Cyber Force Structure: Introduction and Context

October 29 – 30, 2009

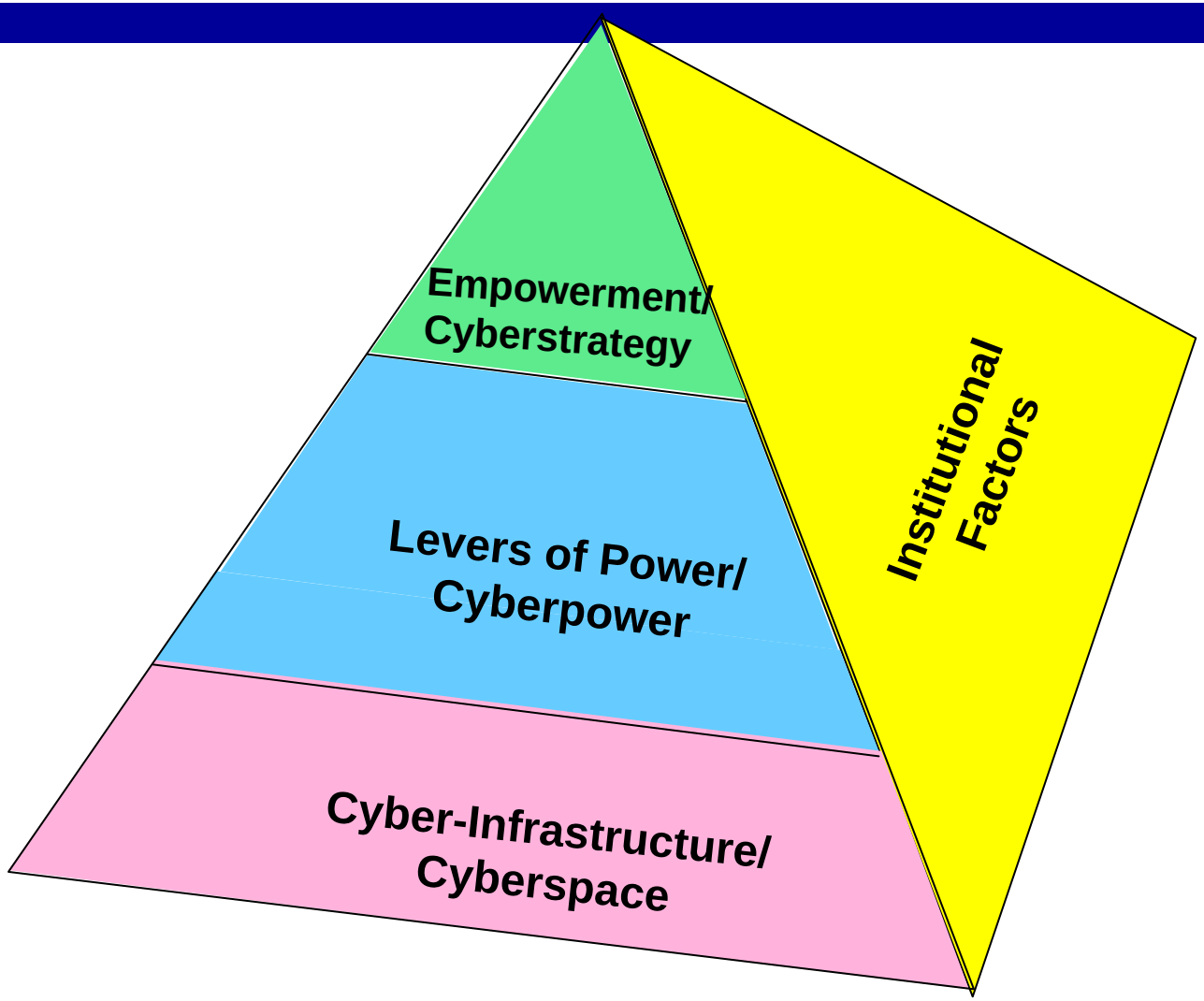
Sponsored by:

Center for Technology and National Security Policy (CTNSP), National Defense University (NDU)

CTNSP Mission, Focus

- Mission: Explore the nexus between
  - Developments in technology
  - National security policy
- Focus
  - Key developments in Information Technology (IT); e.g.,
    - Perspectives on cyberpower
    - Injection of commercial IT into government systems
  - The evolution of Transformation and Complex Operations; e.g.,
    - Center for Complex Operations (CCO)
    - Humanitarian Assistance/Disaster Relief (e.g., STAR-TIDES)
    - Stability Operations (e.g., Information and Communications Technology)
  - Impact on life sciences (e.g., pandemic influenza)
  - Modeling and Simulation of Human, Social, Cultural Behavior

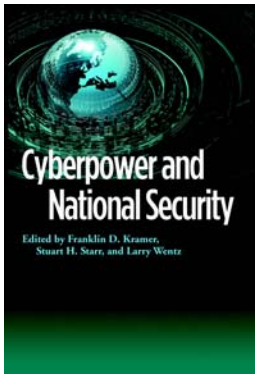
Cyber Framework



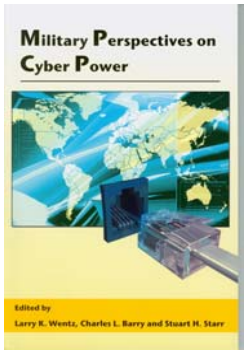
"Without a theory, the facts are silent", F. A. Hayek

Past (1 of 2)

- In response to a request in the 2006 Quadrennial Defense Review, CTNSP has generated two books on cyber issues
  - "Cyberpower and National Security Policy" (Potomac Press)



  - "Military Perspectives on Cyber Power" (CTNSP, NDU)



Past (2 of 2)

Theme	When
Cyber Deterrence	October 2008
Strategic Cyber Risk and Response	January 2009
International Cyber Perspectives	April 2009

Present

- What – Explore challenges for creating the needed cyber force structure
  - Needs
  - Current Capabilities
  - Actions to Redress Shortfalls
- Where, When
  - 155 Marshall Hall, Fort Lesley J. McNair, Washington, DC
  - October 29 (full day), October 30 (half day)

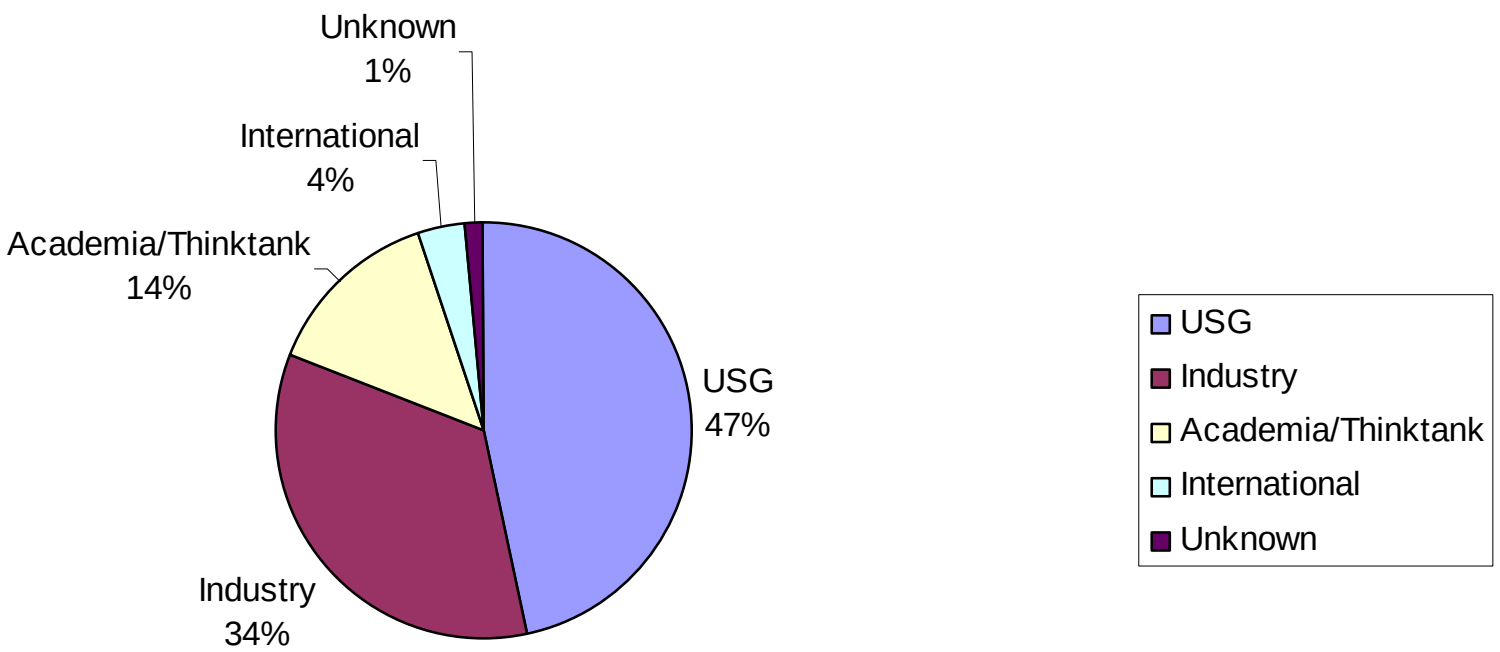
Future

- CTNSP is planning to convene several additional cyber conferences/workshops; e.g.,
  - “The Legal Dimension of Cyber” (Winter 2010)
- A sequel to the book, “Cyberpower and National Security” is planned
- Several wargames are planned to illuminate key cyber issues

Agenda

- CTNSP
  - Mission, Focus
  - Temporal Perspective
    - Past
    - Present
    - Future
- Administrative Remarks
- Closing the Loop

Registration by Affiliation



Administrative Issues

- Food
  - Breakfast: doughnuts and drinks
  - Lunch: sandwiches
- Non-attribution policy of NDU
  - "… **without the express permission of the speaker**, nothing he or she says will be attributed to that speaker directly or indirectly …"
  - The press is participating in the event
    - Washington Post
    - Aviation Week

Agenda

- CTNSP
  - Mission, Focus
  - Temporal Perspective
    - Past
    - Present
    - Future
- Administrative Remarks
- Closing the Loop

Feedback

- A web-based survey has been prepared
- It features a small set of key questions; e.g.,
  - Value of the presentations, panels
  - Positive attributes of the conference
  - Options to enhance future cyber conferences
  - Interest in future CTNSP cyber events
- The URL for the survey is:
  - http://www.surveymonkey.com/s.aspx?sm=54AOVAV9mXhTmy4p4Ly7WA_3d_3d

CTNSP Cyber Program

- Information on past, current and future CTNSP Cyber events available at:

http://www.ndu.edu/ctnsp/cyber_conferences.htm

Final Observation

"Never doubt that a small group of thoughtful, committed citizens can change the world; indeed, it's the only thing that ever does"

- Margaret Mead

Back-up Material

Prior Events (1 of 3)

- What – Workshop on Cyber Deterrence
- Who -- Sponsor: OUSD(Policy); Chair: Terry Pudas, CTNSP
- When, Where -- October 20 – 21, 2008; NDU
- How – Eight panels; e.g.
  - Theory of Deterrence
  - Challenges in a New Global Commons
  - Thresholds and Response
  - The New Article V
  - How to Invest?
  - Ambiguity vs Explicit Declaration
  - Critical Infrastructure
  - How to Move Forward?

Prior Events (2 of 3)

- "Strategic Cyber Risk and Response" (January 2009)
  - Focus:
    - "What cyber advice would you offer to the new Administration?"
    - "How would you strengthen/build Communities of Interest to drive progress in creating and implementing national strategic cyber priorities?"
  - Structure
    - "Attacks, Preparedness, and Response"
    - "Cyber Risk"
    - "Malicious Activity and Cybercrime"
    - "R&D Requirements Planning"
    - "Governance of Cyber"

Prior Events (3 of 3)

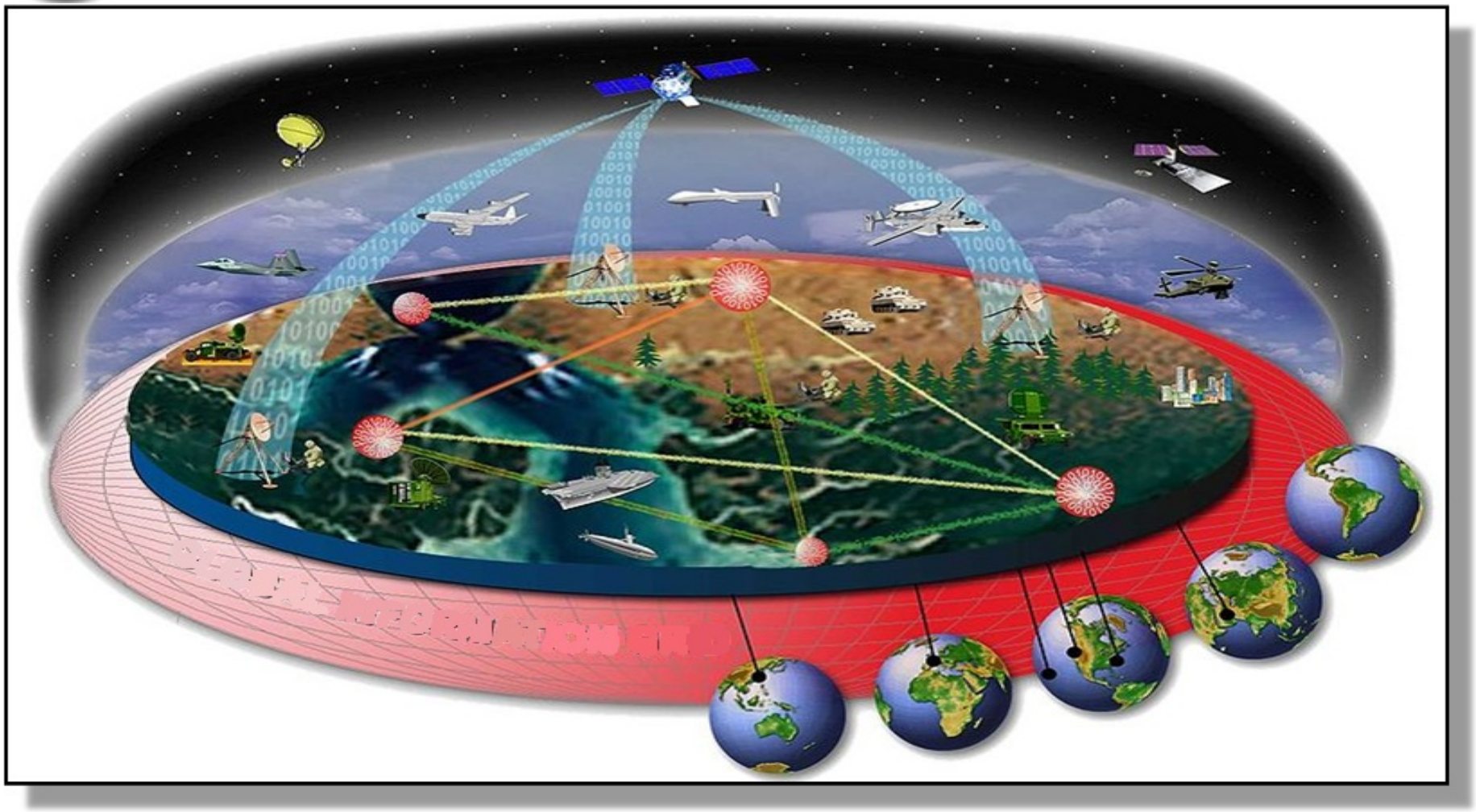
- What – International Cyber Perspectives
- Who -- Chair: Chuck Barry, CTNSP
- When, Where: 29 – 30 April 2009; NDU
- How –
  - Distinguished speakers: GEN Cartwright (USMC), LTG Alexander (USA), LTG Raduege (USAF, ret)
  - Panels
    - The International Challenges of Crime, Security and Governance
    - Policy Challenges in Defending Against Cyber Attacks
    - Critical Cyber Infrastructure Protection
    - Potential Thresholds of War in Cyberspace
    - National Perspectives on: Infrastructure Protection, Cyber Crime and the Potential for War in Cyber Space
    - Institutional/Multilateral Governance Initiatives, Today and Tomorrow

NDU Conference on Cyber Force Structure

Mr. Bob Butler
Deputy Assistant Secretary of Defense for Cyber and Space Policy

29 October 2009

Strategic Context



… Increasing Reliance and Importance of Cyberspace for DoD

UNCLASSIFIED

Strategic Context

- **Cyberspace is a key enabler around the world for commerce and national security**
  - Increasingly congested without clear codes of conduct
  - Warfighting advantage can erode as adversary activity in cyberspace increases
- **Cyberspace is becoming a congested and contested environment**

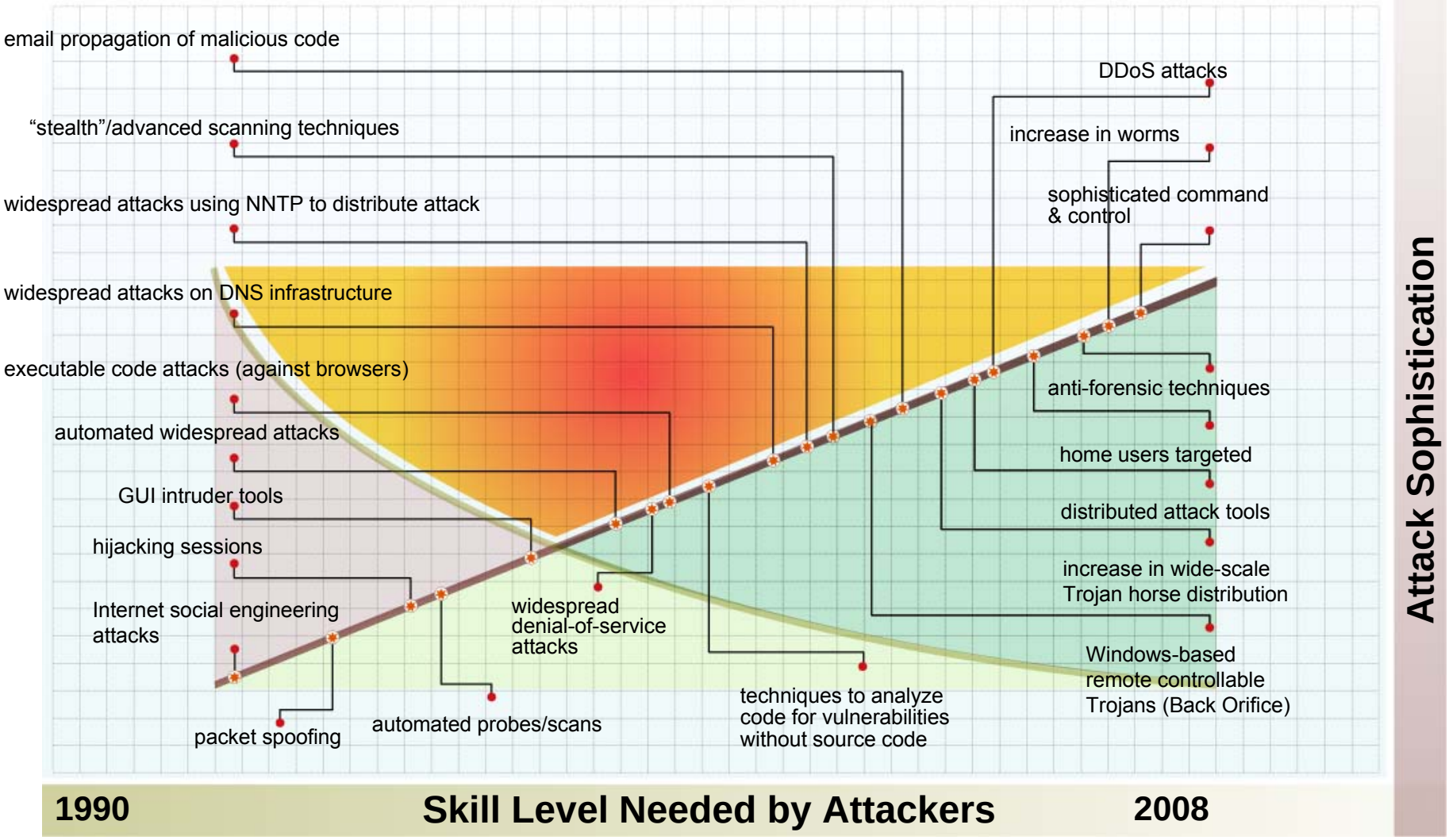
"The security of America's space and cyberspace-based information architecture has become a matter of national concern"

– Michèle Flournoy and Shawn Brimley
"The Contested Commons"

Increasing Risk

Source: US CERT

Increasing Risk



DoD Response

- **Stand up of Cyber Command**
  - Ensure the effective operation and defense of the DoD information networks
  - Better integrate cyber force structure and enhance cyber command and control

- **Review of Cyber Policy and Strategy**
  - Ensure comprehensive approach to DoD cyberspace operations
  - Enabled by tabletop exercise series with focus on discovery learning and solution development for operations, policy and force structure

Questions

- **To operate at net speed for network protection, what new operational concepts are required?**
- **Is a new DoD policy framework required?**
  - What are the distinctions and thresholds among cybercrime, cyber espionage and cyber national security events?
  - What new legislation and/or POTUS direction is/are required to protect our DoD forces from cyber threats?
  - Do we need new declaratory policy on cyber self defense?
- **What else is required to maintain DoD mission critical capabilities against attack?**
- **What then are the resourcing (manpower, education and training) needs required for Cyber Command to best ensure the operation and defense of DoD networks?**

The Cyber Security Education Challenge

NDU Cyber Force Structure Conference

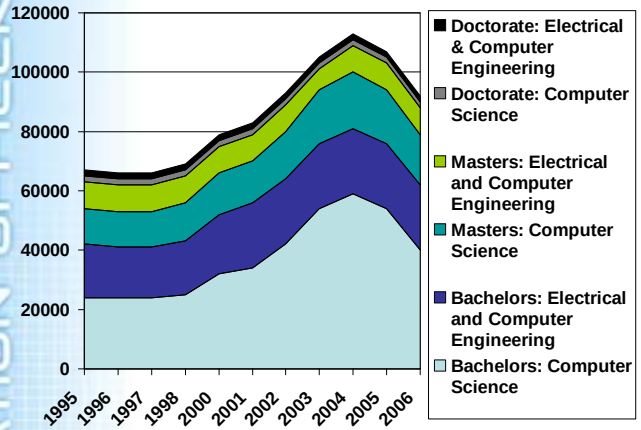
October 29, 2009

George Bieber, DoD CIO DIAP,

DEPARTMENT OF DEFENSE
CHIEF INFORMATION OFFICER
Creating an Information Advantage

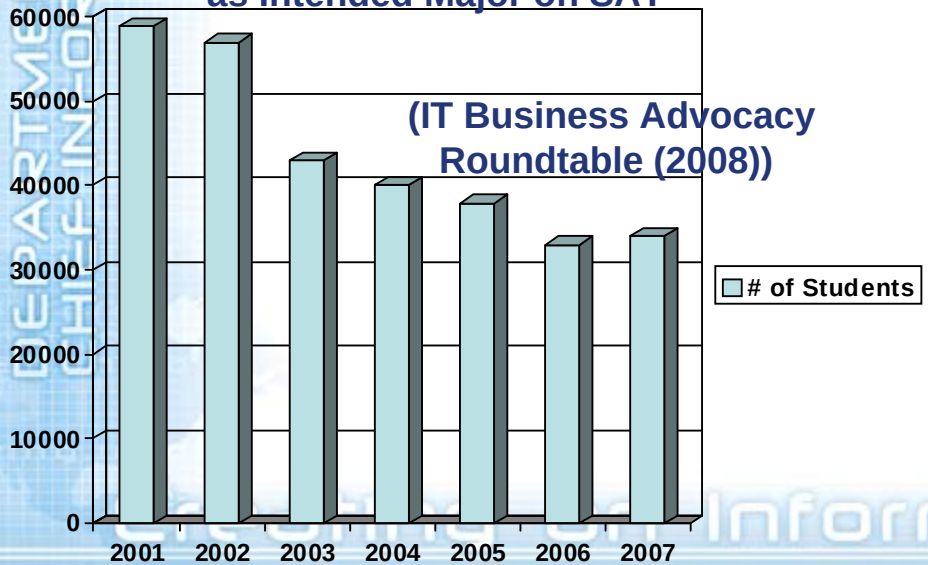
The Challenge

Supply of Traditional NIT Graduates (1995-2000) (NCES)



Computing and Information Sciences as Intended Major on SAT

(IT Business Advocacy Roundtable (2008))



TIMSS Mathematics Test Score Comparison (2007)

Avg. = 500 Source: *TIMSS* (2007)

Grade Four		Grade Eight	
Country	Score	Country	Score
Hong Kong	607	Chinese Taipei	598
Singapore	599	Rep. of Korea	597
Chinese Taipei	576	Singapore	593
Japan	568	Hong Kong	572
Kazakhstan	549	Japan	570
Russian Federat.	544	Hungary	517
England	541	England	513
Latvia	537	Russian Federat.	512
Netherlands	535	**United States**	**508**
Lithuania	530	Lithuania	506
United States	**529**	Czech Republic	504

National Efforts Underway to Build Capacity for a Digital Nation

Federal Focus	expanding to	National Focus
NSA/DHS Designated Centers of Academic Excellence in IA	→	Computer Science and STEM Education
Federal Employee Awareness	→	Public Awareness
Education/training to fill federal jobs	→	K-12 and higher education, including community colleges
Federal Pipeline	→	National Pipeline

Building Capacity via K-12

- Institute standards for computer science in STEM education
- Make computer science courses available for all high school students – emphasizing basic concepts, programming and security
- Provide formal training for high school teachers whose main assignment is computer science
- Introduce secure programming clinics for teachers and rising high school students

DEPARTMENT OF DEFENSE
CHIEF INFORMATION OFFICER
Creating an Information Advantage

Building Capacity via Higher Ed

- Establish a second set of criteria for cybersecurity curriculum to compliment the CNSS standards
  - Focus on fundamentals/principles with goal to produce PhDs, – researchers and faculty
- Mobilize community colleges and academic collaboration
  - Cyber Security Educational Consortium (Tulsa U)
  - International Cyber Security Education Coalition (U of Detroit Mercy and Regis U)
- Provide incentives to increase the number of US citizens who receive graduate degrees in computer science related fields
- Embed fundamental security concepts in core undergraduate computer science curricula
- Secure programming as part of every programming assignment
- Greater emphasis on technological expertise and hands on experience of faculty – Labs, exercises – and people who know how to use them/create them
- Support development of MS and PhDs for building Cyber tools/solutions and for teaching in higher education
  - Distinguished professorships
  - Research outlets for grand challenge oriented problems
  - Loan repayment pay back for service in academia

DEPARTMENT OF DEFENSE
CHIEF INFORMATION OFFICER
Creating an Information Advantage

Way Ahead: Focus Areas

- Standards
- Faculty
- Collaboration
- Curriculum
- Hands on Experience/Labs/Exercises
- Taxonomies
- Teacher Preparation
- Public Awareness
- Education Technologies
- Science and Practice of Learning

DEPARTMENT OF DEFENSE
CHIEF INFORMATION OFFICER
Creating an Information Advantage

Conference on Cyber Force Structure

29 – 30 October 2009

Center for Technology and National Security Policy (CTNSP)

National Defense University (NDU)

NATIONAL PLANNING SCENARIOS

List of Scenarios

- Scenario 1: Nuclear Detonation – Improvised Nuclear Device
- Scenario 2: Biological Attack – Aerosol Anthrax
- Scenario 3: Biological Disease Outbreak – Pandemic Influenza
- Scenario 4: Biological Attack – Plague
- Scenario 5: Chemical Attack – Blister Agent
- Scenario 6: Chemical Attack – Toxic Industrial Chemicals
- Scenario 7: Chemical Attack – Nerve Agent
- Scenario 8: Chemical Attack – Chlorine Tank Explosion
- Scenario 9: Natural Disaster – Major Earthquake
- Scenario 10: Natural Disaster – Major Hurricane
- Scenario 11: Radiological Attack – Radiological Dispersal Devices
- Scenario 12: Explosives Attack – Bombing Using Improvised Explosive Device
- Scenario 13: Biological Attack – Food Contamination
- Scenario 14: Biological Attack – Foreign Animal Disease (Foot and Mouth Disease)
- Scenario 15: Cyber Attack

NATIONAL LEVEL EXERCISE PROGRAM

DHS-sponsored Top Officials (TOPOFF) exercises

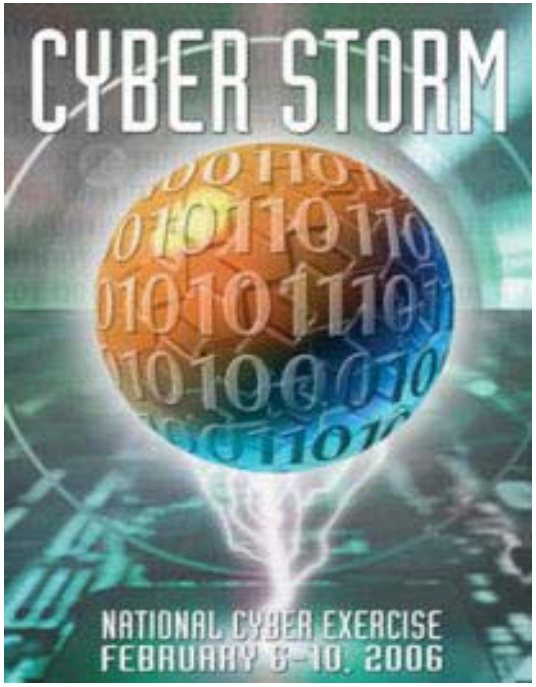
- Strengthen the nation's capacity to prevent, protect against, respond to, and recover from terrorist attacks involving WMDs
- Enable "full-scale, full system tests" of collective preparedness, interoperability, and collaboration across all levels of state, federal, international government and private sector
- TOPOFF 4 Full Scale Exercise was held October 2007

NATIONAL LEVEL EXERCISE PROGRAM

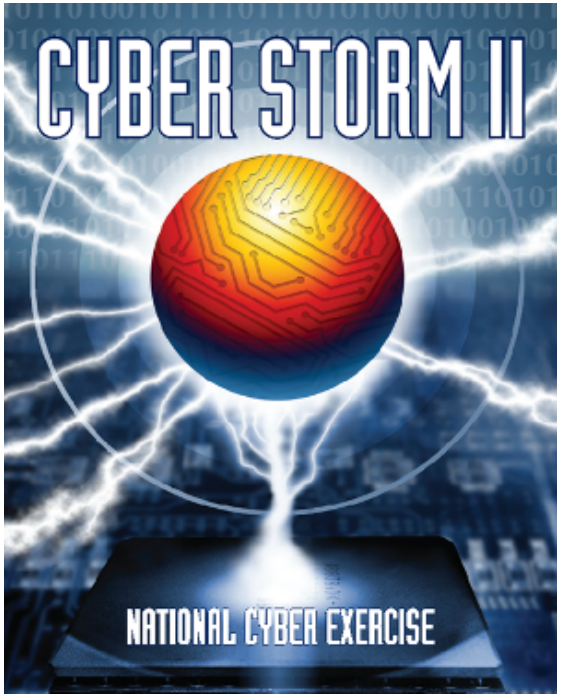
- National Level Exercise 2 – 08- May, 2008
- National Level Exercise 2009- July, 2009
- National Level Exercise 2010
- National Level Exercise 2011

NATIONAL CYBER STORM EXERCISE PROGRAM

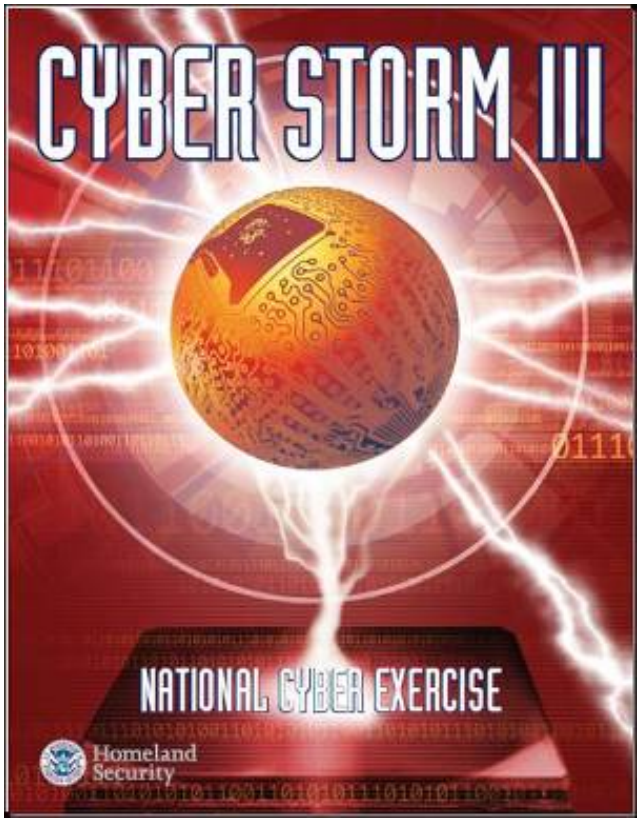
February 6 – 10, 2006



March 10 – 14, 2008



NATIONAL CYBER STORM EXERCISE PROGRAM



NATIONAL LEVEL EXERCISE PROGRAM

- Testing our national preparedness and resiliency
- Scenarios must reflect reality
- Public - private sector collaboration
- Role of private sector CI/KR owners & operators
- Growing interdependencies
- Role of all stakeholders- Federal, State. Local, Tribal, Territorial, Private Sector, International
- Lessons Learned & After Action Reports

THANK YOU!!

Robert B. Dix, Jr.

Vice President

Government Affairs & Critical Infrastructure Protection

Juniper Networks, Inc.

Cyberspace Operations and Professional Military Education

Cyber Force Structure Conference
29 Oct 09
National Defense University
Washington, DC

John Garstka
Senior Analyst
Directorate for Communications and Networking Programs and Policy
DASD (C3, Space and Spectrum)
ASD(NII)

This Presentation is Unclassified

Overview

- Definitions
- QRM Review Language on Education related to Cyberspace Operations
- Programs and Curriculum with Cyber Content
- Current JPME Guidance
- Challenges

Cyberspace

"A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

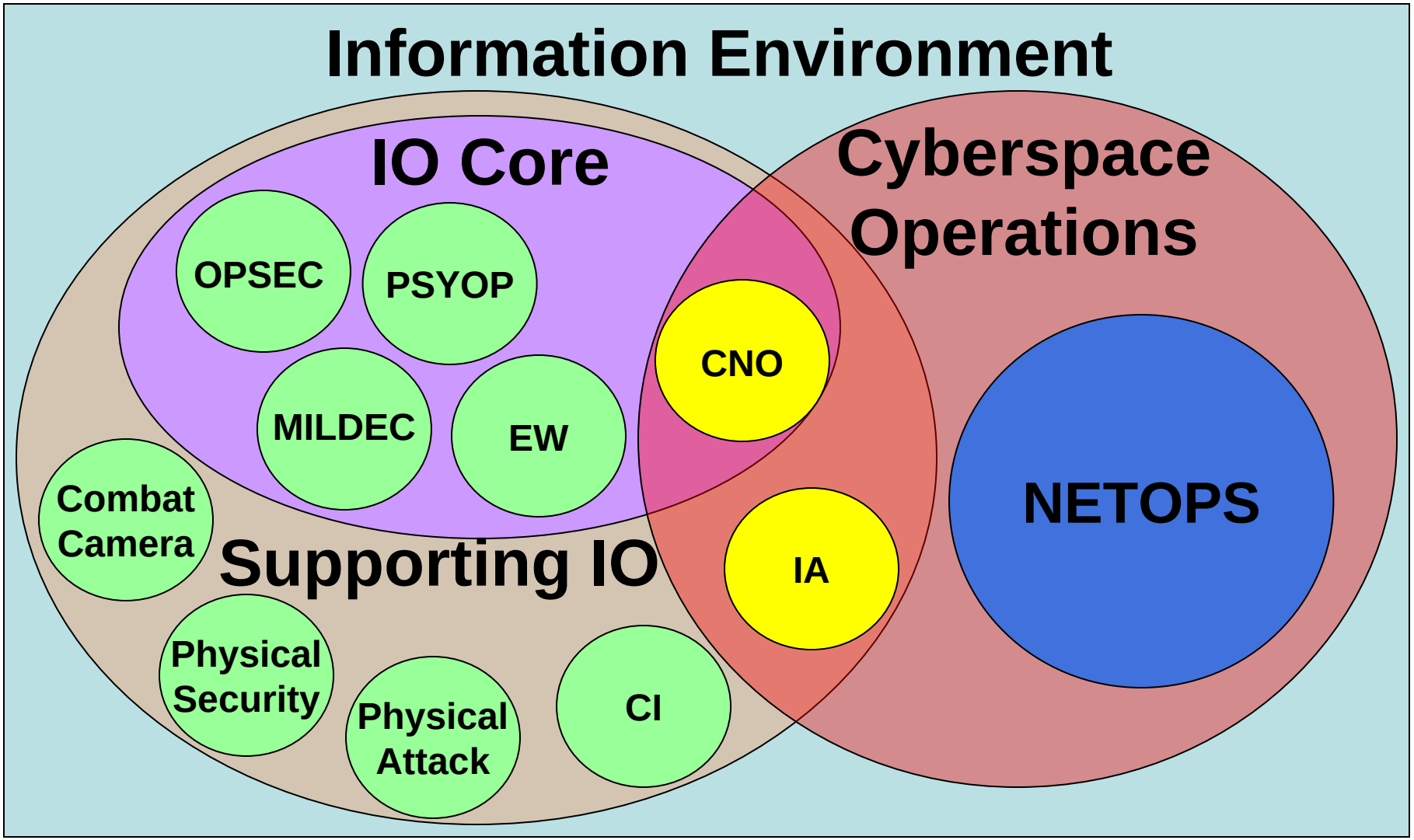
Joint Publication 1-02 *"DOD Dictionary of Military and Associated Terms"*
As amended through 19 August 2009

Cyberspace Operations

"The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the global Information Grid."

Joint Publication 1-02 *"DOD Dictionary of Military and Associated Terms"*
As amended through 19 August 2009

Information Operations and Cyberspace Operations: Current Definitions and Relationships



DoD Quadrennial Roles and Mission Review Report: Language on Education related to Cyberspace Operations

"Internally, the Department is changing its Joint Professional Military Education curricula to include more classes and information on cyberspace to improve knowledge of this domain throughout the force and among civilian employees."

Source: DOD QRM Review Report – Jan 09

Known Educational Programs and Curriculum with Cyber Content

- Ph.D. Programs
  - IA Scholarship Program
  - NSF Scholarship for Service
- Masters Programs
  - Air Force Institute of Technology and Naval Postgraduate School
  - NSF Scholarship for Service
- Certificate Programs and Short Courses
  - Information Resources Management College
- Professional Continuing Education
  - Cyber 200, Cyber 300 (IOC June/Oct 2010)
- Professional Military Education (PME)/Joint PME
  - Coverage in core courses and electives
- Accession Education
  - Cyber 100 (IOC June/Oct 2010)
- Undergraduate
  - Service Academies
  - ROTC
  - NSF Scholarship for Service

Guidance for JPME

- Officer Professional Military Education Policy (OPMEP) - CJCSI 1800.01D - 15 July 2009

- The OPMEP distributes the policies, procedures, objectives, and responsibilities for officer professional military education (PME) and joint officer professional military education (JPME).

- Current version of the OPMEP contains guidance on cyberspace operations.

Primary Joint Professional Military Education

- Institutions and Courses
  - (1) Branch, warfare, and staff specialty schools.
  - (2) Primary PME courses.
- Learning Area 1 – Joint Warfare Fundamentals
  - 6. Comprehend the effects that can be achieved with information and cyberspace operations, and the implications for tactical operations.

Service Intermediate Level Colleges

- Learning Area 4. Joint Planning and Execution Processes
  - d. Comprehend how IO and cyberspace operations are integrated at the operational level.
  - g. Comprehend the role and perspective of the combatant commander and staff in developing various theater policies, strategies, and plans, to include weapons of mass destruction/effects (WMD/E); IO; cyberspace operations; Stability, Security, Transition and Reconstruction (SSTR); intelligence; logistics; and strategic communication.

- Learning Area 5 – Joint Command and Control
  - c. Comprehend the opportunities and vulnerabilities created throughout the range of military operations by reliance on networks and information technology in cyberspace.

Service Senior Level Colleges

- JPME Phase I
  - Learning Area 4 – Joint Warfare, Theater Strategy, and Campaigning in a Joint, Interagency, Intergovernmental, and Multinational Environment
    - d. Analyze the role and perspective of the combatant commander and staff in developing various theater policies, strategies, and plans, to include WMD/E, IO, cyberspace operations, SSTR, joint intelligence, joint logistics, and strategic communication.
    - f. Analyze the integration of information and cyberspace operations to theater campaign development.
- JPME Phase II
  - Learning Area 3 - Joint Warfare, Theater Strategy, and Campaigning in a Joint, Interagency, Intergovernmental, and Multinational Environment
    - d. Analyze the role and perspective of the combatant commander and staff in developing various theater policies, strategies, and plans, to include WMD/E, IO, cyberspace operations, SSTR, joint intelligence, joint logistics, and strategic communication.

National War College and ICAF

- National War College
  - Learning Area 3 – The Military Instrument in War and Statecraft
    - d. Examine key classical, contemporary, and emerging concepts (to include IO, cyberspace operations, traditional and irregular warfare), doctrine, and approaches to war, in all its aspects.
- Industrial College of the Armed Forces (ICAF)
  - Learning Area 4 – Joint Warfare, Theater Strategy and Campaigning in a Joint, Interagency, International, and Multilateral Environment
    - d. Evaluate how information and cyberspace operations are integrated into national security, national military, and theater campaign strategies and applied to support strategic and operational endeavors in joint, interagency, intergovernmental, and multinational operations.

Challenges for Cyberspace Education in PME/JPME

- ***Faculty:*** Faculty with knowledge and experience to cover cyber topics mandated in JPME Guidance are a "low density – high demand" asset

- ***Doctrine:*** Joint Test Pub for Cyberspace Operations currently under development
  - USSTRATCOM has lead for development of Joint Test Pub on Cyberspace Operations
  - Test Pub is "more than concepts but less than doctrine"
  - Elements of cyberspace operations are currently covered in Joint Pubs 3-13 (Information Operations) and 6.0 (Joint Communications System)

Questions?

Cyber Force Structure Conference

MG Gregory Schumacher

Headquarters, Department of the Army

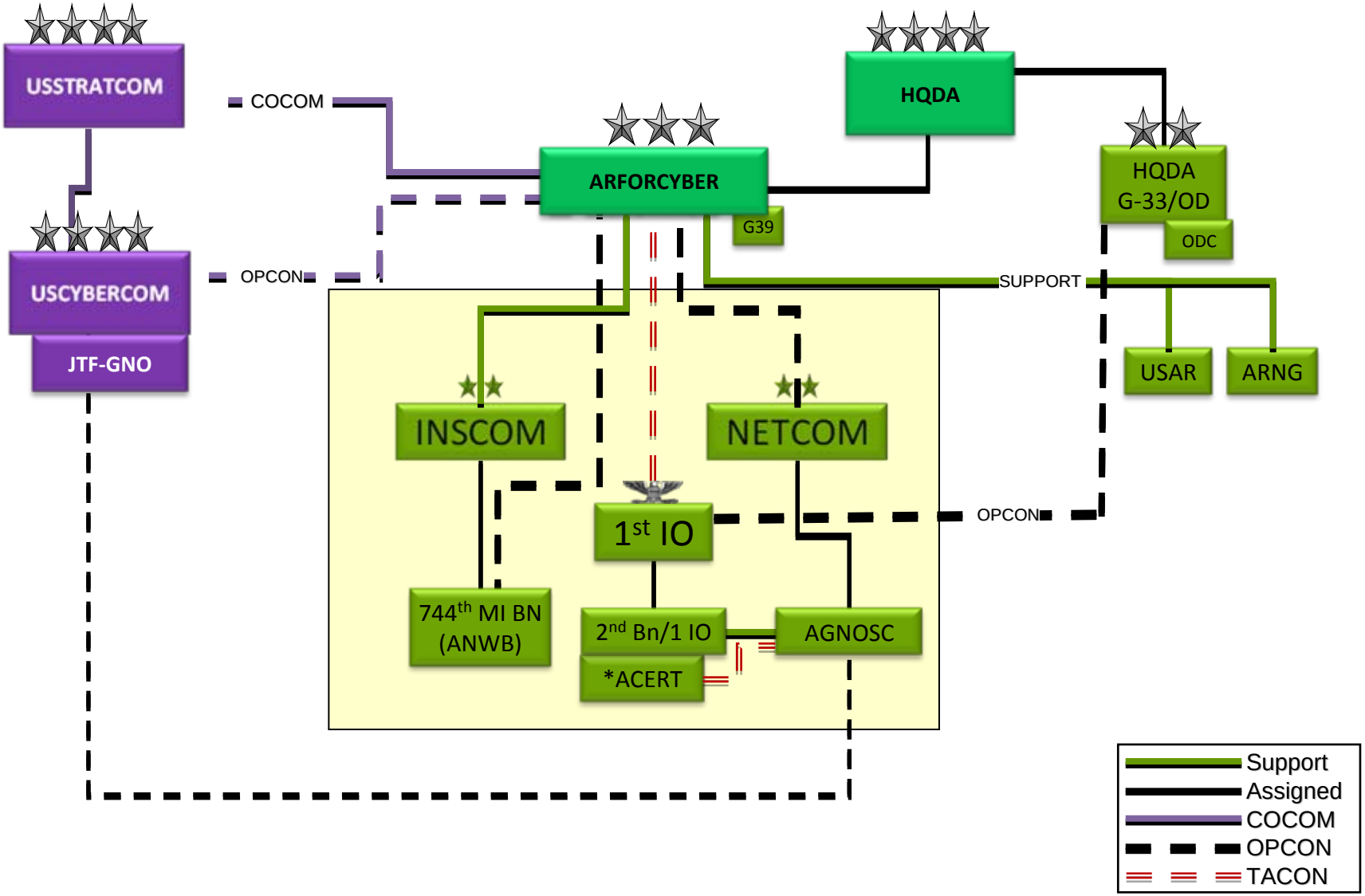
Assistant Deputy Chief of Staff, G-2

OVERALL CLASSIFICATION OF THIS BRIEFING: UNCLASSIFIED

Agenda

- Current Army Cyber Construct
- Army Cyber Functions
- Army Cyber Training
- Future of Army Cyberspace

Current Army Cyber Construct



Army Cyber Functions

- Plan and Engineer the Network
- Install and Operate the Network
- Maintain the Network
- Provide Network Services
- Defend the Network
- Provide Intelligence Support to full spectrum operations in and through Cyberspace

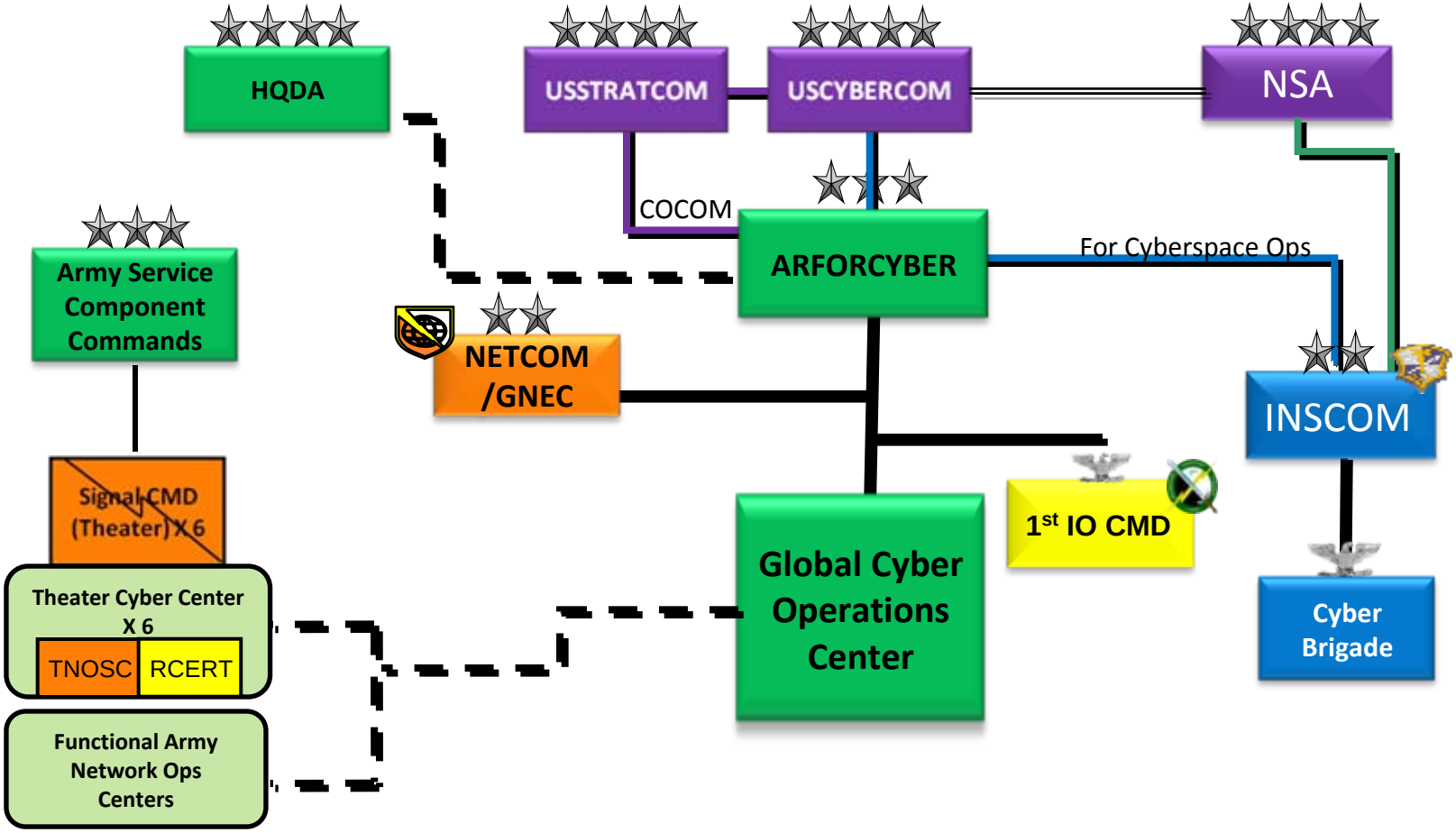
Army Cyber Training

- Branch Responsibility
  - Signal Branch man, train and equips forces to meet Network Operations requirements
  - Intelligence Branch man, trains and equips forces to meet Full Spectrum Operation requirements
- Takes years of training and hands-on experience to become proficient in Cyberspace Operations

Future of Army Cyber

- Enduring capability/requirement for the Army
- Growth is planned/programmed over next several Fiscal Years
- One of the key emphasis for the Department of Defense

Future Army Cyber Construct



Questions?

Panel 5: Views from Think Tanks

Dr. Stuart H. Starr, Chair

CTNSP, NDU

Panelists

- Alan Paller, SANS Institute
- Bob Lavigna, Partnership for Public Service
- Karen Evans, Former Administrator of E-Government and Information Technology, OMB

Some Unorthodox Solutions

- Proposals from John Arquilla, Naval Postgraduate School (NPS)
  - Mobilize “cyber militias”
  - Recruit a small number of “master hackers” (e.g., analogous to privateers)
  - Create an intelligence and technology hub, akin to Bletchley Park in World War II

Nurturing Talent Through Competitions

October 30, 2009

Alan Paller

SANS

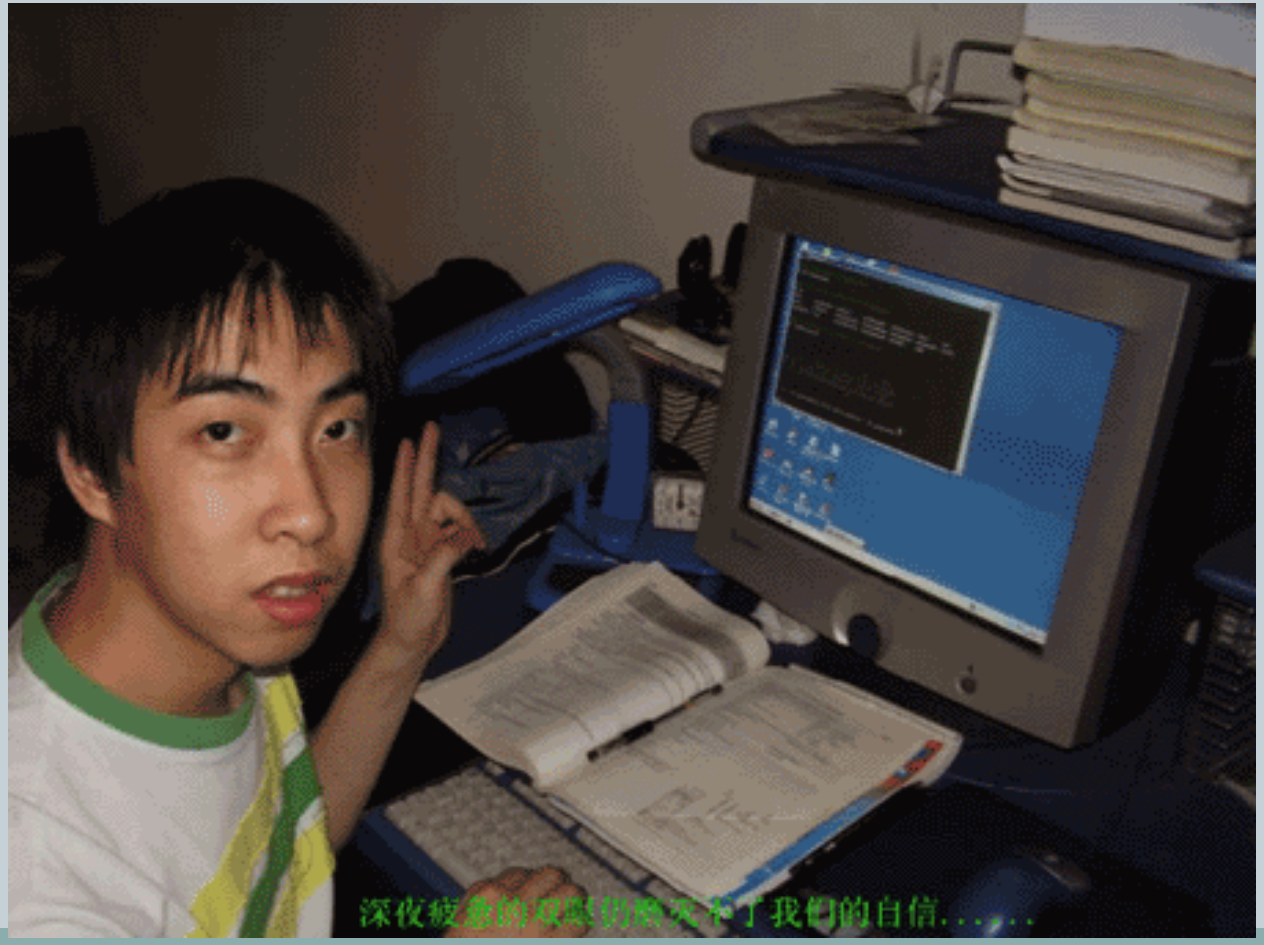
SANS INSTITUTE

Skills Matter: The US Commerce and State Department Story

The same attack – very different results

Finding the talent

Wicked Rose



Developing the future cyber warriors

"In the US we have only 1,000 people with the technical skills to compete in cyberspace at world-class levels.

We need 20,000- 30,000. Now!"

Jim Gosler, CIA's first cyber spymaster

Does the talent exist?

One survey found:

- 3 million people have downloaded hacking software
- Nearly 1 million have actually used it

How could those young people's interest and skills be harnessed for good instead of crime?

The US Cyber Challenge

- Three national competitions launching now
  - Forensics (DoD Cyber Crime Center)
  - Network defense (Air Force Association)
  - Capture the flag (SANS)
- What they get:
  - Cyber camps in colleges around the country
  - Scholarships for SANS and other courses
  - Internships at the FBI, DoE Energy Labs, US-CERT and other cool places (NSA?).
- Bottom line – find and nurture the talent we need

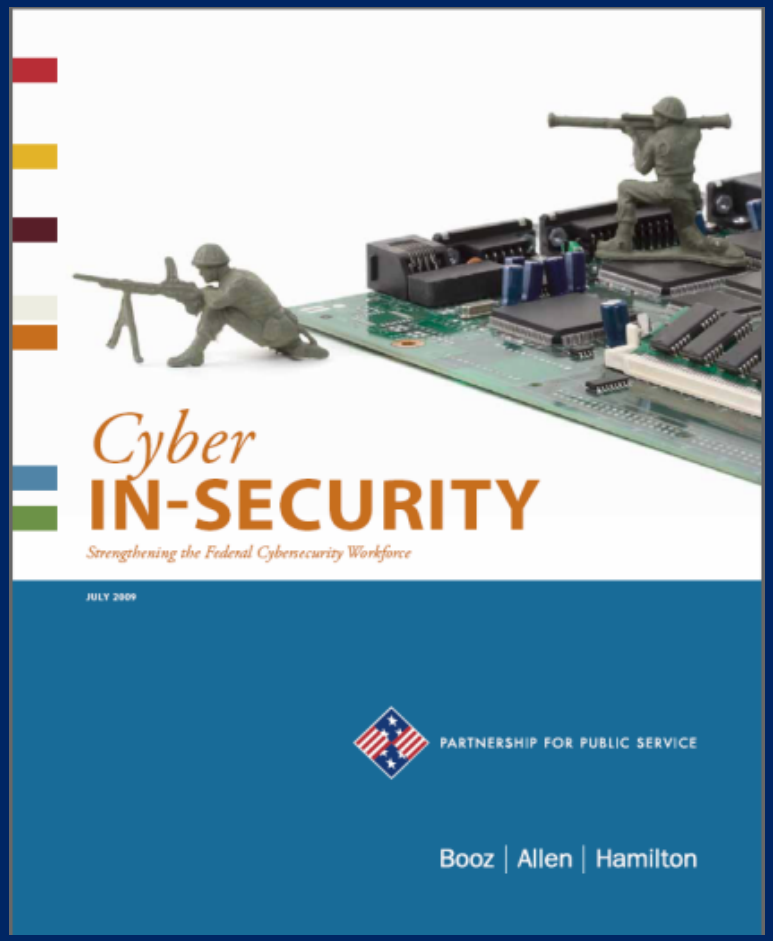
A Fourth Challenge

- Like Boy Scout merit badges
- Steps through each essential skill areas
  - Basic system administration – how servers work, basic networking
  - Building a functional web site
  - Advanced system administration – daemons, virtualization, installing web sites
  - Securing your site
  - Basic Web security - LFI, RFI, SQLi, XSS, CSRF, RCE, etc.
  - Other topics: C programming, shell vulnerabilities, other exploit paths

Your Role(s) If You Choose To Help

- Help build the exercises for Competition 4
- Get the word out to schools and others
- Sponsor awards for your city/county/state
- Sponsor one of the cyber camps
- Sponsor a scholarship for a winner
- Provide an internship (a cool one) for a winner
- Support the program administration support at CSIS

- More information: www.csis.org/uscc



PARTNERSHIP FOR PUBLIC SERVICE

Cyber IN-Security:
Strengthening the Federal Cybersecurity Workforce

Bob Lavigna
Vice President, Research
Partnership for Public Service

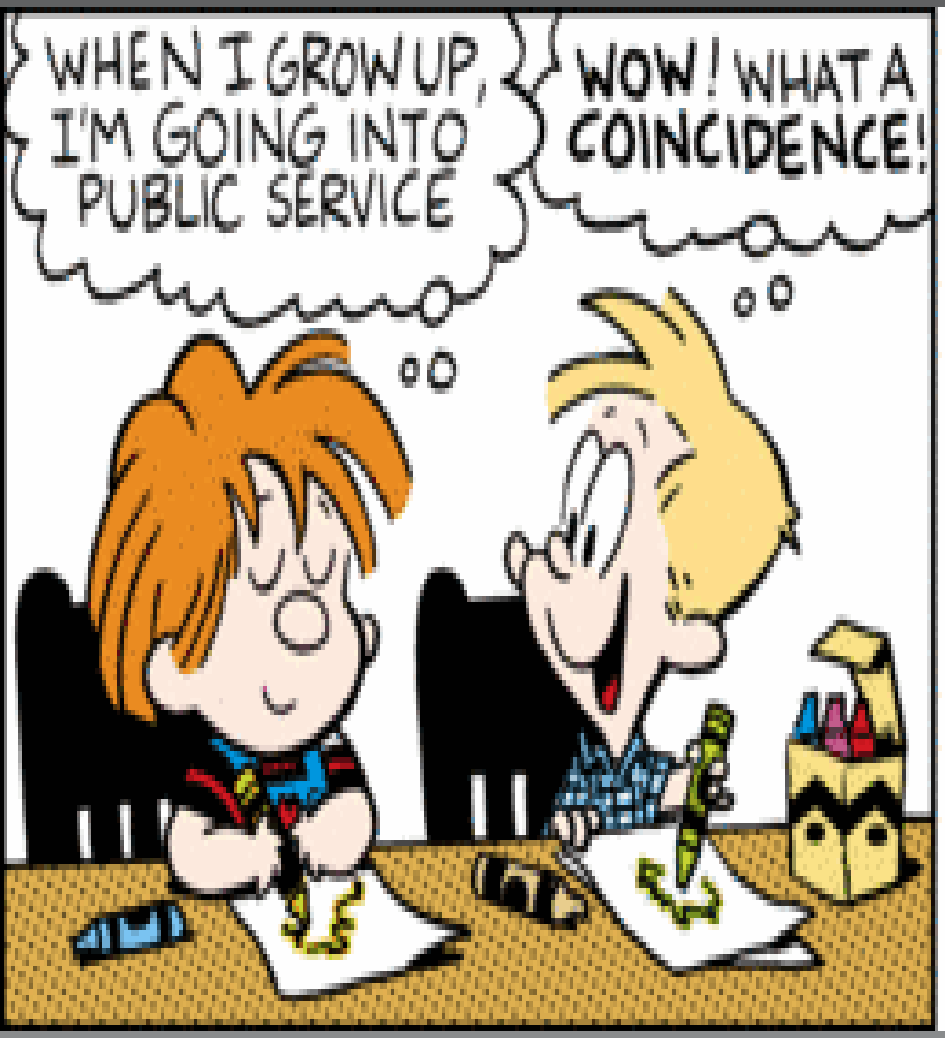
Why It Matters

"It's now clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country."

President Barack Obama
May 29, 2009

"We know that the quality of the people is more important than the quality of the wiring diagrams."

9/11 Commission


WHEN I GROW UP, I'M GOING INTO PUBLIC SERVICE
WOW! WHAT A COINCIDENCE!

I WANT TO WORK AT McDONALD'S, TOO
4-13

Cyber IN-Security: Major Findings

1. Cybersecurity talent shortage
2. No strategic approach to talent issues
3. Talent pipeline inadequate
4. Broken, complicated processes

Many Players, Varying Roles

- ★ CIO Council and Subcommittees
- ★ ODNI, DOD and NSA and other intelligence agencies
- ★ Congressional committees
- ★ Department of Homeland Security
- ★ National Institute of Standards (NIST)
- ★ National Science Foundation (NSF)
- ★ Universities
- ★ Private companies
- ★ OPM
- ★ CHCO Council
- ★ Others …

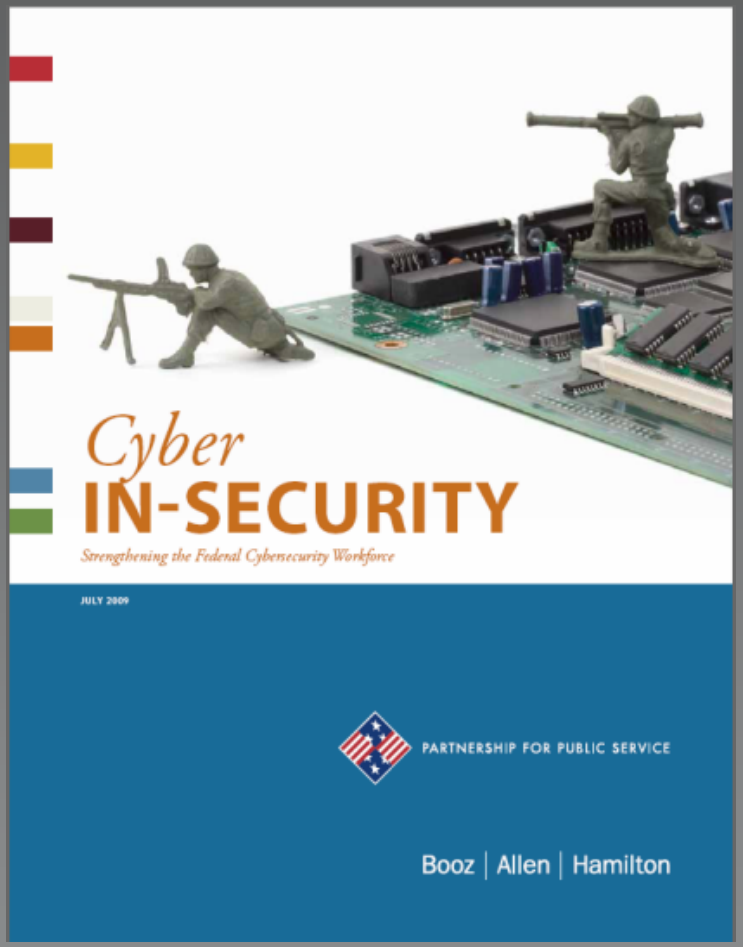
Talent Inadequate

- ★ 76% CIOs/CISOs say recruiting cyber talent high priority in next two FYs
- ★ 60% dissatisfied with quality of cyber applicants
- ★ 70% dissatisfied with quantity of cyber applicants
- ★ Programs to develop pipeline (e.g., Scholarship for Service) exist -- but demand exceeds supply

Complicated Processes/Rules

- ★ 77% CIOs, CISOs, IT managers dissatisfied with time to hire
- ★ 54% dissatisfied with security clearance delays

So, What are the Solutions?



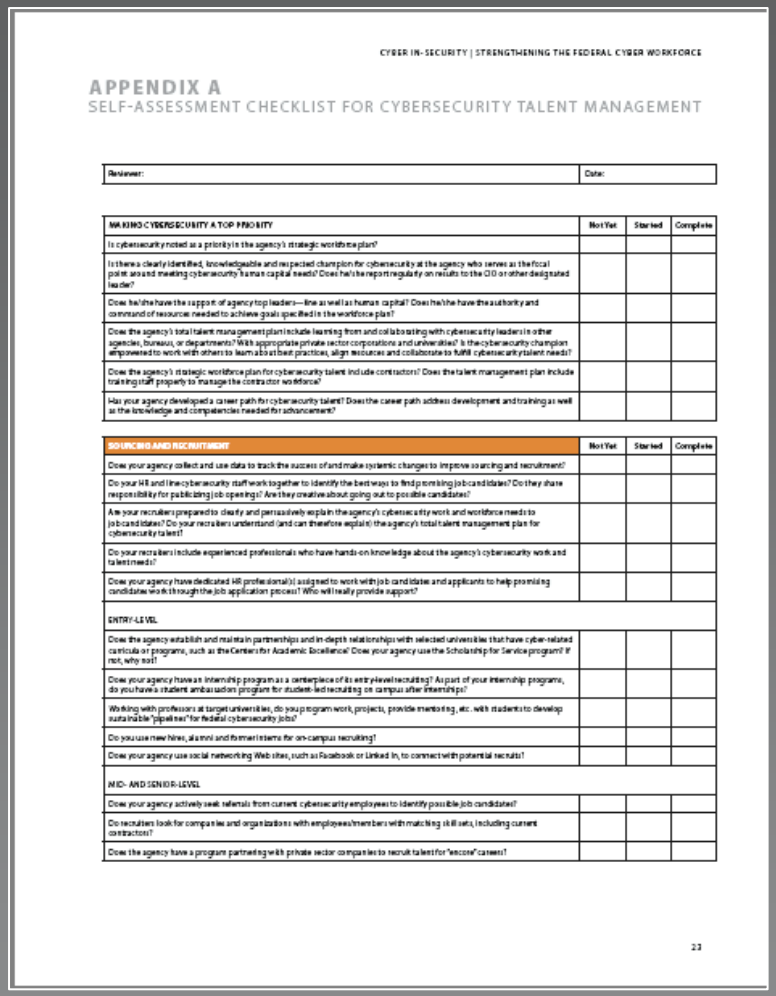
White House Cybersecurity Coordinator

- ★ Develop strategic blueprint for talent
- ★ Mobilize private sector and academia to expand talent pool

White House Cybersecurity Coordinator

Agencies

- ★ Establish responsibility: identify agency champion, define goals
- ★ Use smart recruiting and hiring tactics: "Self-Assessment Checklist" and learn from others
- ★ Train, develop and retain



CYBER IN-SECURITY | STRENGTHENING THE FEDERAL CYBER WORKFORCE

APPENDIX A
SELF-ASSESSMENT CHECKLIST FOR CYBERSECURITY TALENT MANAGEMENT

Reviewer:	Date:

MAKING CYBERSECURITY A TOP PRIORITY	Not Yet	Started	Complete
Is cybersecurity noted as a priority in the agency's strategic workforce plan?			
Is there a clearly identified, knowledgeable and respected champion for cybersecurity at the agency who serves as the focal point around meeting cybersecurity human capital needs? Does he/she report regularly on results to the CIO or other designated leader?			
Does he/she have the support of agency top leaders—line as well as human capital? Does he/she have the authority and command of resources needed to achieve goals specified in the workforce plan?			
Does the agency's total talent management plan include learning from and collaborating with cybersecurity leaders in other agencies, bureaus, or departments? With appropriate private sector corporations and universities? Is the cybersecurity champion empowered to work with others to learn about best practices, align resources and collaborate to fulfill cybersecurity talent needs?			
Does the agency's strategic workforce plan for cybersecurity talent include contractors? Does the talent management plan include training staff properly to manage the contractor workforce?			
Has your agency developed a career path for cybersecurity talent? Does the career path address development and training as well as the knowledge and competencies needed for advancement?			

SOURCING AND RECRUITMENT	Not Yet	Started	Complete
Does your agency collect and use data to track the success of and make systemic changes to improve sourcing and recruitment?			
Do your HR and line-cybersecurity staff work together to identify the best ways to find promising job candidates? Do they share responsibility for publicizing job openings? Are they creative about going out to possible candidates?			
Are your recruiters prepared to clearly and persuasively explain the agency's cybersecurity work and workforce needs to job candidates? Do your recruiters understand (and can therefore explain) the agency's total talent management plan for cybersecurity talent?			
Do your recruiters include experienced professionals who have hands-on knowledge about the agency's cybersecurity work and talent needs?			
Does your agency have dedicated HR professional(s) assigned to work with job candidates and applicants to help promising candidates work through the job application process? Who will really provide support?			
ENTRY-LEVEL			
Does the agency establish and maintain partnerships and in-depth relationships with selected universities that have cyber-related curricula or programs, such as the Centers for Academic Excellence? Does your agency use the Scholarship for Service program? If not, why not?			
Does your agency have an internship program as a centerpiece of its entry-level recruiting? As part of your internship programs, do you have a student ambassadors program for student-led recruiting on campus after internships?			
Working with professors at target universities, do you program work, projects, provide mentoring, etc. with students to develop sustainable "pipelines" for federal cybersecurity jobs?			
Do you use new hires, alumni and former interns for on-campus recruiting?			
Does your agency use social networking Web sites, such as Facebook or LinkedIn, to connect with potential recruits?			
MID- AND SENIOR-LEVEL			
Does your agency actively seek referrals from current cybersecurity employees to identify possible job candidates?			
Do recruiters look for companies and organizations with employees/members with matching skill sets, including current contractors?			
Does the agency have a program partnering with private sector companies to recruit talent for "encore" careers?			

23

PARTNERSHIP FOR PUBLIC SERVICE
OURPUBLICSERVICE.ORG

OPM

- ★ Assign high-level team to develop government-wide cybersecurity talent management plan
- ★ Fix federal hiring process
- ★ Resolve long-standing problems around IT classifications, career paths, competitive salaries

OPM

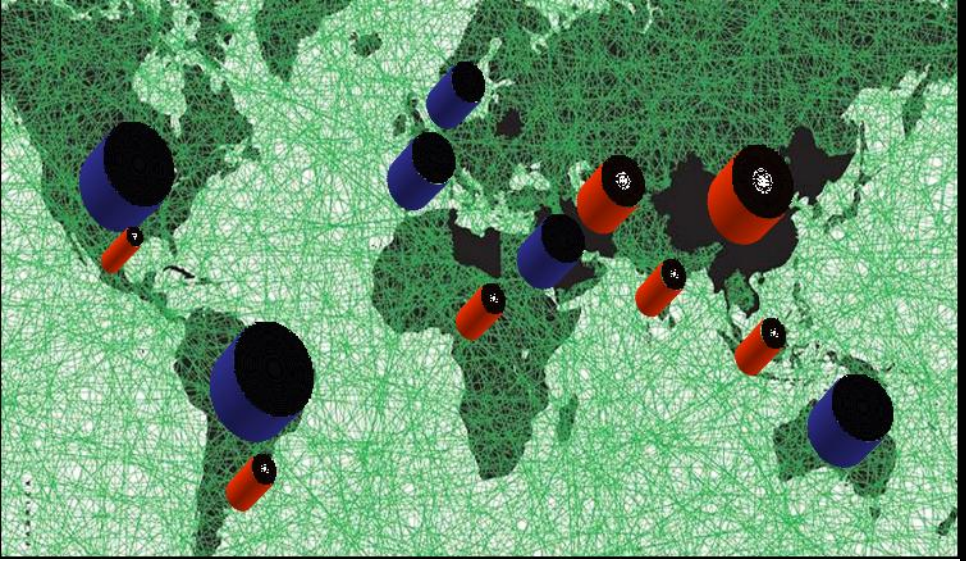
Congress

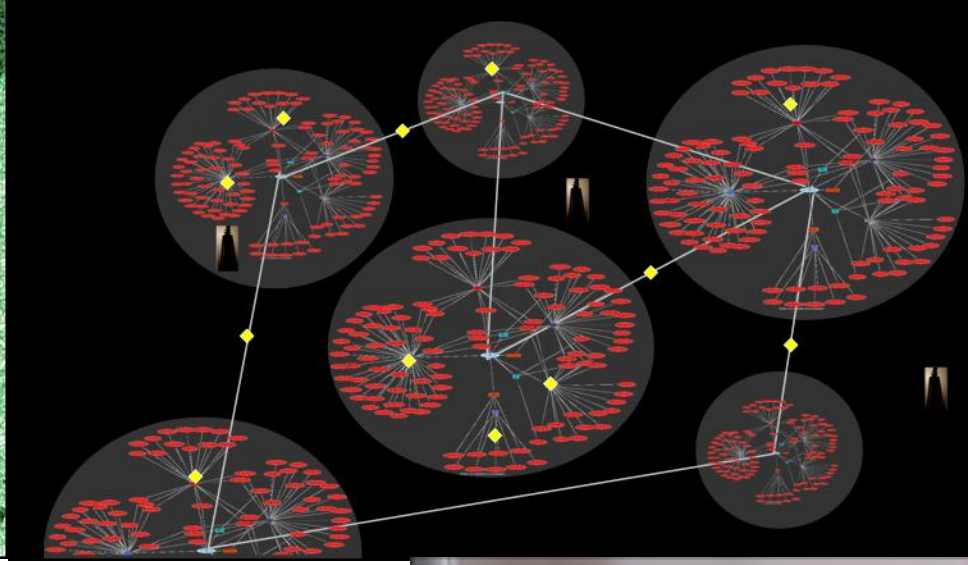
- ★ Provide funding to keep federal talent "state of the art"
- ★ Expand programs to train students
- ★ Exercise oversight via annual reports on the "health" and capacity of the cybersecurity workforce

Congress

PARTNERSHIP FOR PUBLIC SERVICE

ourpublicservice.org





CYBER:
Views From Industry

Bennett R. Hart , VP
Chairman AFCEA CYBER Policy Committee

A presentation to:

Cyber Force Structure Conference

Center for Technology and National Security Policy (CTNSP)

National Defense University (NDU)

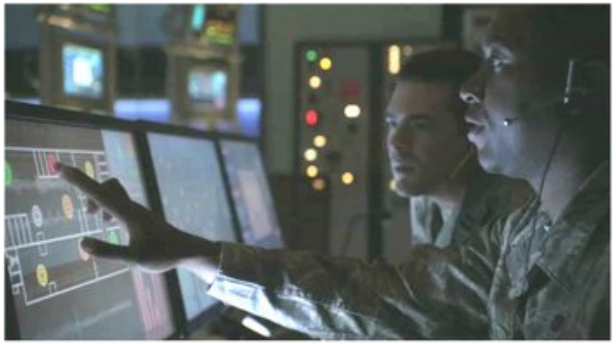
Oct. 30, 2009

© Copyright QinetiQ North America Operations LLC 2009

Our Adversaries can be Local or Global

Cyber Attacks Traced to the U.S., Britain

By Kim Zetter July 14, 2009 | 2:58 pm | Categories: Cybersecurity



International fingerpointing in the recent cyber attacks against U.S. and South Korean websites has widened to include Great Britain, as researchers examining the attacks trace them to a server in the United Kingdom.

But the British company that owns the server says it, in turn, traced the attacks to a VPN connection originating in Miami, Florida.

With hawks in Congress and the press urging President Barack Obama to launch an all-out cyber war in retaliation for the website outages, things are looking bad for the Sunshine State. Though it should be noted that the Miami connection was likely just another proxy used by the hacker, who could be based in the U.S. or anywhere else.

Researchers at Bkis Security in Hanoi, who reported findings about the British server on their company's blog, say that the denial-of-service attacks that struck more than three dozen government and commercial sites last week were launched from more than 166,000 computers in 74 countries controlled by a server in the UK. The IP range for the server is 195.90.118.xxx, which is registered to Global Digital Broadcast,

http://www.wired.com/threatlevel/2009/07/brits-attack-us/

© Copyright QinetiQ North America Operations LLC 2009

CYBER: Views from Industry

1. Industry Vulnerabilities
2. Balance Cybersecurity Risks
3. Cyber Policies, Rules of Engagement (ROEs)
4. Multiplicity of Definitions
5. Professional Cyber Career Field

© Copyright QinetiQ North America Operations LLC 2009

Control Industry Vulnerabilities

- Employee Awareness
- Make / procure the tool sets
- Get the latest security patches
- Work with government security (CERTS / NOCS)
- Control internal network policy (personal computers / use)

© Copyright QinetiQ North America Operations LLC 2009

Balance Cybersecurity Risks

- Balance communications, interoperability and timeliness
- Must triage the systems and networks with users
- Kids blogs ? Picture phones?
- SIPRNET hard to get ? DD 254? 18 months? Locked up ?
- Publish Guidelines

© Copyright QinetiQ North America Operations LLC 2009

Cyber Policy / Rules of Engagement

- Northwest Airlines Flight 188 to Minneapolis
- What do when under attack ? Close down ? Reduce applications ? Attack back ?
- What are the strategies ? Back up ? COOP ?
- Wargames – Schriever, Carlisle Barracks, Newport
- “Grey Beard” Sessions – Table tops

© Copyright QinetiQ North America Operations LLC 2009

Multiplicity of Definitions

- The standardization and consolidation of the multiplicity of definitions that exist today in the Cyber Domain may be too hard?
- Bring the Communities of Interest (COIs) together
- Understand what the other organization means with terms
  - Identify
  - Attribution
  - Forensics

© Copyright QinetiQ North America Operations LLC 2009

Professional Cyber Career Field

- Within the government,
- Within industry
- Within academia
- Identify core classes
- Provide degree areas / experience certifications

© Copyright QinetiQ North America Operations LLC 2009

What You Have Seen

- … Network edge defenses are permeable
- Adversaries test and know the way in
- The trust model of interconnected systems are exploited
- There is a business case and roadmap to the development of these techniques.

THE H SECURITY

6 July 2009, 10:25

Ex-Goldman Sachs developer arrested for code theft

According to a **Reuters report[1]** Sergey Aleynikov, a Russian immigrant living in the US, was arrested by the FBI on the 3rd of July for stealing code from a New York based financial institution. The report states that it is believed that Aleynikov had worked at Goldman Sachs from 2007 until June 2009, and was responsible for "the development of a real time co-located high frequency trading platform".

A copy of the affidavit at **the Zerohedge blog[2]** alleges that Aleynikov notified the "Financial institution" that employed him that he intended to resign and move to a new company based in Chicago which was engaged in high volume automated trading. The affidavit goes on to allege that Aleynikov, in his last days at his employer, configured his desktop system to copy and compress files, encrypt the resulting file and move an estimated 32MB of data over an https connection to web site based in Germany.

Aleynikov, according to the affidavit, "claimed, however, that he only intended to collect 'open source' files on which he had worked, but later realised that he had obtained more files than he intended" and that he denies that he has distributed any of the "Financial institution's" proprietary software. The affidavit says, though, that the encryption of the files and the subsequent deletion of the software used to encrypt them indicates some other motivation.

(dj/wm[3])

URL of this article:
http://www.h-online.com/security/news/113691

Links in this article:
[1] http://blogs.reuters.com/commentaries/2009/07/05/a-goldman-trading-scandal/
[2] http://zerohedge.blogspot.com/2009/07/is-case-of-quant-trading-industrial.html
[3] mailto:djw@h-online.com

THE WALL STREET JOURNAL.

Computer Spies Breach Fighter-Jet Project

North Korean hackers blamed for sweeping cyber attack on US networks

By Matthew Shaer | 07.08.09

Print this | Letter to the Editor | Republish | Email and share | Get e-mail alerts | RSS

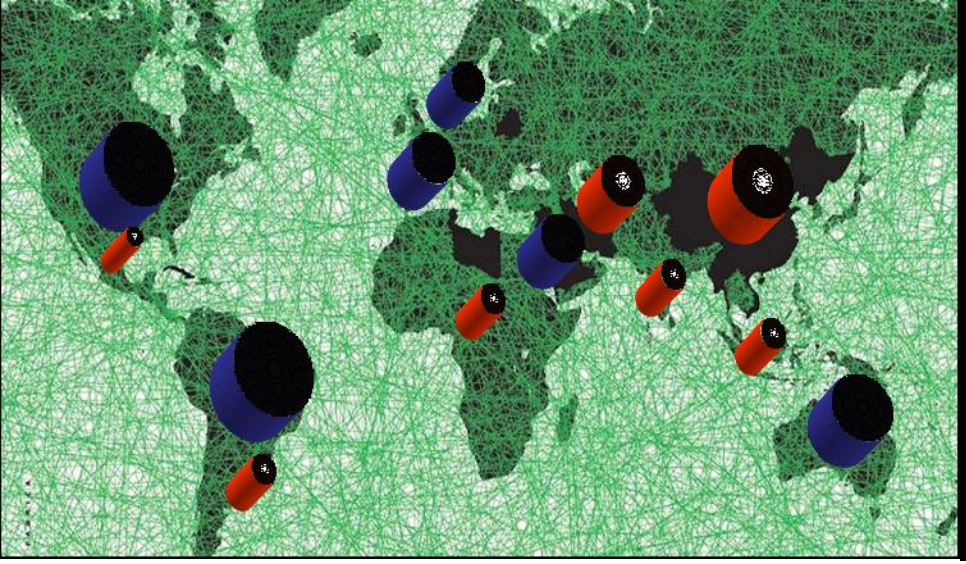
Update: Attacks continue today in South Korea

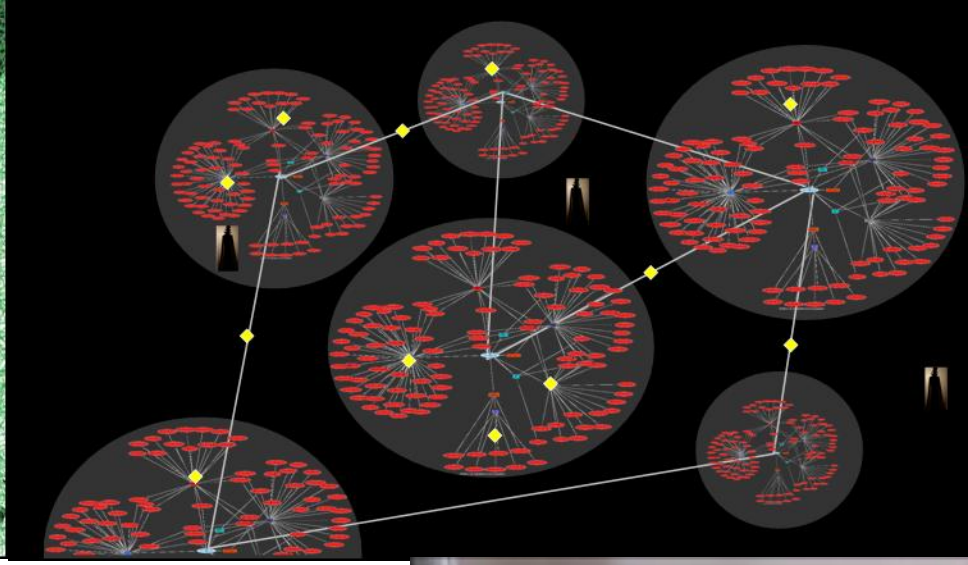
A series of attacks on computer networks in South Korea and the US was apparently the work of North Korean hackers, several news agencies are reporting today. The attacks, which targeted the White House, the Pentagon, and the Washington Post, among other high-level institutions, are raising concerns that the long-simmering conflict with North Korea is expanding into a dangerous new theater.

According to Seoul's National Intelligence Service, the "attacks appeared to have been elaborately prepared and staged by a certain organization or state." In that statement, North Korea was not specifically named, but the Yonhap news agency said the NIS had traced the attacks to North Korea

Adversaries test against the known defenses

© Copyright QinetiQ North America Operations LLC 2009





CYBER:
Views From Industry

Bennett R. Hart , VP
Chairman AFCEA CYBER Policy Committee

A presentation to:

Cyber Force Structure Conference

Center for Technology and National Security Policy (CTNSP)

National Defense University (NDU)

Oct. 30, 2009

© Copyright QinetiQ North America Operations LLC 2009