Information Assurance Program at West Point

Daniel-Ragsdale@usma.edu   John.Hill@usma.edu
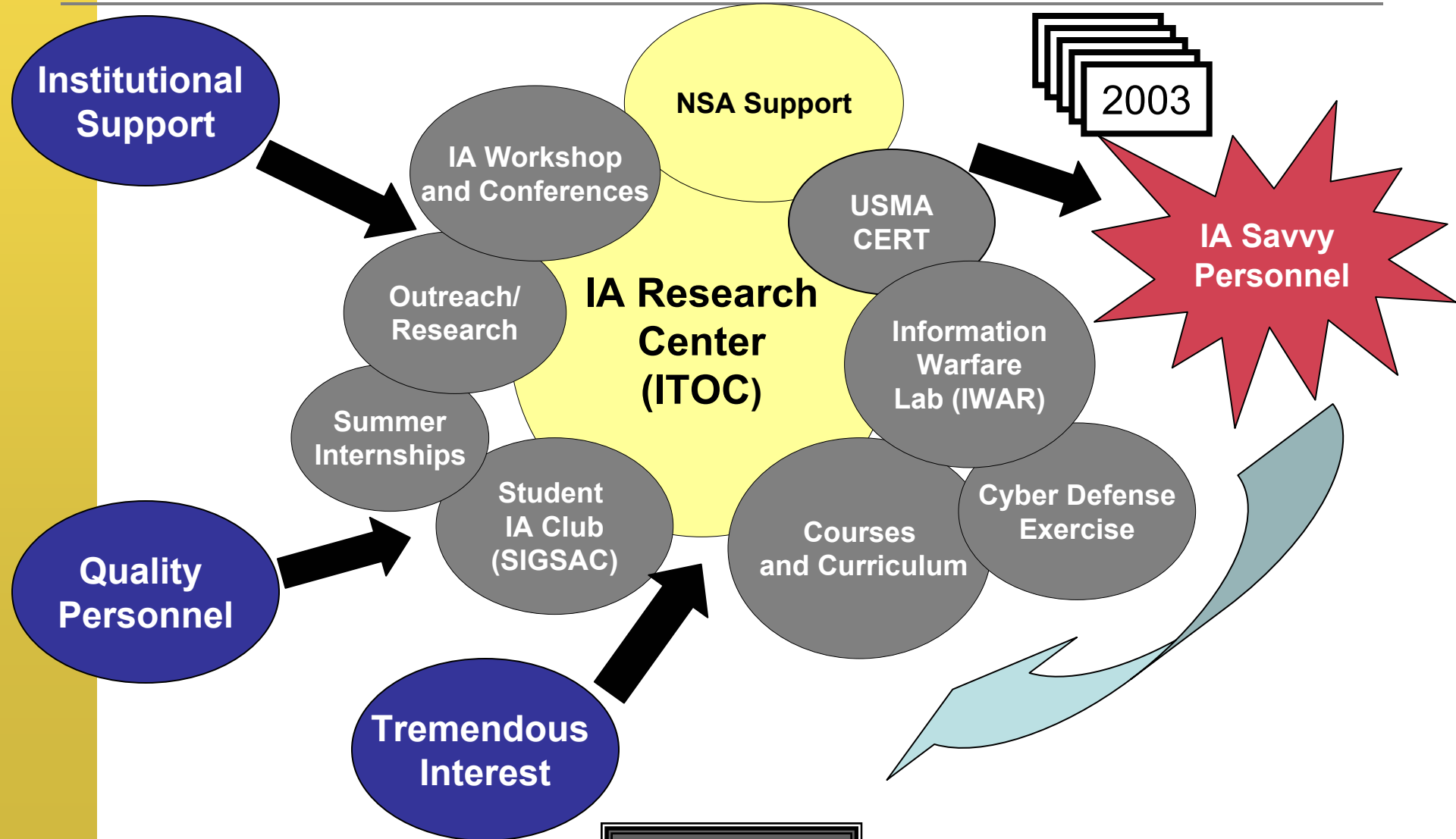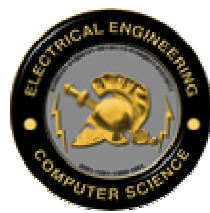**Scott.Lathrop@usma.edu   Gregory.Conti@usma.edu**
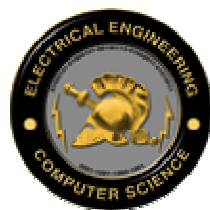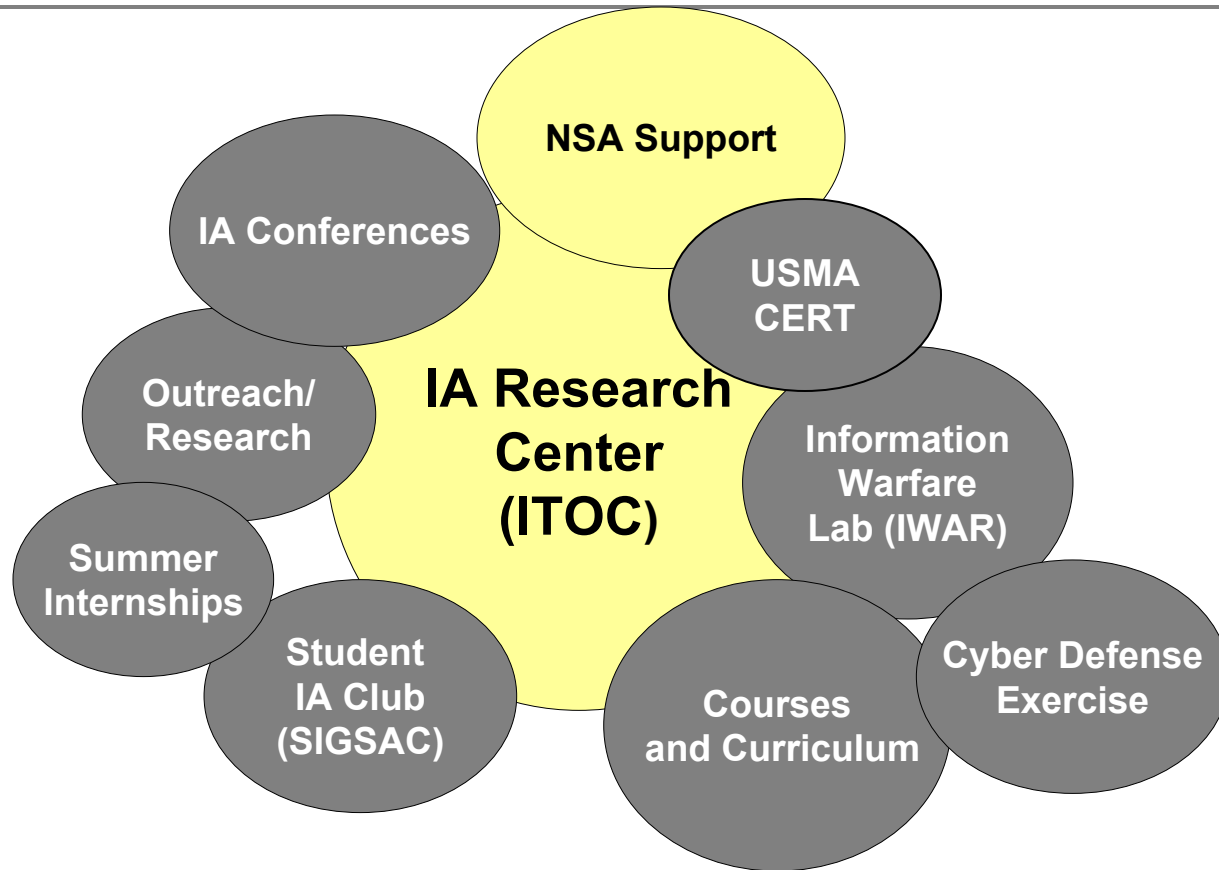
Duty, Honor Country

USMA Information Assurance Program

Institutional Support

Quality Personnel

Tremendous Interest

IA Workshop and Conferences

Outreach/ Research

Summer Internships

Student IA Club (SIGSAC)

NSA Support

IA Research Center (ITOC)

USMA CERT

Information Warfare Lab (IWAR)

Courses and Curriculum

Cyber Defense Exercise

2003

IA Savvy Personnel

USMA IA Program

NSA Support

IA Conferences

USMA CERT

Outreach/ Research

IA Research Center (ITOC)

Information Warfare Lab (IWAR)

Summer Internships

Student IA Club (SIGSAC)

Courses and Curriculum

Cyber Defense Exercise
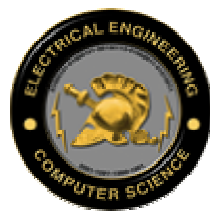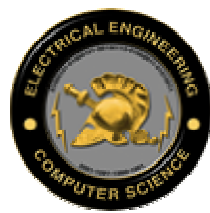
USMA IA Program Mission

- "Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah Blah …"

-*LTC Dan Ragsdale*
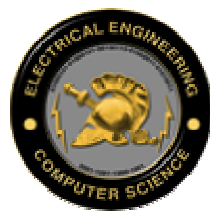*ITOC Director*

Information Assurance Courses

- Primary
  - **CS482 *Information Assurance***
  - IT460 *Policy and Strategy of Cyberwar*
  - MA489 *Cryptography*
  - LW489 *Cyberlaw*
- Supporting
  - CS484 *Computer Networks*
  - IT105 *Introduction to Information Technology*
  - IT305 *Introduction to Military Information Technology*
- Other computer science courses
  - Have IA awareness woven into them
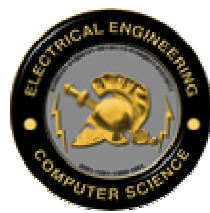
Student IA Club

- ACM SIGSAC Chapter
- Formed January 2001
- 450+ Members
  – Interdisciplinary (All Academic Departments Represented)
- Won 2001-2002 ACM Outstanding Activities Award
  – SIGSAC IWAR Lab
  – Speakers
  – Community Service
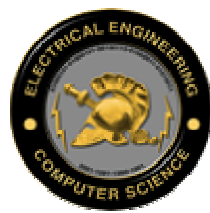- www.itoc.usma.edu/sigsac/

- NSA - Network Evaluation Intern Program
- US Secret Service, Electronic Crimes Branch – Honeypot research
- Joint C4ISR Battle Center - Enhanced C4ISR Homeland Security Operations (ECHO)
- ITOC - Information Assurance Vulnerability Alert (IAVA) Compliance Prototype
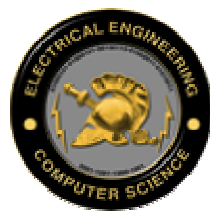- AMC-DOD - UAV multi-mission payload analysis
- Microsoft – Microsoft Intern

- US Army Information Technology Agency - Network Security Services-Pentagon

- Livermore National Laboratory - UAV Simulation

- High Performance Computing Modernization Office - Network Monitoring Initiative

- RCERT Pacific - Intrusion Detection and Analysis

- 1st IO Command(ACERT,RCERT Korea & Europe) - Intrusion Detection and Analysis

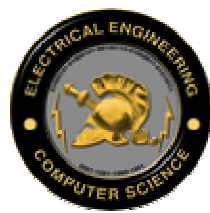- AMC-DOD - Crowd Simulation in Realistic Simulations

Guest Speaker Program

- Government

- Military

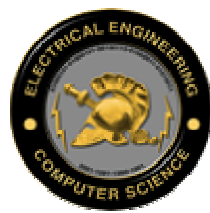- Academia

- Business

ITOC Research Topics

- Information Technology and Operations Center
  - Decision Support
    - Automated Imagery Analysis
    - Automated Terrain Analysis
  - Information Assurance
    - Network Deception (Honeynets / Network Camouflage)
    - Open Source Tool Employment
    - Intrusion Detection and Response
    - Information Assurance Simulation
    - Network and Computer Forensics
    - Wireless Security

ITOC Outreach Projects

- Information Assurance Vulnerability Alert (IAVA) Compliance Prototype – NSA, 1st IO Command

- Network Deception (Honeynets) - 1st IO Command, US Secret Service

- Information Assurance Curriculum and Training Development – NSF, 1st IO Command

- Classroom XXI – Army Training and Doctrine Command

- Military Academy Attack Defense Network (MAADNet) – Office of the Secretary of Defense, NSF

- Network Forensics and Email Recovery– US Secret Service

- Wireless Security

- T4IA – NSF

4th Annual IEEE
Information Assurance Workshop
June 18-20, 2003
West Point, New York

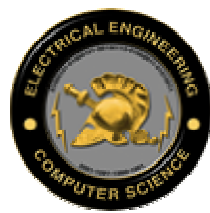Sponsored by IEEE and NSA
http://www.itoc.usma.edu/workshop/

Duty, Honor Country

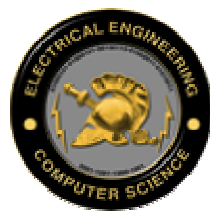# Information Warfare Analysis and Research (IWAR) Lab

- Isolated network
  - Wide variety of target machines
  - Full 18 seat classroom
  - Dedicated lab director
- Used to support courses
  - CS482 *Information Assurance* (primary user)
  - SS490 *Policy and Strategy of Cyberwar* (primary user)
  - CS484 *Networks* (projected)
  - IT105 *Intro to Information Technology* (awareness)
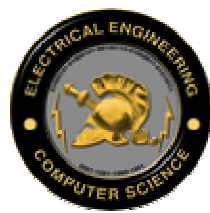 - IT305 *Intro to Military Information Technology*
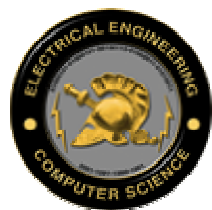
IWAR Laboratory Design Goals

- Realistic
  - Provide a "real world" signature
  - Shared Resources
  - *Soft* and *Hard* targets

- Heterogeneous
  - Operating Systems
  - Network Protocols/Equipment
  - Offensive and Defensive Tools

- Reconfigurable
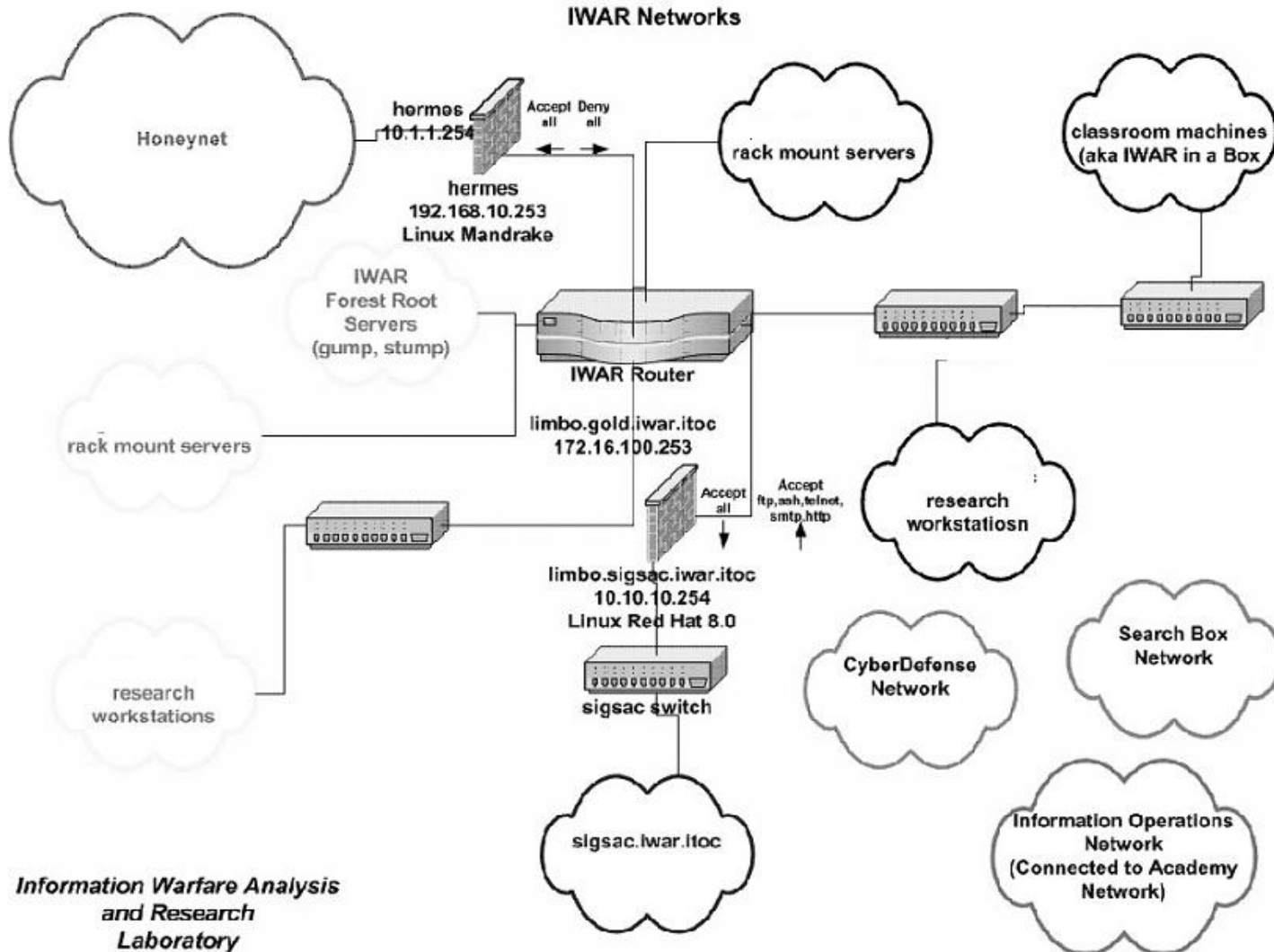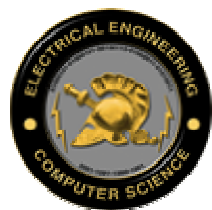 - Ghost Images
  - Removable hard drives

IWAR Tools and Capability

- Firewalls
- Malicious Active Content Exploits
- Vulnerability Scanners
- Viruses and Worms
- Cryptography and Encryption
- Trojan Horses
- Application and Protocol Wrappers
- Buffer Overflow Exploits
- Honey Pots/Honeynets
- Access Control Methods

- Protocol Exploits
- Integrity Maintenance Systems
- Network Sniffers
- Mail and Protocol Spoofers
- Distributed DoS Tools
- Intrusion Detection Systems
- Race Condition Exploits
- Password Cracking Software
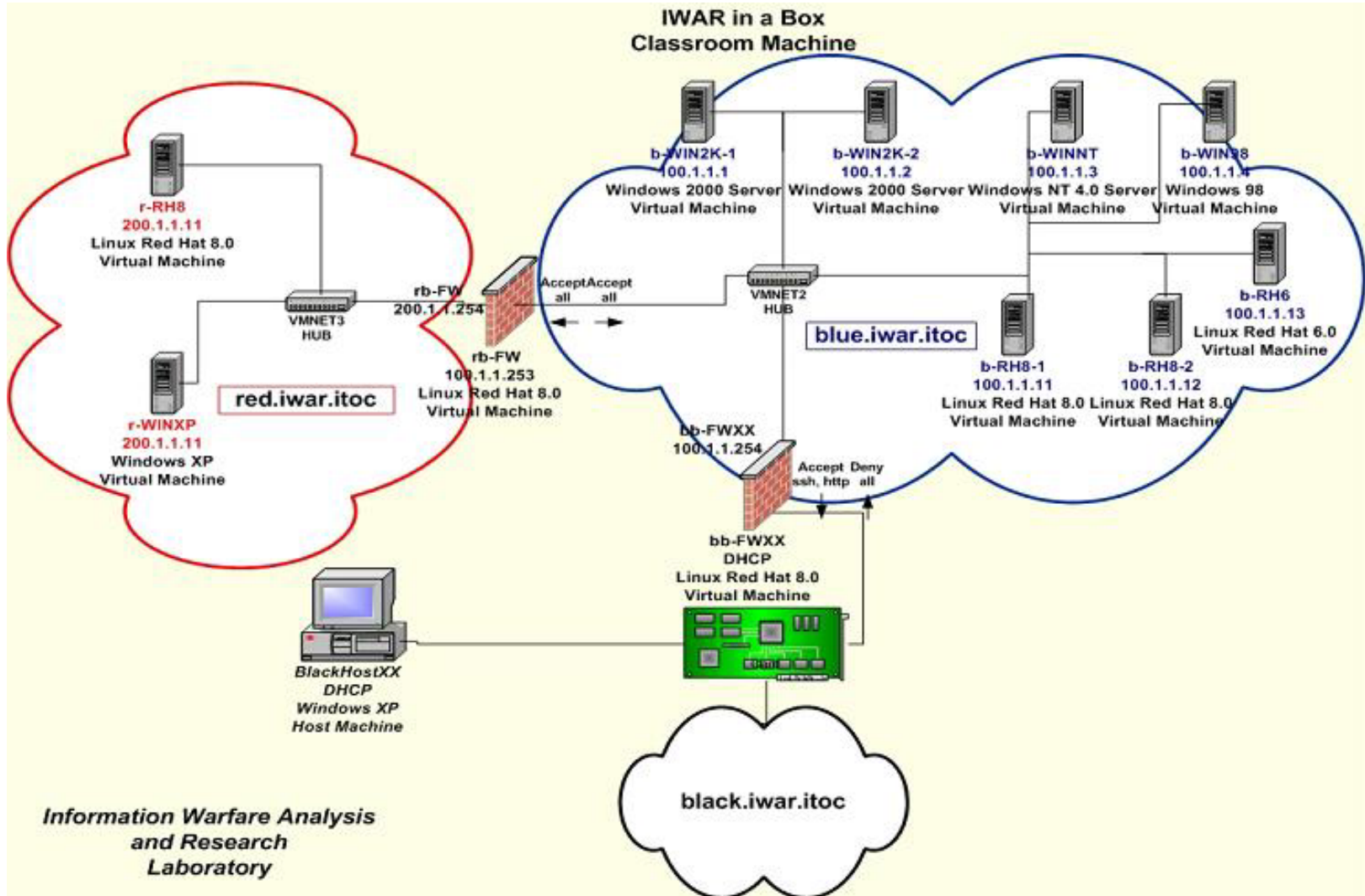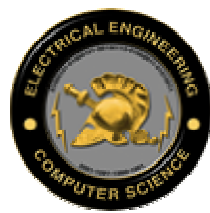- Forensics Analysis Tools
- Port Scanners

IWAR Networks

IWAR Networks

Honeynet

hermes
10.1.1.254

Accept Deny
all all

hermes
192.168.10.253
Linux Mandrake

rack mount servers

classroom machines
(aka IWAR in a Box)

IWAR
Forest Root
Servers
(gump, stump)

IWAR Router

limbo.gold.iwar.itoc
172.16.100.253

rack mount servers

Accept
all

Accept
ftp,ssh,telnet,
smtp,http

research
workstatiosn

limbo.sigsac.iwar.itoc
10.10.10.254
Linux Red Hat 8.0

research
workstations

sigsac switch

CyberDefense
Network

Search Box
Network

sigsac.iwar.itoc

Information Operations
Network
(Connected to Academy
Network)

Information Warfare Analysis
and Research
Laboratory

IWAR-in-a-Box

Information Warfare Analysis and Research Laboratory
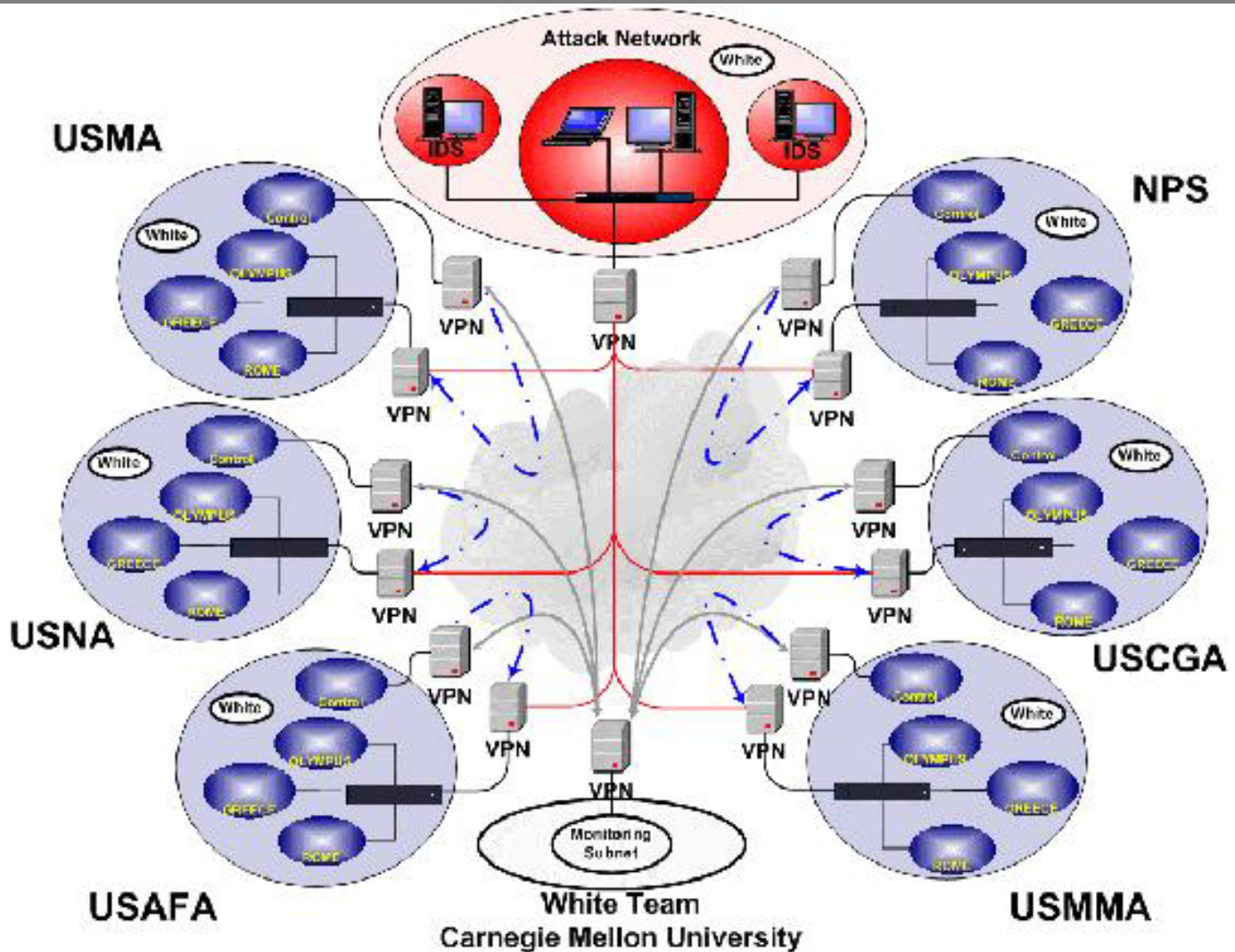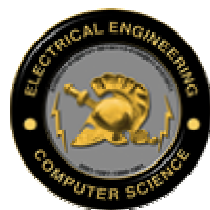
Cyber Defense Exercise

- Sponsored by the National Security Agency, Director of Information Assurance
- General Concept
  - Defense of a network against an adversarial force
  - Blue Forces
    - US Service Academies and NPS
  - Red Forces
    - National Security Agency
    - 92nd Information Warfare Aggressor Squadron
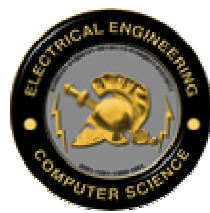   - 1st Information Operations Command
  - White Cell
    - Carnegie Mellon

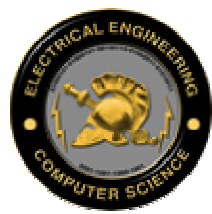# Cyber Defense Network

Cyber Defense Exercise

- **Key Educational Aspects**
  - Competitive
  - Active learning
  - Project-based
- **Developmental Areas**
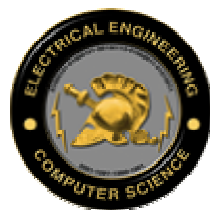 - Leadership Ability
  - Planning Ability

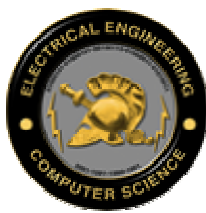## Cadets take aim at cyber foes

CDX Award Ceremony

NSA

- Full Time NSA Liaison
- IA Conference Sponsorship
- NSA Trip
- NSA Internships
- Intelligence Community Access
- CDX Support
- Sabbaticals

INFORMATION SYSTEMS SECURITY ORGANIZATION

- NSA Information Assurance Center of Excellence Program
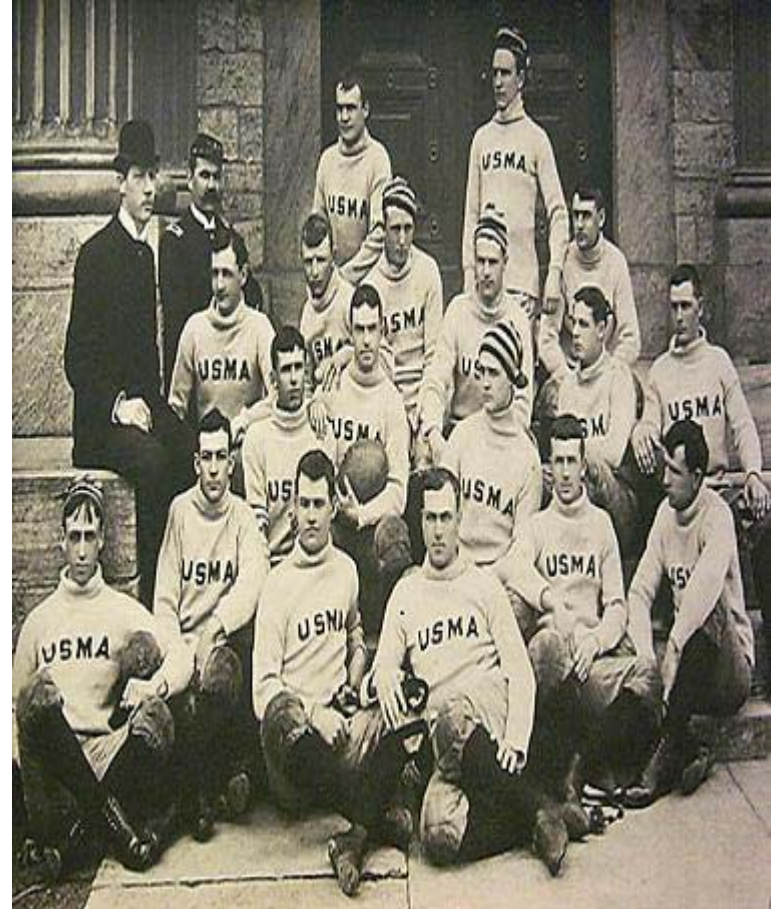
- NSA Information Assurance Director's Trophy

Preparation for War

"On the fields of friendly strife are sewn the seeds that upon other fields on other days will bear the fruits of victory…"
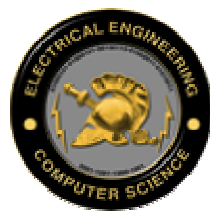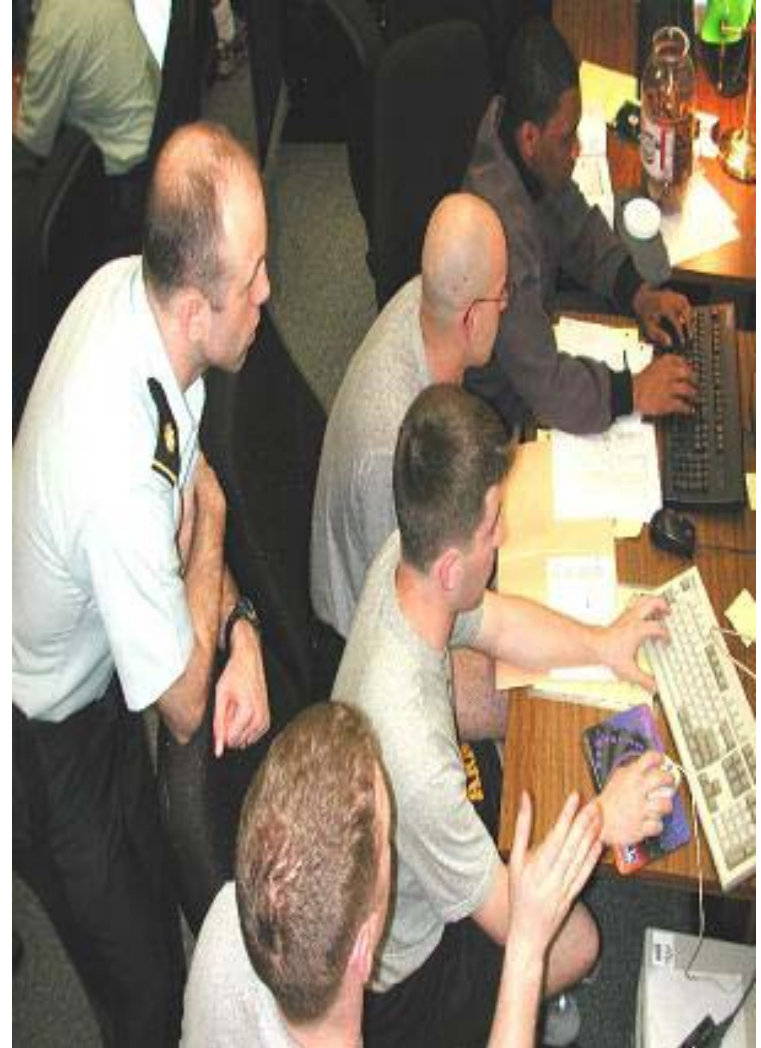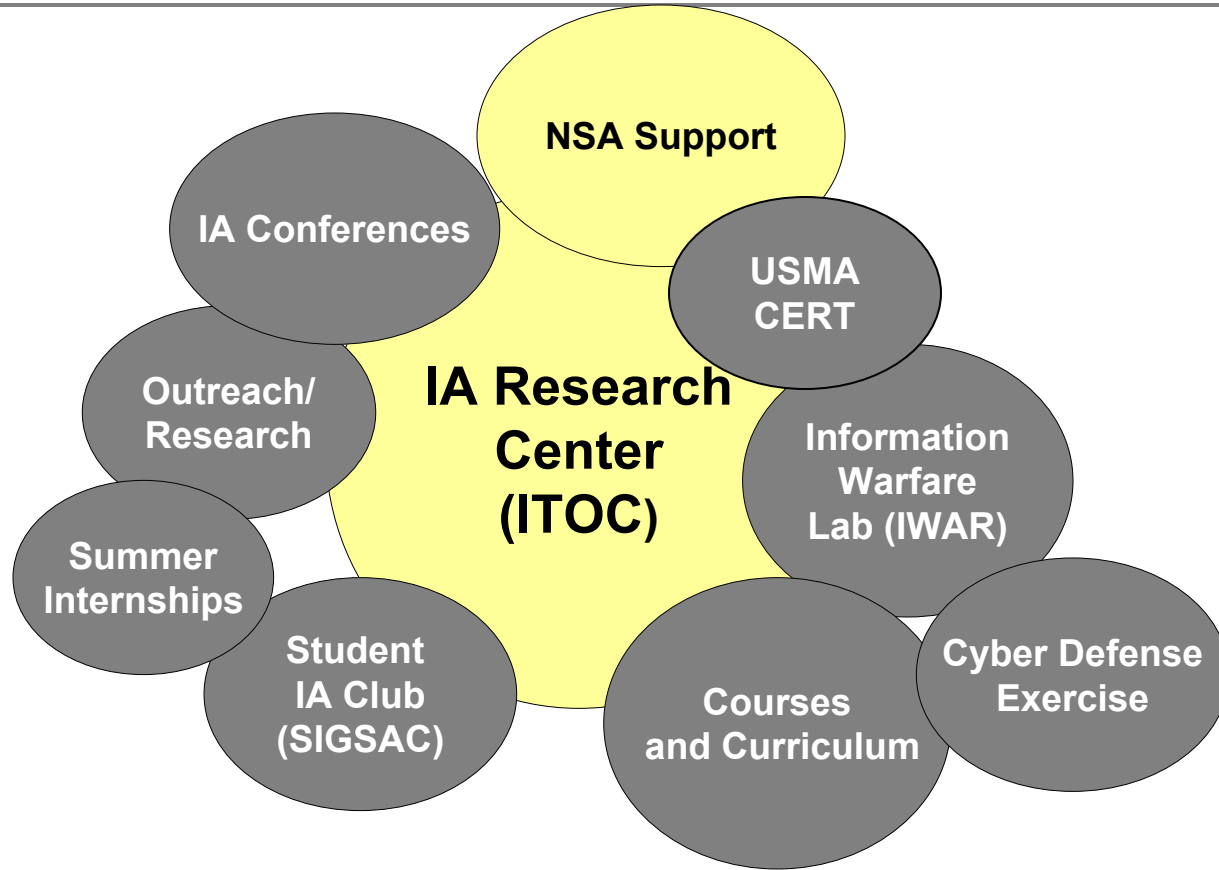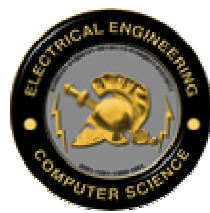
GEN Douglas MacArthur

"On the *networks* of friendly strife are sewn the seeds that upon other *networks* on other days will bear the fruits of victory…"
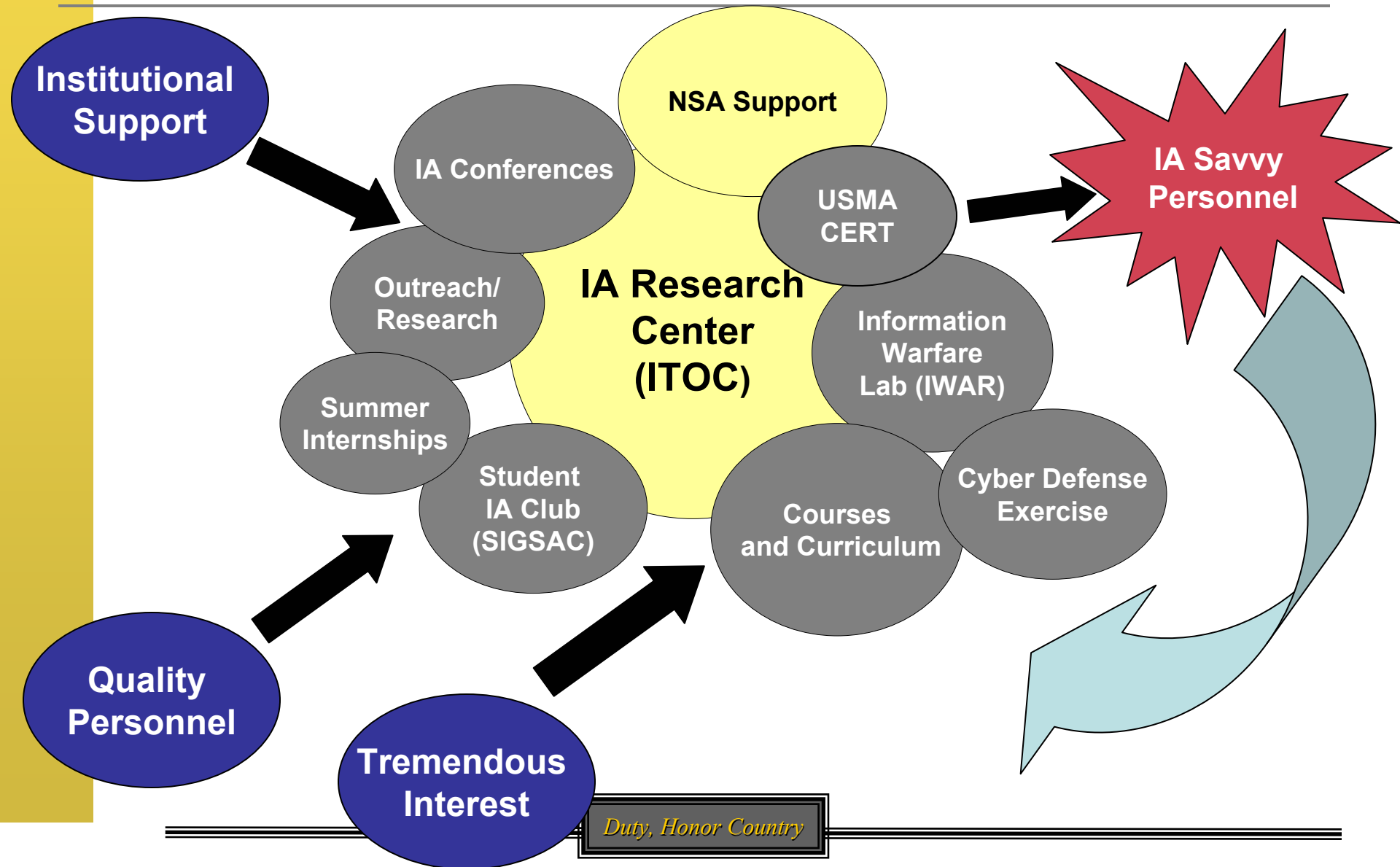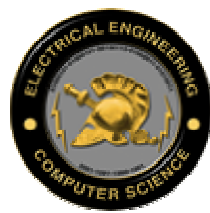
MAJ Greg Conti

USMA IA Program

NSA Support

IA Conferences

USMA CERT

Outreach/ Research

IA Research Center (ITOC)

Information Warfare Lab (IWAR)

Summer Internships

Student IA Club (SIGSAC)

Courses and Curriculum

Cyber Defense Exercise

USMA IA Program

Questions?

- … and a reminder!

**4th Annual IEEE
Information Assurance Workshop
June 18-20, 2003
West Point, New York**

Sponsored by IEEE and NSA
http://www.itoc.usma.edu/workshop/