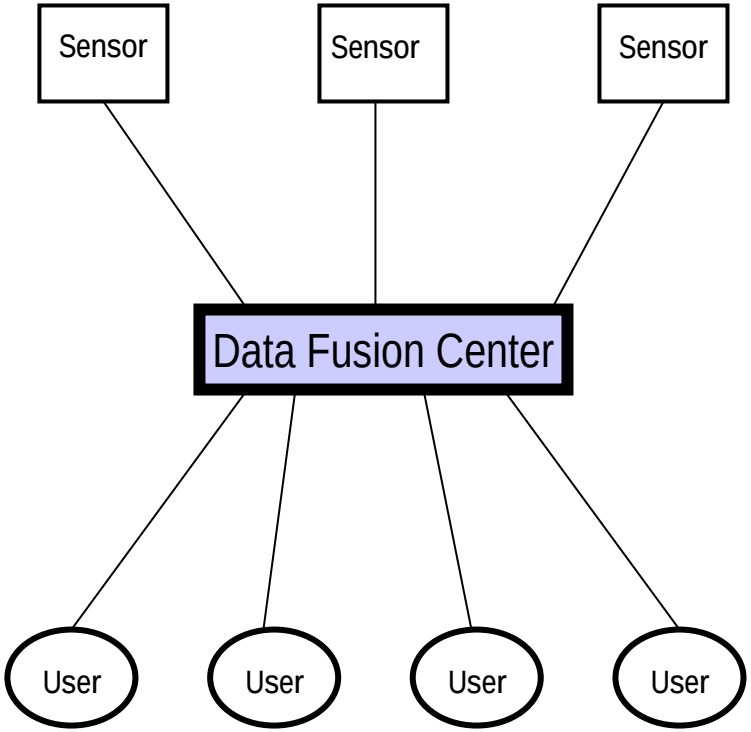
Martin C. Libicki

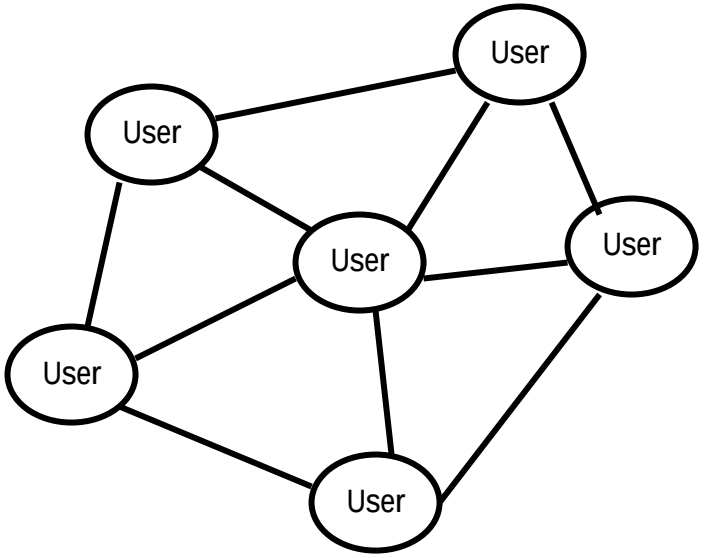
1 May 2008

Focus on Stryker Combat

- From *Network-Centric Operations Case Study*, RAND's Dan Gonzales *et al*
  - Based on a Joint Certification Exercise at the Joint Readiness Training Center (Louisiana) in early 2004
- What *aspects* of network-centric operations explains the improvement?
  - Is it access to information (might be done via broadcasting), or
  - Something more 'network-y'
    - Improved information sharing
    - *Shared* situational awareness
    - Collaboration and thus self-synchronization

Conceptual Topologies Emphasizing Different Aspects





Light Infantry Brigade (LIB) vs. Stryker Brigade Combat Team (SBCT)

	LIB	*SBCT*
Pct. of Forces Identified/Located	<10	80
Speed of Command	48 hours	3 hours
Blue:Red Casualty Ratio	1:1	1:10
End Strength	2705	3498
Riflemen	1062	1353
Mortarmen	132	168
Snipers	18	51

The Stryker Brigade had Many Conventional Advantages

- The LIB warriors had to walk and face ambushes
  - SBCT warriors drove 25 km to combat
- Stryker vehicle had more firepower
- The LIB had only 42 hours to conduct reconnaissance with a quarter of the recon units available to the SBCT which had 60 hours to do recon
  - Hence, a near 6:1 advantage in collection team-hours
- Both sides had comparable use of advanced sensors
  - Strykers had UAVs but ‘only’ for confirmation
- *But* vast differences in connectivity
  - LIB: FM Radio, poor quality voice
  - Stryker: EPLRS, NTDR, MILSATCOM, CNR commercial SATCOM -- thus 14 to 1536 kbps throughput -- but only to those in vehicles

Outcomes

- Objective: seize a town (Shughart-Gordon) in a mixed light combat situation
- Method: avoid fielded forces (2/3rds of total), attack the town directly
- SBCT but not LIB found best avenue of approach to ‘surprise’ town defenders
  - (Unclear reference to successful deception)
- SBCT was able to attack 13 hours earlier
- SBCT destroyed the enemy force and cleared every building
- By contrast, operating against the LIB, the enemy massed effects of combat power to defeat the brigade in detail, most often resulting in mission failure
- 10:1 difference in casualty exchange rates

Explaining the Results

- Was the information you had complete and accurate? (Most of the priority intelligence requests [PIRs] were ‘where’ questions)
  - IB: 10 - 20 percent said yes about red and blue
  - SBCT: 80 - 90 percent said yes about red and blue
- Time to get accurate information from spotters: 12 hours (LIB) v. 2 minutes (SBCT)
- LIB had to allocate 48 hours between plan and execution to get the word out; the SBCT was able to do this in 3 hours and hence attack early, achieving surprise
- One infantry battalion commander: “I could see on the COP the lead battalion accomplished its mission early. I moved up our attack time to achieve momentum”
- Many references to distributed planning in the ‘text’ but was it access or data?
  - “Instead of focusing discussion on the base level of knowledge and comprehension of the situation, these interactions in the SBCT were observed to reach the higher levels of analysis and application.”
  - JRTC Observer: “The Stryker brigade best exemplified this capability with collaborative planning between between the main [command post] and the tactical [command post]…VTC capability should be extended to lower echelons … to enhance situational awareness [and] understanding.”

Observations

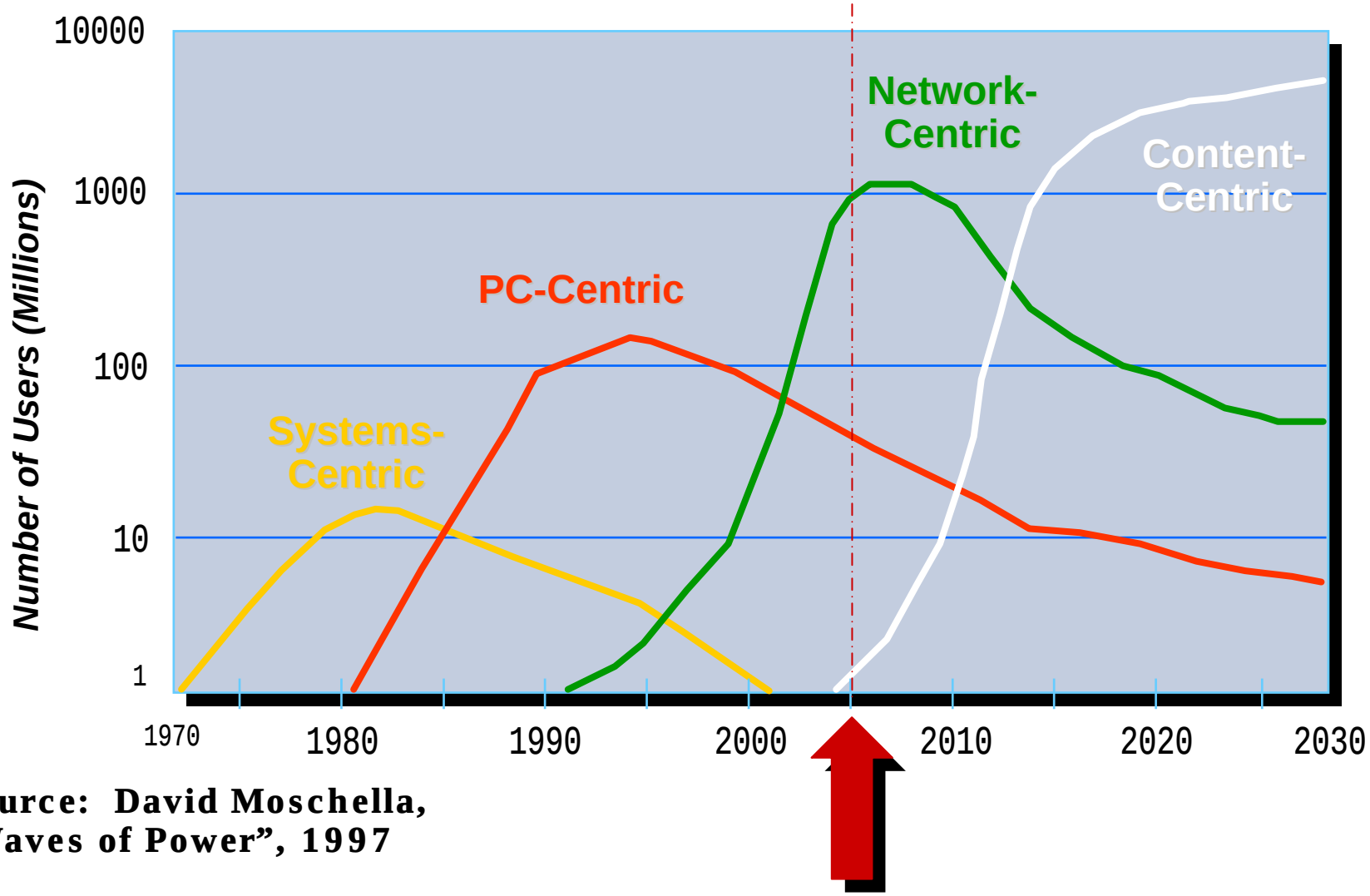
- The Network helps
  - Knowing exactly how much it helps will have to await experiments undertaken by skeptics rather than enthusiasts
- In what way?
  - … the Common Operational Picture (COP)?
    - Primarily, from knowledge base to operators
    - Secondarily, from operators to knowledge base
  - … information sharing?
  - … collaboration?
  - … self-synchronization?
  - … speed of command?
    - Meetings do go much faster if most of the time is not spent figuring out the 'ground truth'
- The hypothesis that a better COP accounts for *all* of the improvement cannot be disproved by these experiments

Deputy Assistant Secretary of Defense for Information and Identity Assurance

ROBERT LENTZ

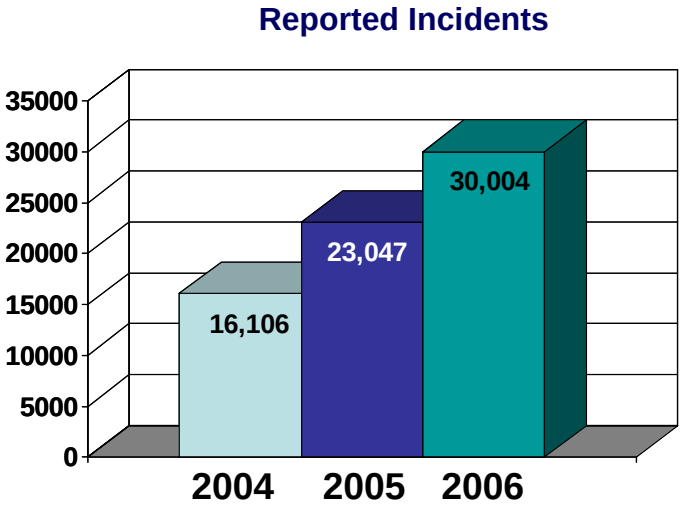
Room 3E240
6000 Defense Pentagon
Washington, DC 20301-6000
703-695-8705

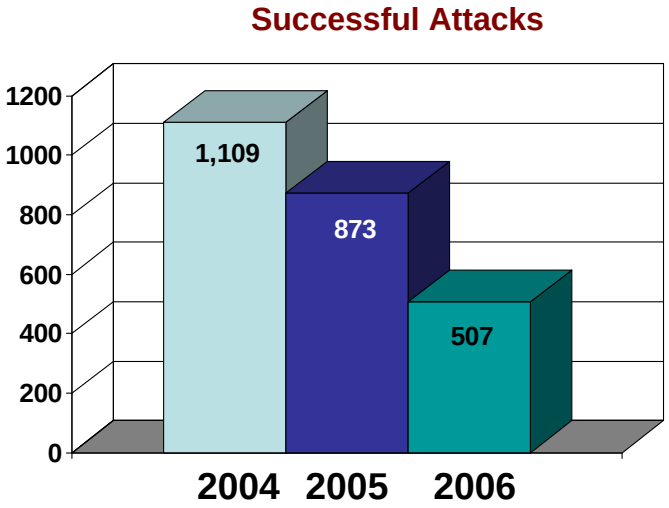
Stages of IT Industry Growth In the Information Age

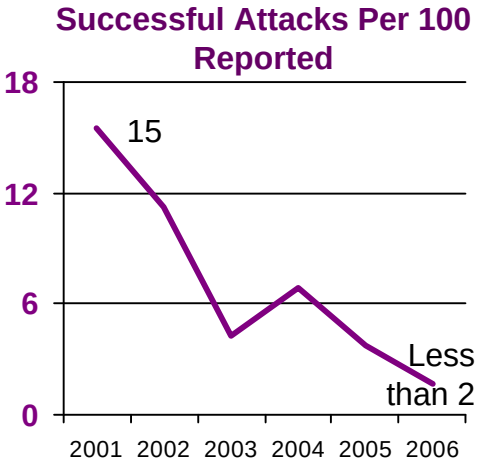


Source: David Moschella, "Waves of Power", 1997

We're Making Progress

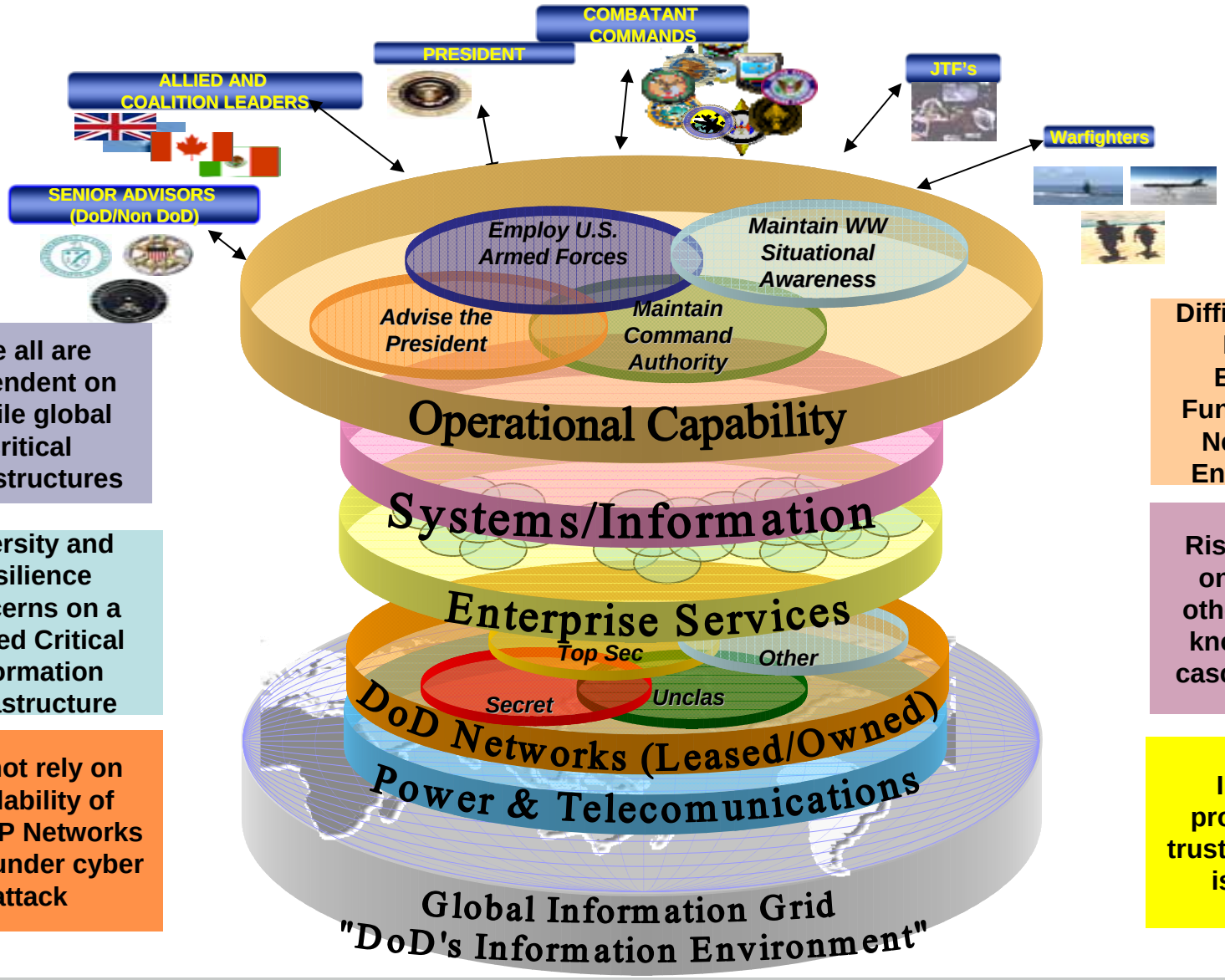






- IA Transformational Priorities needed to close the gaps
  - Cybersecurity Initiative
  - International IA Program
  - Defense Industrial Base IA
  - Globalization Task Force
  - GIG Mission Assurance

GIG Support to Mission Assurance



We all are dependent on fragile global critical infrastructures

Diversity and resilience concerns on a Shared Critical Information Infrastructure

Cannot rely on availability of other IP Networks when under cyber attack

Difficult to Map Mission Essential Functions in a Net Centric Environment

Risk accepted on behalf of others without knowledge of cascade effects

Integrity protection & trust in our data is critical

DoD IA Strategic Plan

Operationalizing the IA Baseline

Vision: **TRUSTED INFORMATION—ANYTIME, ANYWHERE**

Operations

Goal: Achieve Mission Assurance

- Secure the Core Networks
- Trusted Information Sharing
- Assured Weapons Platforms

Technology

Goal: Protect Information

- Cross Domain Solutions
- Data at Rest—Data in Motion
- Key & Identity Management
- Trusted Computing/High Assurance Platform
- Deploy Protection Capabilities

Goal: Defend Systems & Networks

- Federal Desktop Core Configuration
- Insider Threat Mitigation
- Enterprise CND Tools & Capabilities
- CND Enterprise Sensor Grid

Processes

Goal: Transform & Enable IA Capabilities

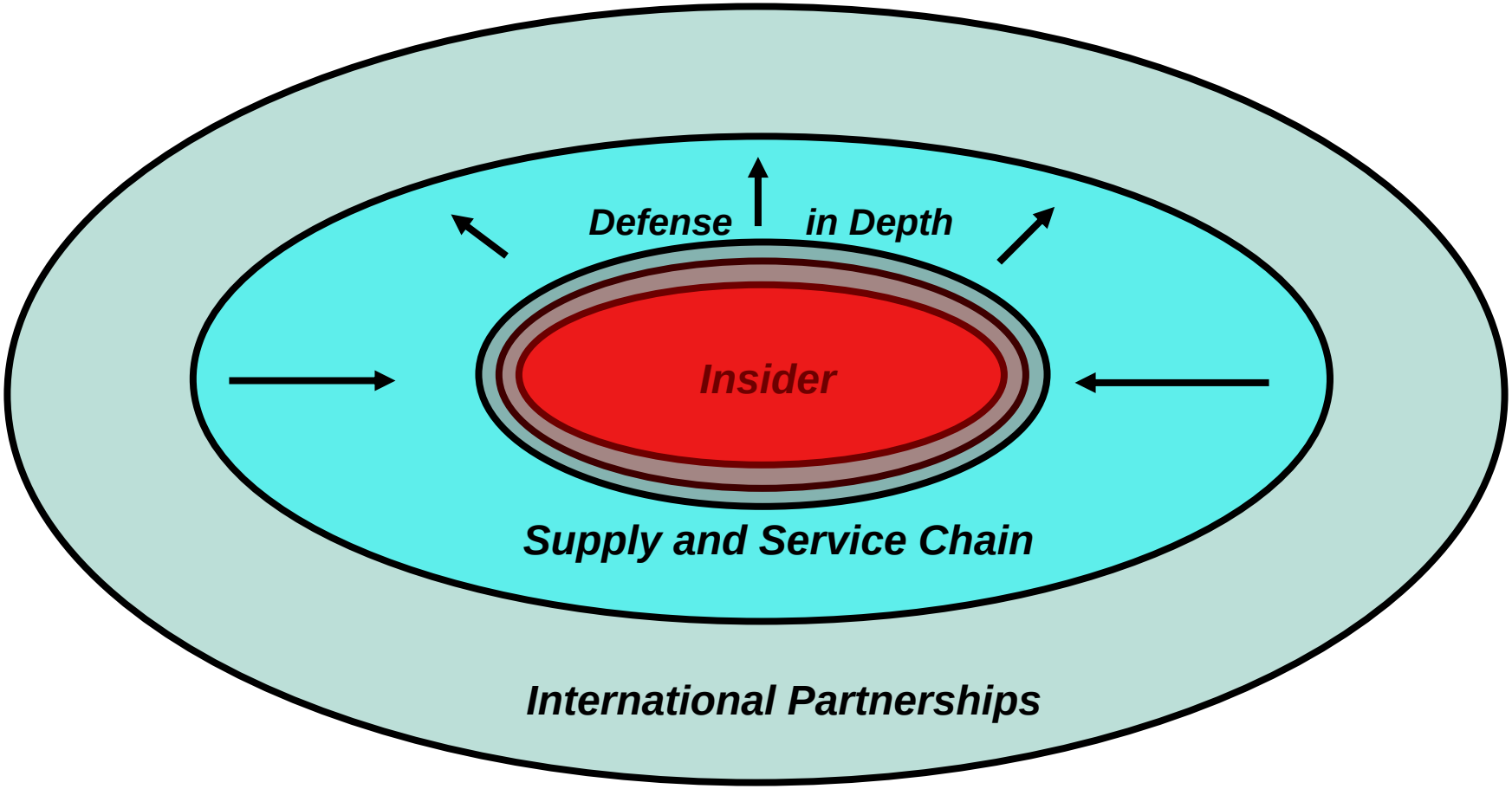
- IA/Cyber Architecture
- Defense Industrial Base IA
- International & Research Programs
- Globalization Task Force
- GIG Mission Assurance

People

Goal: Create an IA Empowered Workforce

- Certification
- Workforce Management
- Training Enhancement
- IA Outreach
- Benefits Realization

“Defense in Breadth”



We need to play Soccer . . .

Take Aways

- **Technological Superiority is a *National Priority***

- ***IA Top Technical Challenge in Information Age* – integrity, quiet theft**

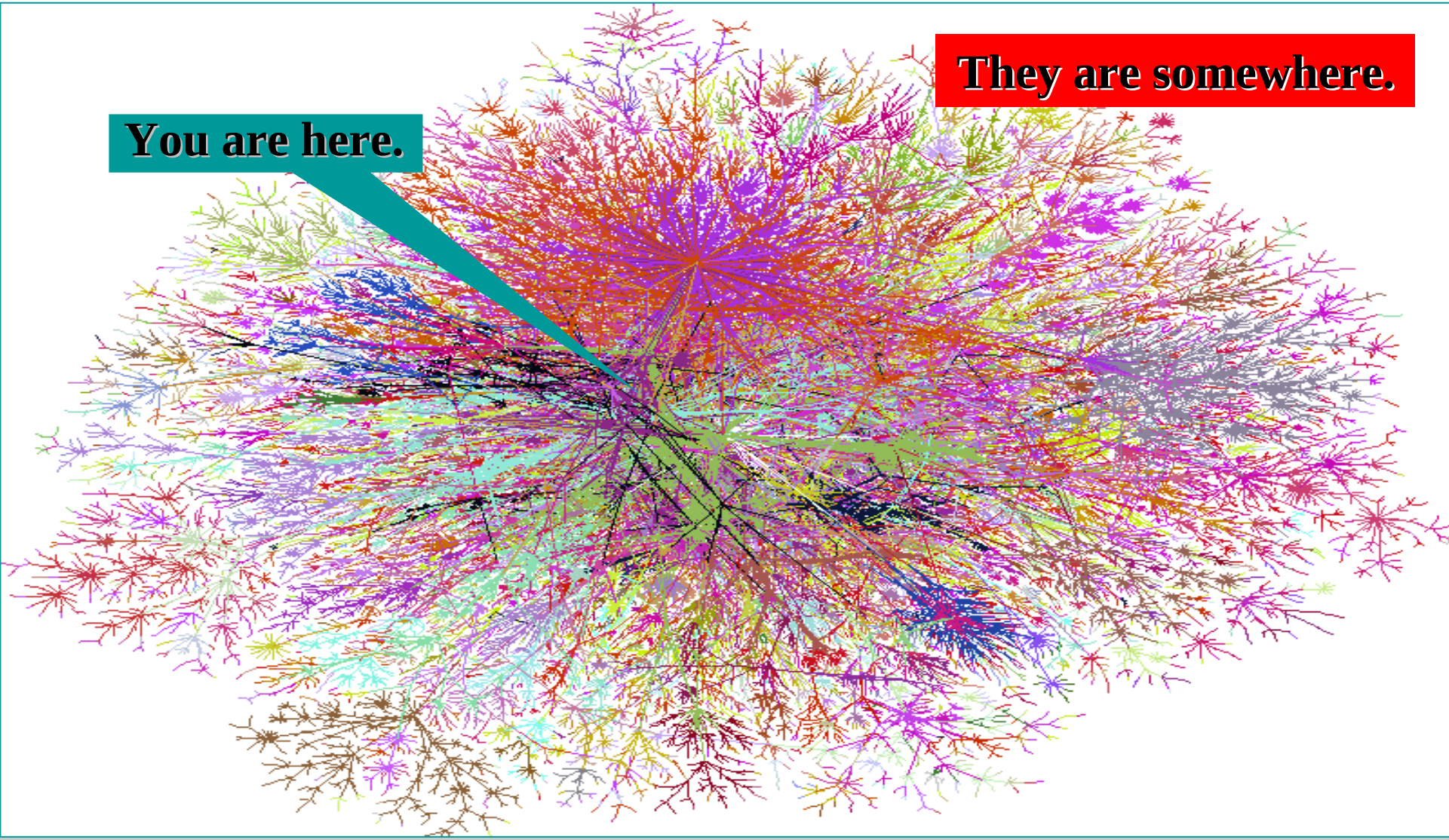
- ***Ineffective Public/Private partnership***

- ***Constantly playing R&D catch up***

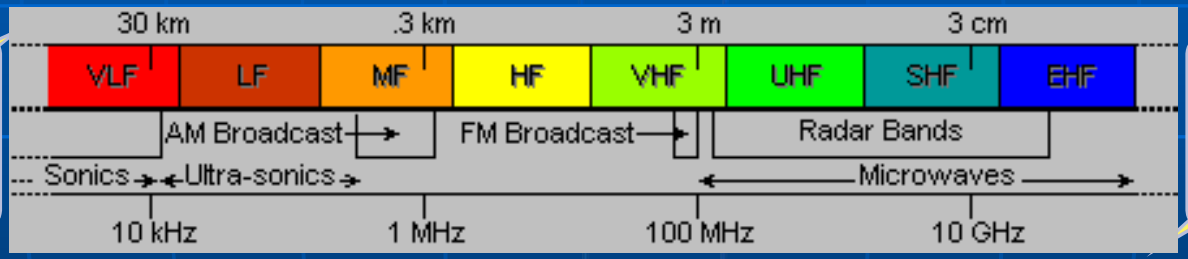
- ***Underestimating supply chain threat***

- ***Mission Assurance***

Reality of the Global Information Grid



CYBER PERSPECTIVES: The SERVICES



Dr. Dan Kuehl
Information Resources Management College (IRMC)
National Defense University (NDU)
Ft McNair Washington, D.C.

My Opinions: not the USG, DOD, or NDU!

kuehld@ndu.edu 202 685 2257

Cyberspace is…..??

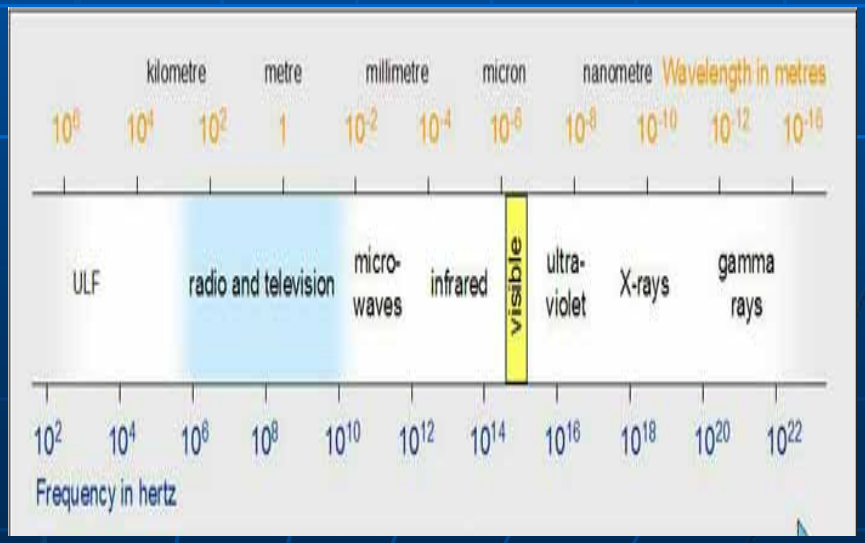
- "Cyberspace is [our nation's critical infrastructures'] nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work."
  - NS to Secure Cyberspace, 2003
- "An unconstrained interaction space …for human activity, relationships and cognition…where data, information, and value are created and exchanged…enabled by the convergence of multiple disciplines, technologies, and global networks…that permits near instantaneous communication, simultaneously among any number of nodes, independent of boundaries."
  - Navy SSG, 2007
- "Cyberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected and internetted information systems and their associated infrastructures"
  - CTNSP cyber project (pub pending); essentially same as NMS/CO and USAF, 2007

Cyberspace is….

Man-made technologies are necessary to exploit ALL of the natural phenomena and environments…..
airplanes in the air, ships at sea, satellites in space

Electronics

Cyberspace



Tim Harrell, Booz-Allen-Hamilton

Services & Cyberspace

- Army, Navy , USAF and USMC have four different perspectives on Cyberspace (and Information Operations)
  - Cyberspace not included in the “Functions of the Armed Forces”
  - Cyberspace seen through the unique lens of each Service’s warfighting domain
  - Organization – Doctrine – Personnel
    - Training, Education, Career/Promotion issues

Army Cyber

- Organizational
  - 1st IO Command, part of InsCom; CNO support
    - Two activities: IO, and Army CERT
  - LandWarNet, part of NetCom; CND support
- Doctrinal: FMs 3-0 (2008) and 3-13 (2003)
  - Cyberspace is not a warfighting domain
  - Operational focus is on enabling C2 of Army operations: “network-enabled battle command’
  - Cyber supports either NetOps or Intelligence
- Personnel
  - FA 30 is IO, FA 39 is Psyop, FA 53 is Signals

Army: FM 3 (Feb 2008)

- IO's 5 Tasks, Intended Effects, Capabilities
  - Military Deception
  - Operations Security
    - OPSEC, Physical Security, Counter-Intel
  - C2W
    - Physical/Electronic Attack, CNA/E, EW Support
  - Information Protection
    - Info Assurance, Electronic Protect, and CND
  - Information Engagement
    - Leader/Soldier Engagement, Psyop, PA, Combat Camera, Strategic Communication and DSPD
- None are "cyber specific"
- Activities dispersed across staff, hampers integration

Navy Cyber

- Organizational
  - Network Warfare Command at Little Creek
    - Combined wide range of IO-related activities, including Navy IO Center (ex-FIWC), Navy Security Gp, Navy TF/CND
    - Navy component of US Strategic Command
  - Center for Information Dominance, Corry Station
- Doctrinal
  - Cyberspace and future fleet ops still under study; Strategic Studies Group at Naval War College
- Personnel
  - 3 Informations: Professional, Warfare, Intelligence
  - “Cryptology” is now Info Warfare

Navy Cyber

- Convergence of Sea/Cyber Power
  - Changing everything about seapower, maritime ops
  - Global Reach Forward, Virtually Enabled Ops, Enabling Concepts
    - SEA CoNNECT
    - Cyber Ships, robotics, decision aids
  - Cyber Warfare as primary warfare area
    - Every sailor cyber-enabled
  - Defense Cyber Institute

- "An unconstrained interaction space …for human activity, relationships and cognition…where data, information, and value are created and exchanged…enabled by the convergence of multiple disciplines, technologies, and global networks…that permits near instantaneous communication, simultaneously among any number of nodes, independent of boundaries."
  - Navy SSG, 2007

USMC Cyber

- Organizational
  - C4 focal point, Marine Corps Enterprise Network as backbone
  - Creating Marine Corps IO Center at Quantico
- Doctrinal: MCWP 3-40.4, “MAGTF IO”
  - “growing sophistication, connectivity, and reliance on IT…vulnerabilities and opportunities presented by increasing dependence…”
    - Battlespace Shaping, Force Enhancement, Force Projection
  - Support warfighting, intel, business and enterprise management
  - Focus is C2
- Personnel
  - Creating IO career field: IO, Psyop, and “Technical IO”

USAF Cyber

- Organizational
  - 8AF into AF Cyber Command (Sept 2007)
    - Congressional food fight over where to locate HQ: “cyberturf”
  - AFIO Center, 67 Net War Wing; (San Antonio)
- Doctrinal: AFDD 2-5
  - USAF “flies, fights, wins” in 3 synergistic domains
    - Air, Space and Cyber
    - Most visionary approach: began with “Cornerstones of IW” 1995
    - Three arenas: Electromagnetic, Influence, Networks
- Personnel
  - No IO career field but is creating Cyber specialty

USAF Cyber

- SAB Cyber Warfare Study
  - Within OODA framework
    - Sense, Data and Ops Integration, Effects
  - Cyber War
    - Environment, Doctrine, OTE, Fight
  - 3 Levels
    - Network wars; Cyber adjunct to kinetics, Malicious data manipulation
- Clarifies NMS-CO def
  - "…domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures"
  - Contains networks, electronic systems, and the entire EMS
  - Offensive, Defensive, and Infrastructure Ops can all take place within Cyberspace

Discussion

- Is Cyberspace a warfighting domain?
  - Define “domain”
- Has the USAF grabbed the turf?
- Are we making the right changes the Cyber RMA requires in…
  - Organizations, doctrines, technology
- What are our coalition partners/allies doing?
- Who is the “Billy Mitchell” of Cyberspace?

Cyberpower and National Security: Key Issues

Mr. Franklin D. Kramer
Center for Technology and National Security Policy (CTNSP)
National Defense University (NDU)

May 2008

This is a DRAFT/DRAFT for Discussion Purposes and Subject to Revision

All “recommendations” are for discussion purposes only and may be revised

Cyber Policy Organization

- Recommendation: Create a new organization along lines of Council of Economic Advisers (or could be a joint task force like the National Counter-Terrorism Center (NCTC)
  - Multiple authorities in multiple arenas working on cyber
  - Government needs to think about “private” aspects of cyber since so much cyber which government relies on is private
  - Need a Center to integrate or at least coordinate and review
    - Can analyze key issues
    - Can coordinate organizational relationships

Internet Security Challenges -- Recommendations

- Government should adopt “differentiated security” approach
  - Indispensable networks -- government provide security
    - Military, and need to determine which others (e.g., defense industry, military logistical support)
  - Key networks -- government require security and could provide part
    - Examples might be electrical grid, parts of financial networks, communications grid
    - Could provide functions such as monitoring, response, special support
  - Others -- government could encourage security
    - Coordination, information, perhaps incentives
- Government R&D should analyze key cyber functions and cost/benefits of specific security approaches
  - Seek private sector input
- Need Executive-Congressional dialogue

Human Capital and R&D --- Issues

- Enhance human capital
- Expand cyber labs
  - "We as a nation don't have a national lab structure associated with [cyber] so we aren't growing the intellectual capital we need to . . . at the rate we need to be doing." Gen. Cartwright, Feb.2007
- Increase funding to agencies
- Provide more funding for R&D
  - DHS cyber R&D funding limited—less than $50M annually
- Incentivize private sector
- Summary: Create a very large program

Internet Governance

- USG seeks to continue existing Internet governance
  - Very complicated
  - Substantially private
  - Raises diplomatic issues
  - But has worked well for US, up to now
- Future: Will face requests to change
  - 2010 [contract with ICANN]
- Recommendation: Undertake review of future governance structures/issues

NCO--Recommendations

- Plan to conduct operations against an adversary that is highly cyberwar-capable
  - Red teaming and vulnerability assessment[s]--under operational conditions; need to include private networks
  - Need to build into plans “work-arounds” and capacity to operate degraded—Mission Assurance
- Conduct R&D and acquisitions necessary to overcome vulnerabilities
  - Infrastructure resilience key--include redundancy &reconstitution
  - Include cyber vulnerability as factor in R&D and acquisition process

CNA -- Recommendations

- Reduce classification and enhance integration
  - CNA classification should be comparable to other capabilities; e.g.,
    - Special techniques/specific plans have higher classification
    - General capabilities lower
  - CNA concepts/engineering that are widely known should be discussable at unclassified level just as EW concepts/engineering are
  - Planning should be integrated under standard planning approaches
    - No integration—"we make sure the recce teams don't tell the defenders what they found, or the attackers, and the attackers go out and attack and don't tell anybody they did. It's a complete secret to everybody in the loop and it's dysfunctional." Gen. Cartwright, Feb. 2007
  - Effects assessments required—many/most may be qualitative, but judgment calls are better than no calls at all

Deterrence and Response--Recommendations

- Cyber deterrence as part of overall tailored deterrence
  - Use all elements of national power; not just cyber versus cyber
- Create cyber declaratory policy
  - Nation-states with geopolitical aims potentially take account
- Cyber deterrence/response -- potential of offense
  - "We've got to get out of the mindset that it is purely a defensive activity and we are willing to accept attack and then respond by building a better defense." Gen. Cartwright, Feb. 2007
  - Responding in context of ongoing conflict different than responding to cyber only
    - Differentiate active counterinsurgency war (e.g., Iraq) or response to active terrorists who have attacked US (e.g., Al Qaeda) from more generalized situation
  - Policy/legal review required to determine appropriate constitutional/statutory/international and geo-political response to cyber attacks

Cyber Influence

- US needs both strategic and tactical capabilities
  - Critical to irregular conflicts
  - Differentiate strategic communications (long term) from tactical communications (short term)
- Interagency approach required
  - Currently lack capabilities -- multi-disciplinary required; e.g.,
    - Technical
    - Marketing
    - Cross-cultural
  - Organization needs enhancement
  - Resources need to be added

Cyber and Stability Operations

- Cyber technology can support both
  - Enhanced engagement/Phase 0 (e.g., education, health, maintain contact/reachback)
  - Coordinated intervention
  - Host nation development as critical factor in each
- Proper use of cyber enhances governance functions; e.g.
  - Financial controls reduce corruption, regularized spending
  - Central government/provincial interface can be improved
- Recommendation -- Adopt I-Power approach:
  - Joint civil-military effort
  - Partnerships with international players
  - Focus on host nation government, economic, social development

Cyber DOTMLPF -- Recommendations

- Establish Cyber laboratories
  - R&D centers
- Enhance Cyber training
  - Included in regular exercises
  - Specialized
- Consider creation of Cyber Corps
  - Joint, multidisciplinary
  - Integrate attack, defense, exploitation, influence
  - Should it be interagency? (e.g., State? DHS?)

International

- Fundamental issues same, including security, governance, uses in geo-political context
- Key specifics
  - NATO
    - Deterrence/response to attacks; e.g., Estonia
    - Security for NATO systems (and national systems that provide NATO capabilities)
    - NATO Network Enabled Capability (NNEC)
  - International governance -- law enforcement to limit cyber attacks
  - Public diplomacy -- creating partnerships and forums in battle of ideas

Summary: A New Framework

- In the Information Age, a new framework—both nationally and internationally--for government's role concerning cyber must be constructed, including
  - Security: to assure reliability
    - National regulatory framework--to better protect critical infrastructure and connection to cyberspace
  - Human capital, R&D: to maintain cutting edge capability
  - Geo-political use
    - Need for "tailored deterrence" for cyberspace
    - Cyberspace is critical to US international influence, but USG needs to substantially enhance capabilities
    - Cyberspace has the potential to play an increasingly important role in stabilization and reconstruction operations ("I-Power")
  - International
    - Effective security will necessarily require international cooperation
    - No defined or internationally accepted policy on how to respond to cyber attacks
  - Organization needs restructuring
    - Create new Cyber Policy organization (like Council of Economic Advisers)