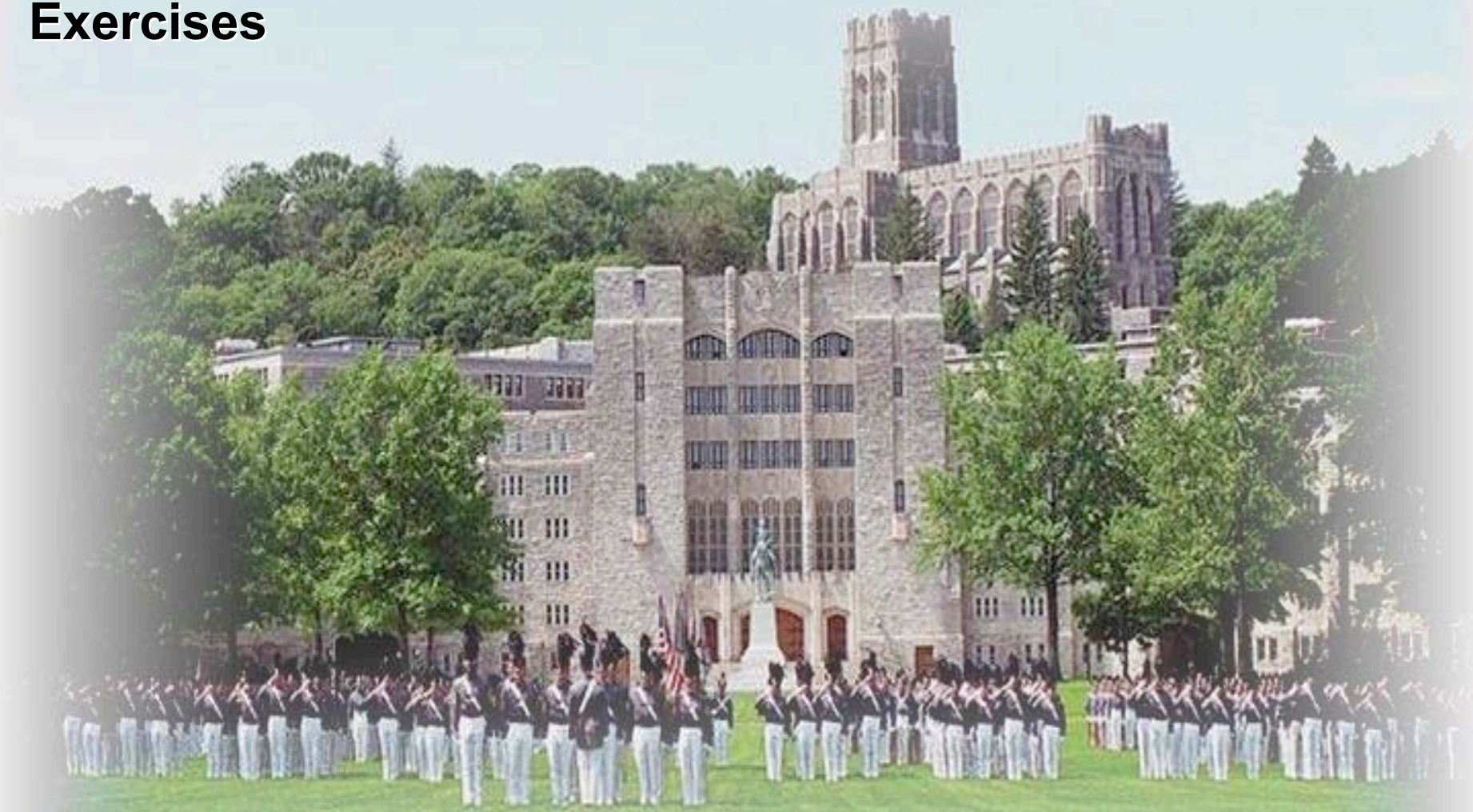
Enhancing Network Security Through Competitive Cyber Exercises



USENIX '05 Annual Technical Conference

Colonel Dan Ragsdale, Ph.D.
daniel.ragsdale@usma.edu – http://www.itoc.usma.edu/ragsdale

Bottom Line Upfront (BLUF)

- Cyberspace is the ultimate intellectual battlefield
- Enhance education and awareness through
  - Competition
  - Active learning
  - Team efforts
- Competitive cyber exercises are scalable
  - … therefore, feasible
- Learn from our lessons
  - http://www.itoc.usma.edu/cdx
  - Exploring a **National Cyber** Security **Exercise** for Universities

Agenda

- Background
- CDX Stuff
- So what?
- Questions

Presentation Highlights

- 1 Experiment
  - Raise hands
- No DBP
- No Silly Glasses
- No Imitations (unless you insist)
- Surgeon General's Warnings
- Not an infomercial for West Point!
- Acronym Police
- Best Contributor

Speaker Background

- Expectation Management
- A “Real” Infantry Officer
- Birth Order
- Teacher
- Texas Aggie
- Irreverence – no intent to offend!

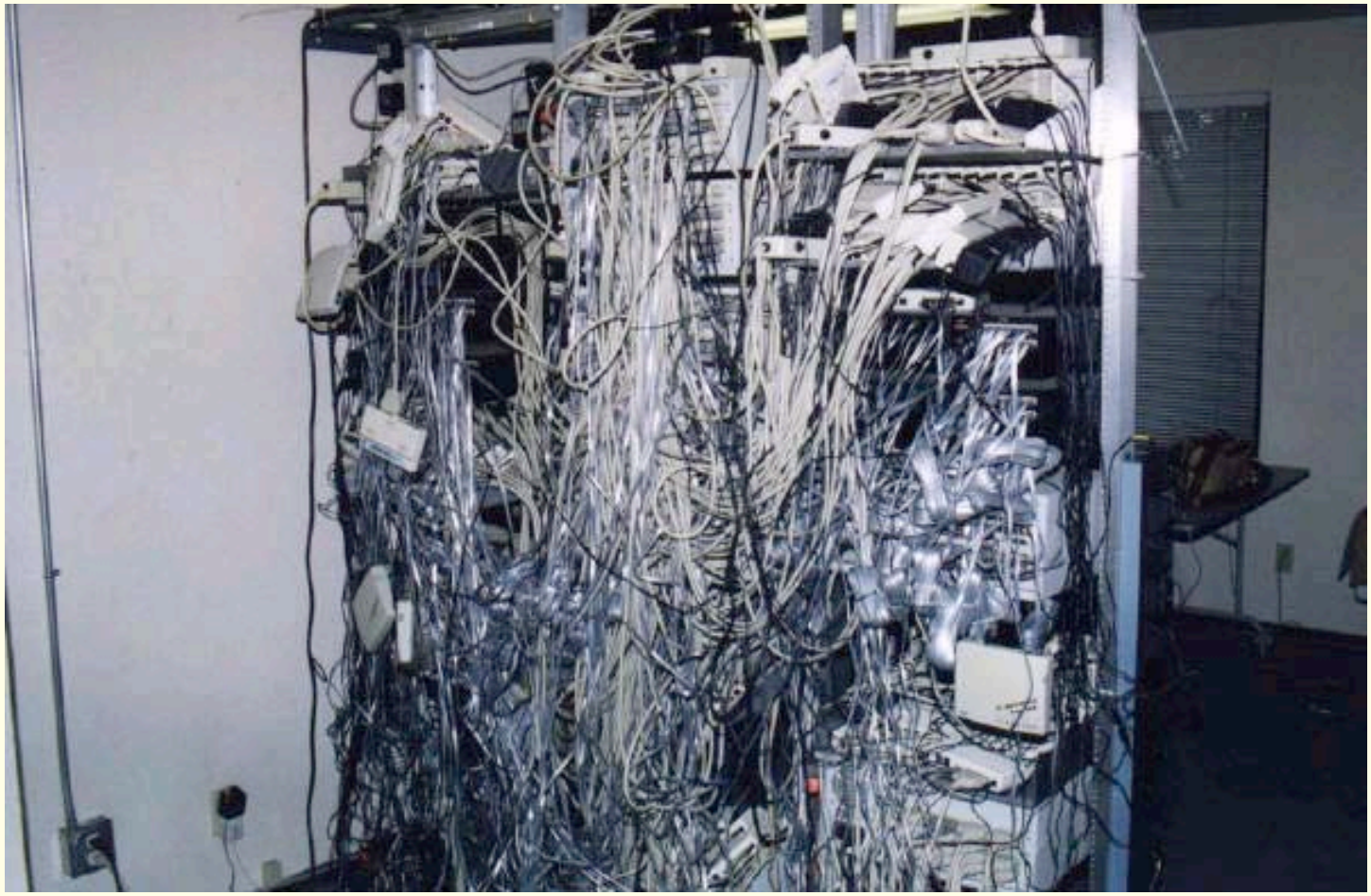
General Motivation

- Google Results on “Phishing”
  - 3 Aug 2004
    - Results 1 - 10 of about **995** for **phishing**
  - 14 April 2005
    - Results 1 - 10 of about **4,680,000** for **phishing.**
    - Results **1** - **10** of about **41,500,000** for **fishing**
- Other results on 14 April 2005
    - Results **1** - **10** of about **15,200,000** for **spyware**
    - Results **1** - **10** of about **76,200,000** for **spam**

More Specific Motivation

- Current “Buzz words”
  - Information-driven Organization
  - Network Centric Warfare
  - Asymmetrical Warfare
- Lt. General Boutelle, Army CIO
  - “Cyber Security is a Force Protection Issue!”
- Traffic Distribution
- Unaware Users – information leakage
  - Yahoo Accounts
  - Blogs
  - Green Zone Information (next slide)

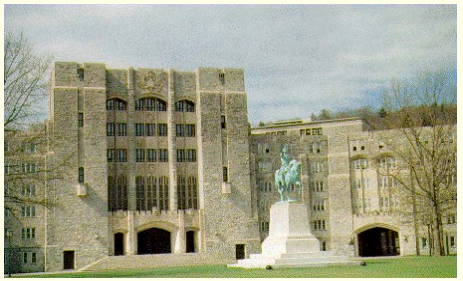
Do We Need More Motivation?



USMA Essential Mission

To develop leaders of character for our Army who are inspired to careers as Army officers and lifetime service to the nation

USMA Vision



…to be the world's premier leader development institution

Preparation from a Military Perspective

"[To] not prepare is the greatest of crimes; to be prepared beforehand for any contingency is the greatest of virtues."

Sun Tzu

From a presentation by:
Craig E. Kaucher
LTC, U.S. Army

USMA IA Education Overriding Goal

Enhance IA education with true *hands-on* experiences

I see and I forget…

I hear and I remember…

I do and I understand.

Attributed to Confucius

Is competition really such a bad thing?

- Mom: “Honey, Everyone is special,”
- Dash: "Which is another way of saying nobody is.”

Our "Solution"

- We needed an exercise that is
  - Competitive (with a really big trophy)
  - Hands-on
  - Realistic
  - Team-based
- The CDX was born!

How to Achieve Your Goals in the Workplace (Next slide)

Encoding Scheme

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z are represented by:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

What qualities help us to achieve our goals?

K N O W L E D G E - 11 14 15 23 12 5 4 7 5 = 96%

H A R D W O R K - 8 1 18 4 23 15 18 11 = 98%

A T T I T U D E - 1 20 20 9 20 21 4 5 = 100%

Having the ability to **BS BULL….** 2 21 12 12 19 8 9 20 = 103%

What can we conclude?

If you want to achieve your goals in the workplace…

What did we leave out?

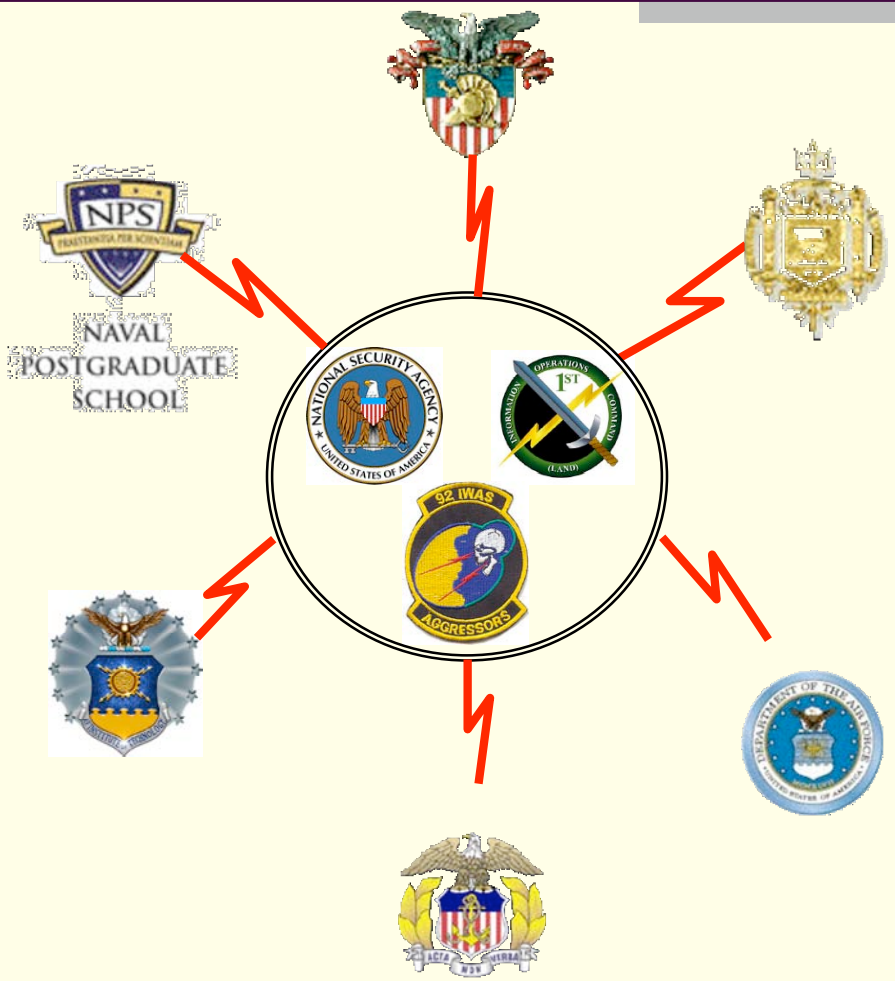
http://www.whogotya.com/pages/Humor/hardwork.htm

Other "Intellectual" Competitions

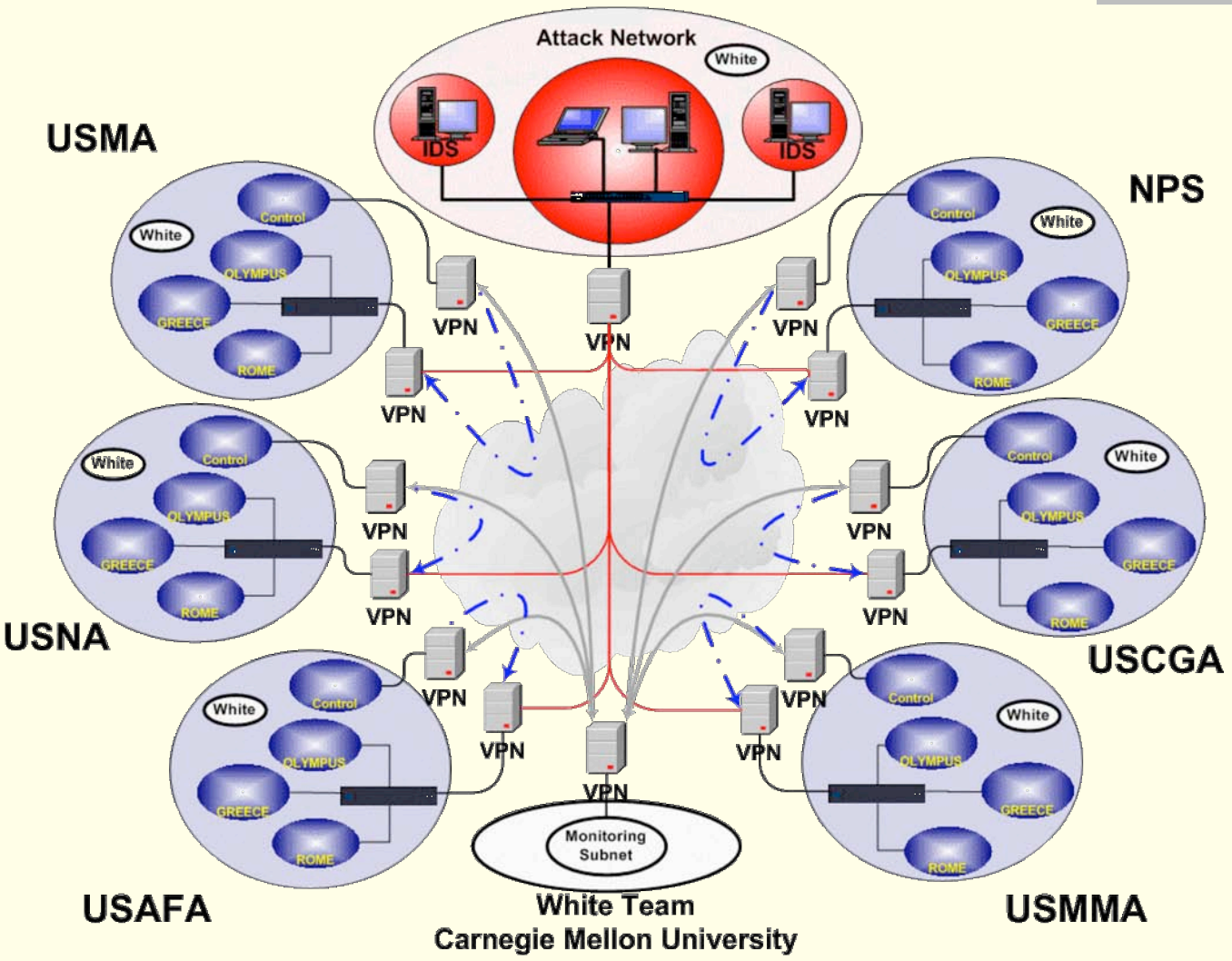
- Chess
- Poker
- Jeopardy / Who Wants to be a Millionaire / The Intern
- DEFCON 12 Contests
  - **Capture the Flag**
  - **Wi-Fi Shootout II**
  - Wardrive
  - Robot Warez
  - IP Appliance Contest
  - Coffee Wars V
  - Lockpick
  - Scavenger Hunt

Cyber Defense Exercise (CDX)

- Inter-Service Academy competition
- Focus on defense
- Conceived at West Point
- Directed and sponsored by the NSA



Cyber Defense Network



CDX Award Ceremony

Cyber Defense Exercise General Concept

- Generic Components
  - Blue Forces - US Service Academies, NPS and AFIT
  - Red Forces - NSA, the USAF 92nd IW Aggressor Sqdn, and the US Army 1st IO Command
  - White Cell – CERT and SEI at Carnegie Mellon
- Scoring based on
  - Maintaining required functionality
  - Defending against an intrusions
  - Reporting of all suspicious activity

The US Navy:
Our Brothers and Sisters in Arms

ACTUAL transcript of a US naval ship with Canadian authorities off the coast of Newfoundland in October, 1995. This radio conversation was released by the Chief of Naval Operations on 10-10-95.

Actually a hoax : see http://www.snopes.com/military/lighthse.htm

CDX Timeline

- 1997
  - Military Academy Cyber competition concept conceived (Texas A&M and Waxahachie)
- 1999
  - Initial coordination visit USMA / USAFA
- 2000
  - NSA Fellow arrives at USMA
  - Focus on defense
  - NSA and PKI PM Office Funding
  - Hard work!

CDX Timeline

- 2001 – 1st CDX
  - USMA, USAFA, and NPS
  - Blue Forces and Red Forces
  - Bar Room Brawl
- 2002 – 2nd CDX
  - USMA, USAFA, USNA, USCGA, and NPS
  - Blue Forces, Red Forces, and White Cell
  - Better student performance, but less “action”
  - Approved Software lists (i.e., Honeynet SW)
    - Managed by White Cell
    - Not advertised
- 2003 – 3rd CDX
  - USMA, USAFA, USNA, USCGA, USMMA, NPS, AFIT
  - Blue Forces, Red Forces, White Cell, and Orange Forces
  - Some Denial of Service attacks allowed
  - Anomalies

CDX Timeline

- 2004 – 4th CDX
  - USMA, USAFA, USNA, USCGA, USMMA, AFIT
  - Refined anomalies
  - "Attack server" maintained at each school
  - Social engineering allowed
  - 24-hour active period
- 2005 – 5th CDX (ongoing)
  - Same competitors
  - Further Refined anomalies
  - More Forensics

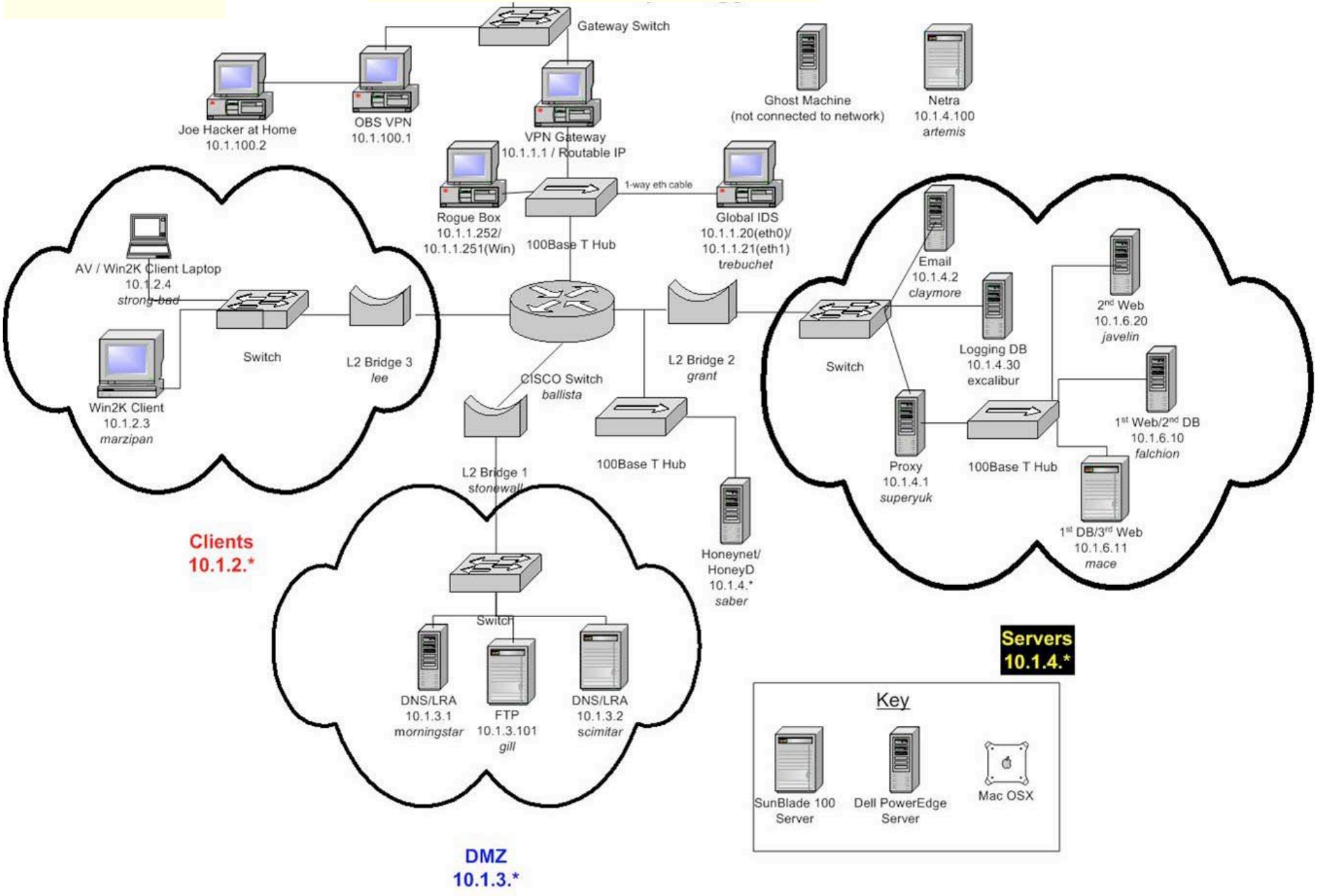
General Benefits

- Approximately 300 Participants (and national attention)
  - Cadets and Midshipmen
  - Dozens of faculty
  - Red Teams and White Teams
- The bar has been raised at all participating schools!!!
- Known Spin offs
  - IA Defense Exercise
  - International Exercise
  - NSF Workshop to Define a National Cyber Defense Exercise Competition (IEEE S&P)
  - Collegiate Cyber Defense Competition (CCDC®)

Developmental Benefits

- Great increases in:
  - Technical knowledge
  - Awareness
  - Interest (at individual and senior leader levels)
- Developmental benefits
  - Leadership Skills
  - Organizational Skills
  - Communication Skills
- How measured
    - Student and Lieutenant feedback
    - Red team and faculty observation

Student Design 2004



Challenges / Lessons Learned

- High level support is essential
- Funding for infrastructure and support
- CDN initial setup and administration
- Coordination with external participants
- Faculty and student time commitment
- Live network traffic
- White Cell is critical
- Offensive tools are not necessary!
- Many more…

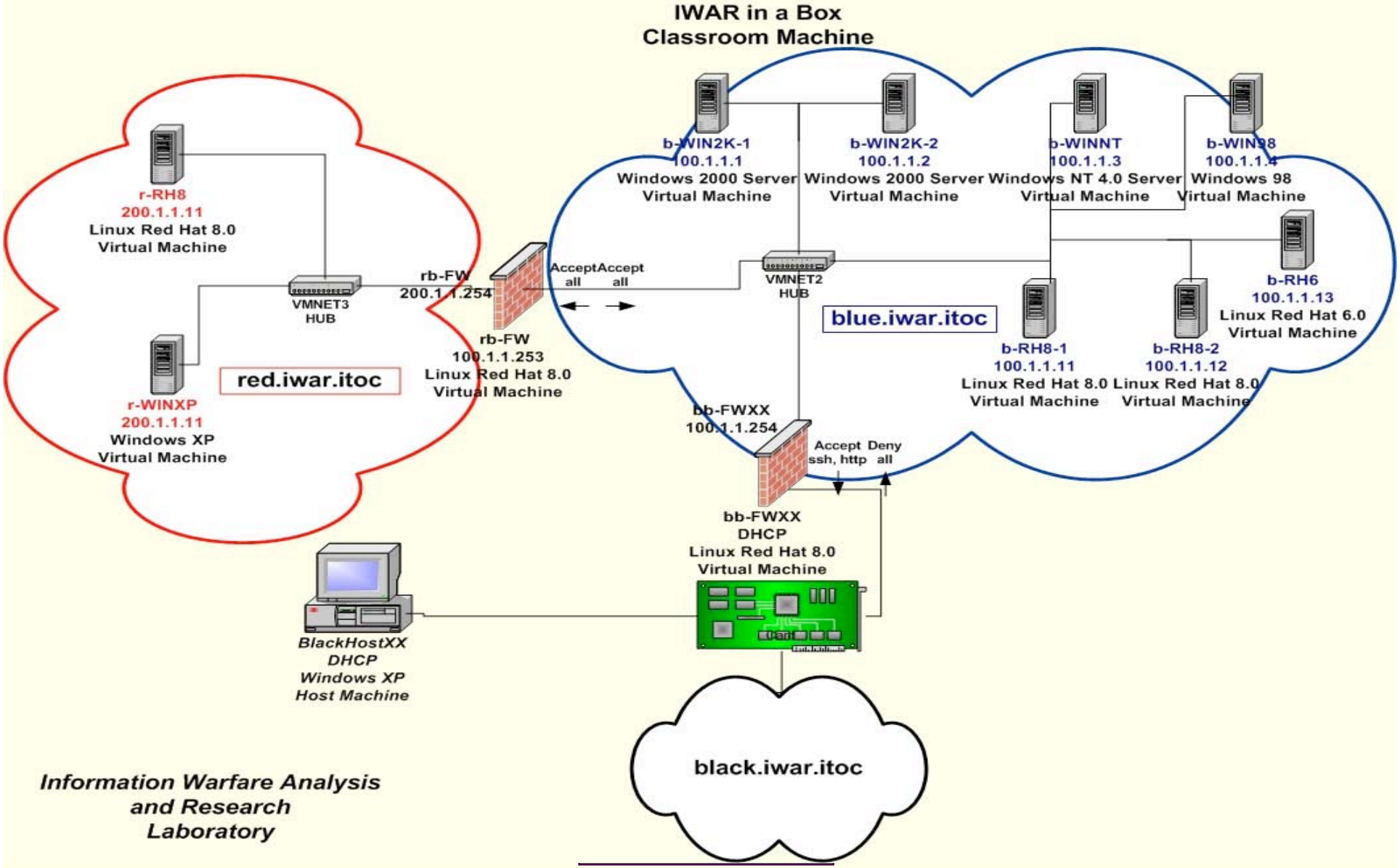
Considerations for CDX Competitions at Other Settings – this is the key slide!

- Exercise Duration
- Exercise Purpose
- Exercise Scope
- Exercise Scenarios
- Participant Locations
  - Red Teams
  - Blue Teams
  - White Cell
- Red team makeup
- Equipment
- Funding

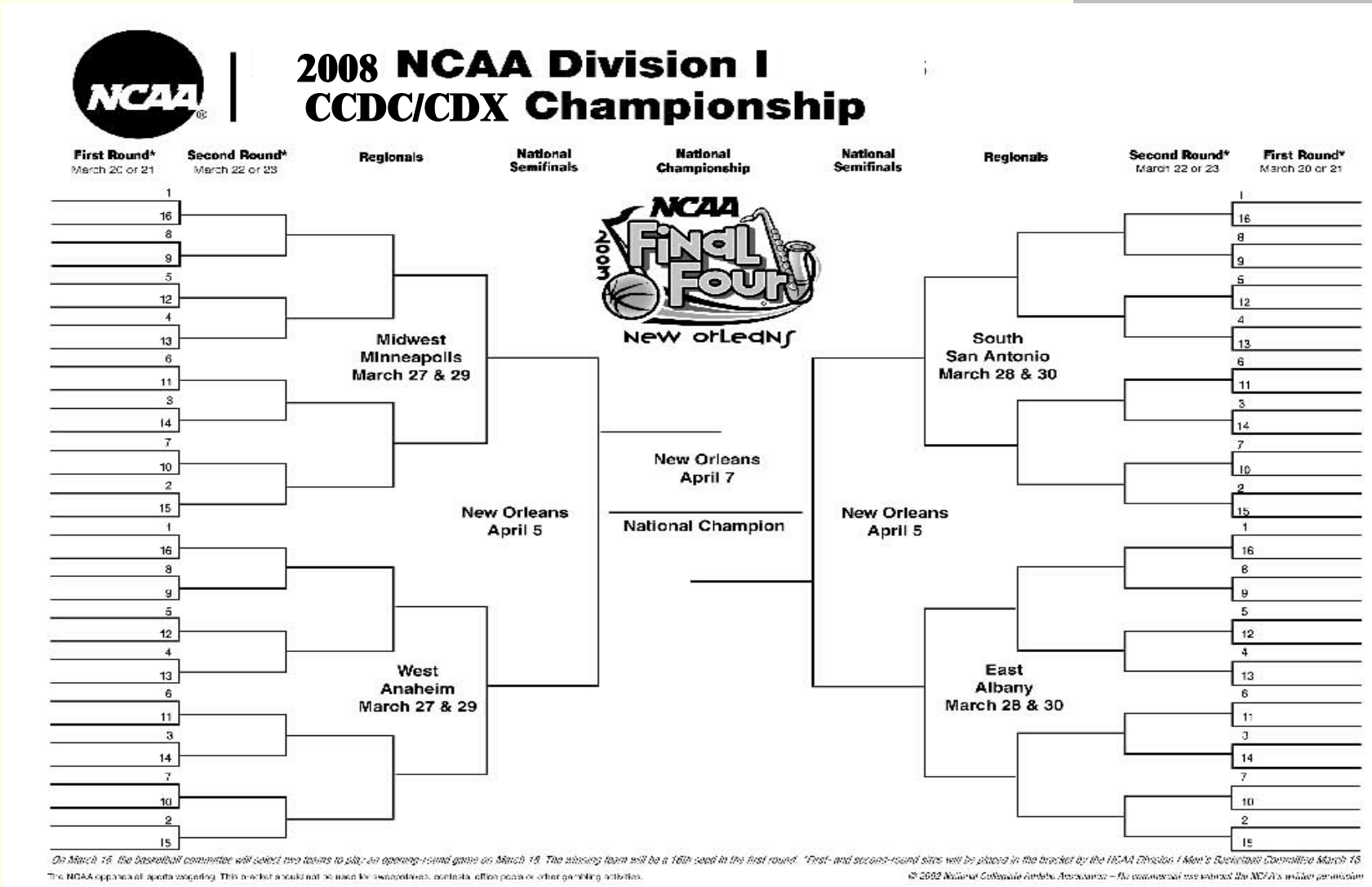
Virtualization is the key!

- VMWare
  - Workstation
  - GX Server
- Virtual PC and Virtual Server
- Reduced Costs
- More
  - Scalable
  - Recoverable
- Enhanced Post Analysis

Virtual Information Assurance Network



Future of the CDX / CCDC ?



CDX in the News

- **NBC New York Affiliate (WNBC)**, "Cyber War“
- **"Cadets train for Cyber Warfare (and other similar titles)"**, Michael Hill, AP
  - **National (7):** MSNBC CNN CNN International USA Today ABC News Yahoo News Army Times
    International (8), Regional TV Stations (6), Regional Newspapers (29)

2005 USMA Morning Update

COL R;

Boy am I tired... We are recovering from a bad first day, but I think we are in the hunt... The first day we shot ourselves in the foot...

-Ron

Ronald C. Dodge JR., Ph.D.
Lieutenant Colonel, Academy Professor
Director, Information Technology and Operations Center

Almost Bottom Line (BLUF)

- Cyberspace is the ultimate intellectual battlefield
- Enhance education and awareness through
  - Competition
  - Active learning
  - Team efforts
- Competitive cyber exercises are scalable
  - … therefore, feasible
- Learn from our lessons
  - http://www.itoc.usma.edu/cdx
  - Exploring a **National Cyber** Security **Exercise** for Universities

6th Annual IEEE Information Assurance Workshop

"The West Point Workshop"

United States Military Academy, West Point, New York

June 15TH- 17TH 2005

www.itoc.usma.edu/workshop

Duty, Honor, Country