The Fight in the Cyber War Today

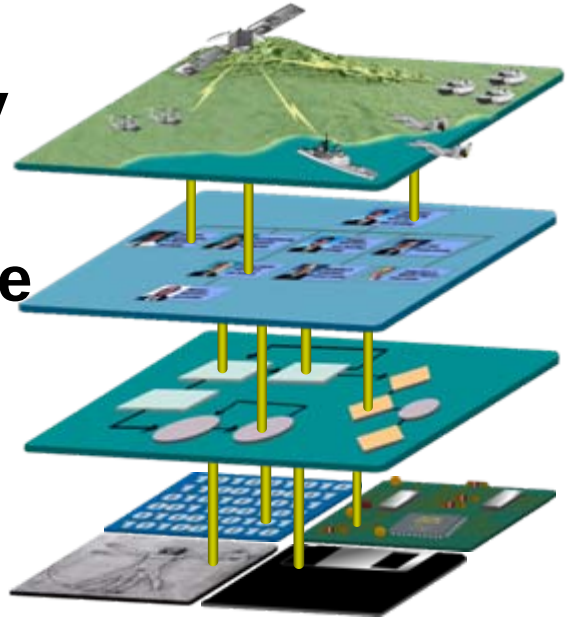
Col Robert J. Skinner
688 Information Operations Wing
Commander

UNCLASSIFIED

"Perfection is not attainable, but if we chase perfection we can catch excellence"
(Vince Lombardi)

Senior Leader Views

- **Senior Leader View**
  - **“Information technology enables almost everything the U.S. military does” Deputy Secretary of Defense William Lynn III**
  - **“Cyberspace pervades everything we do, in every domain, and extends from your workspace to the battlespace.” Secretary of the Air Force Michael B. Donley**
  - **Cyber Domain Essential to Dominance**
  - **Definition of “Integration and Sustainability”**



Environment

Vulnerability

Risk

Network Traffic

- 90 Trillion Emails Sent in 2009
- 81% Spam – 200 Billion Spam Emails/Day
- 80% of HTTP Bandwidth is App-Based not Browser-Based

Vulnerability

Risk

DoD Global Information Grid

- 7,000,000 DoD Computers Worldwide
- 1,000s of Warfighting and Support Applications

Malware

- 10 Million Pieces of New Malware Cataloged First Half of 2010
- Daily Production of Malware Increased from 100 in 2008, 500 in 2009 to 3,300 in 2010

Threat

Future

Battle Damage Assessment

- Average Cost of Network Intrusions Per Year $3 Million
- Pentagon Spent $100 Million in the Last 6 Months Responding to and Repairing Cyber Attack Damage

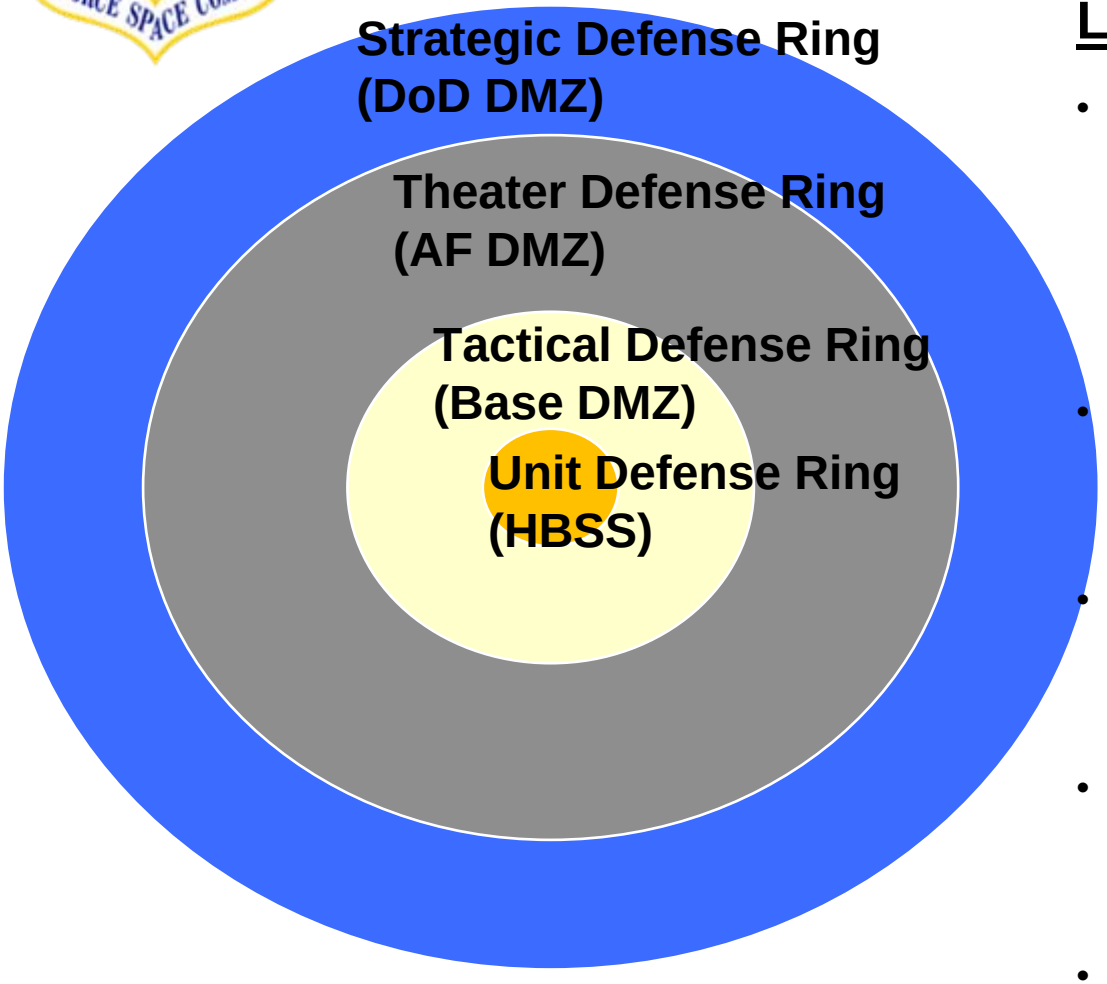
Threat

Future

People*Threat*People*Threat*People*Threat*People*Threat*People*Threat*People*Threat*

People*Threat*People*Threat*People*Threat*People*Threat*People*Threat*People*Threat*

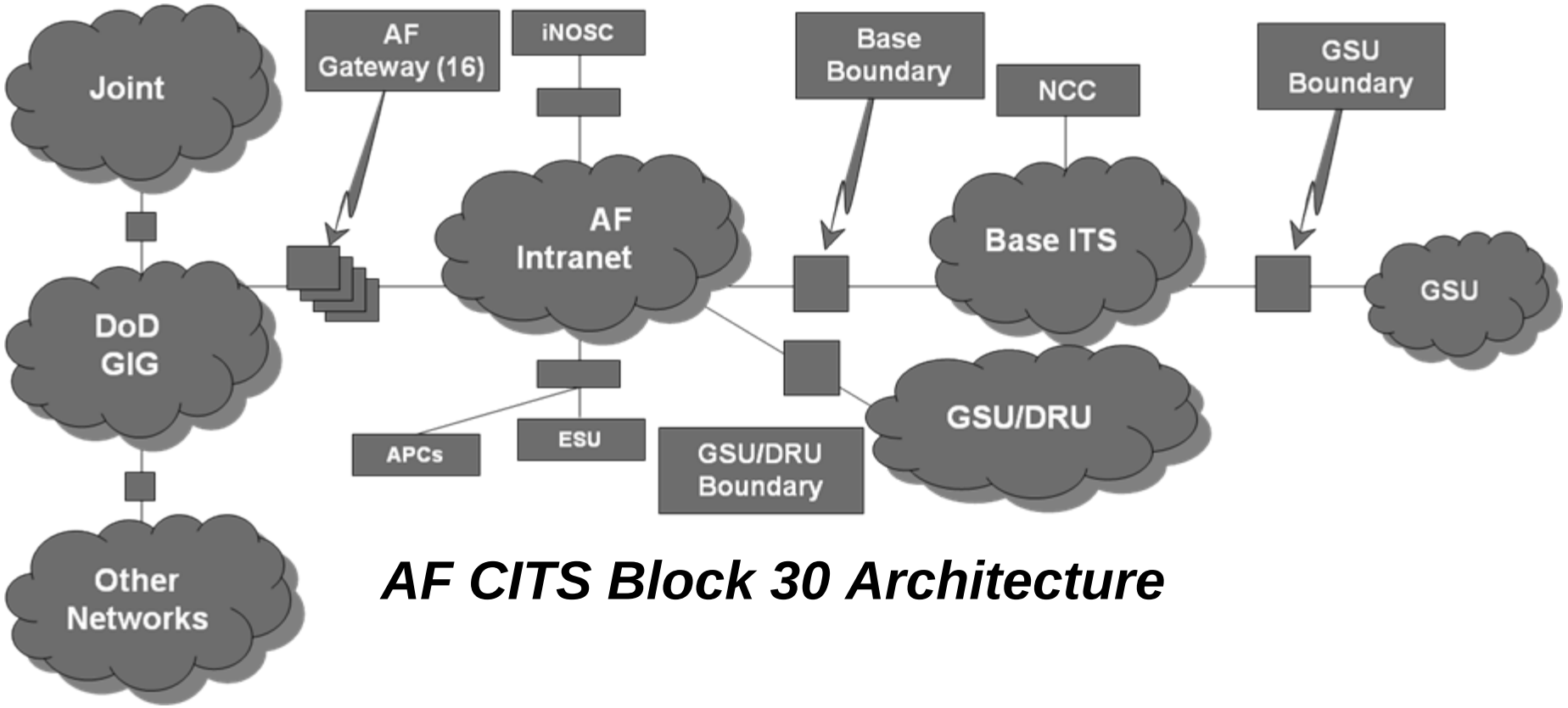
Current Cyberspace Layered Defense Thinking



Layers of Defense

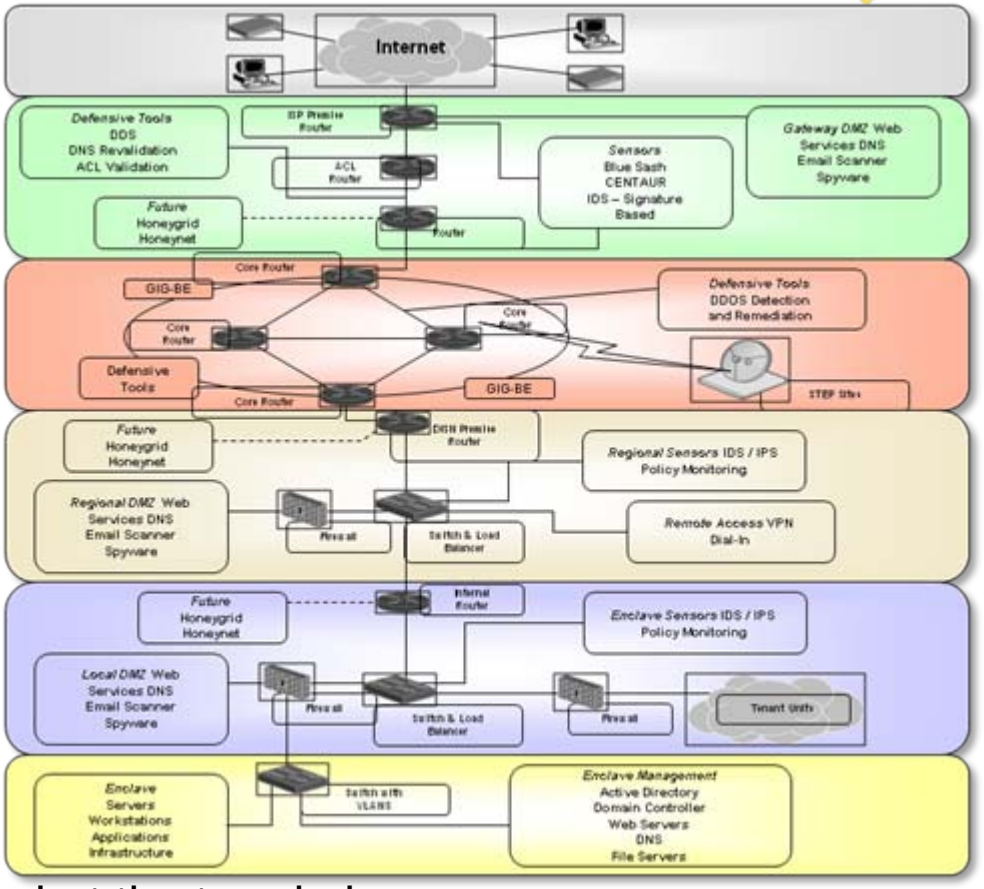
- **Unlike "traditional" air defenses, must protect against outside & inside threats**
  - **Attacks can be initiated from outside or inside the network**
- **Strategic Defense Ring**
  - **DoD DMZ under DISA C2 to protect GiG**
- **Theater Defense Ring**
  - **AF DMZ under AF C2 to protect AFNet**
- **Tactical Defense Ring**
  - **Base DMZ under AF C2 to protect individual base**
- **Unit Defense Ring**
  - **Individual system protection (ie HBSS) under AF C2 to protect against insider threat**

What Does This Look Like in our AF?



AF CITS Block 30 Architecture

Defense in Depth akin to "Political Maps"



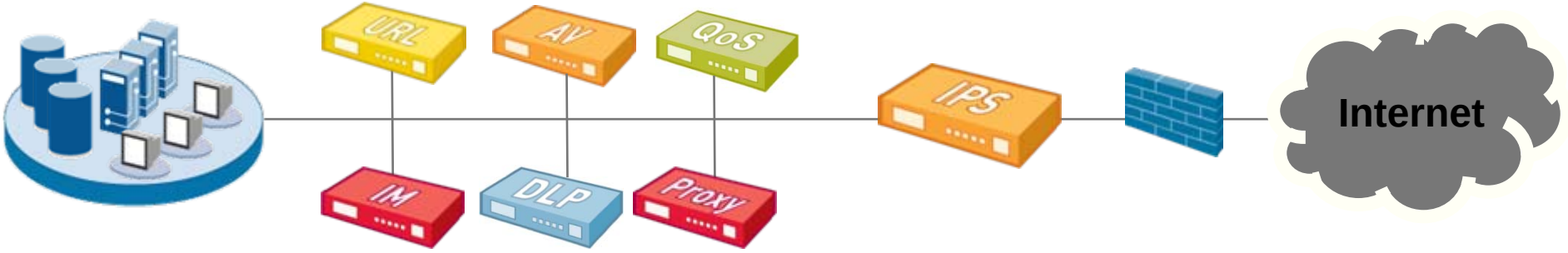
Political Maps:

- Gives general 2 dimensional orientation
- Contains no topographical info-can't tell what the terrain is

Defense in Depth:

- Addresses the path of data in & out of the net (network layers 2,3 & 4)
- Tells us nothing about what happens after data arrives (network layers 5 & above)

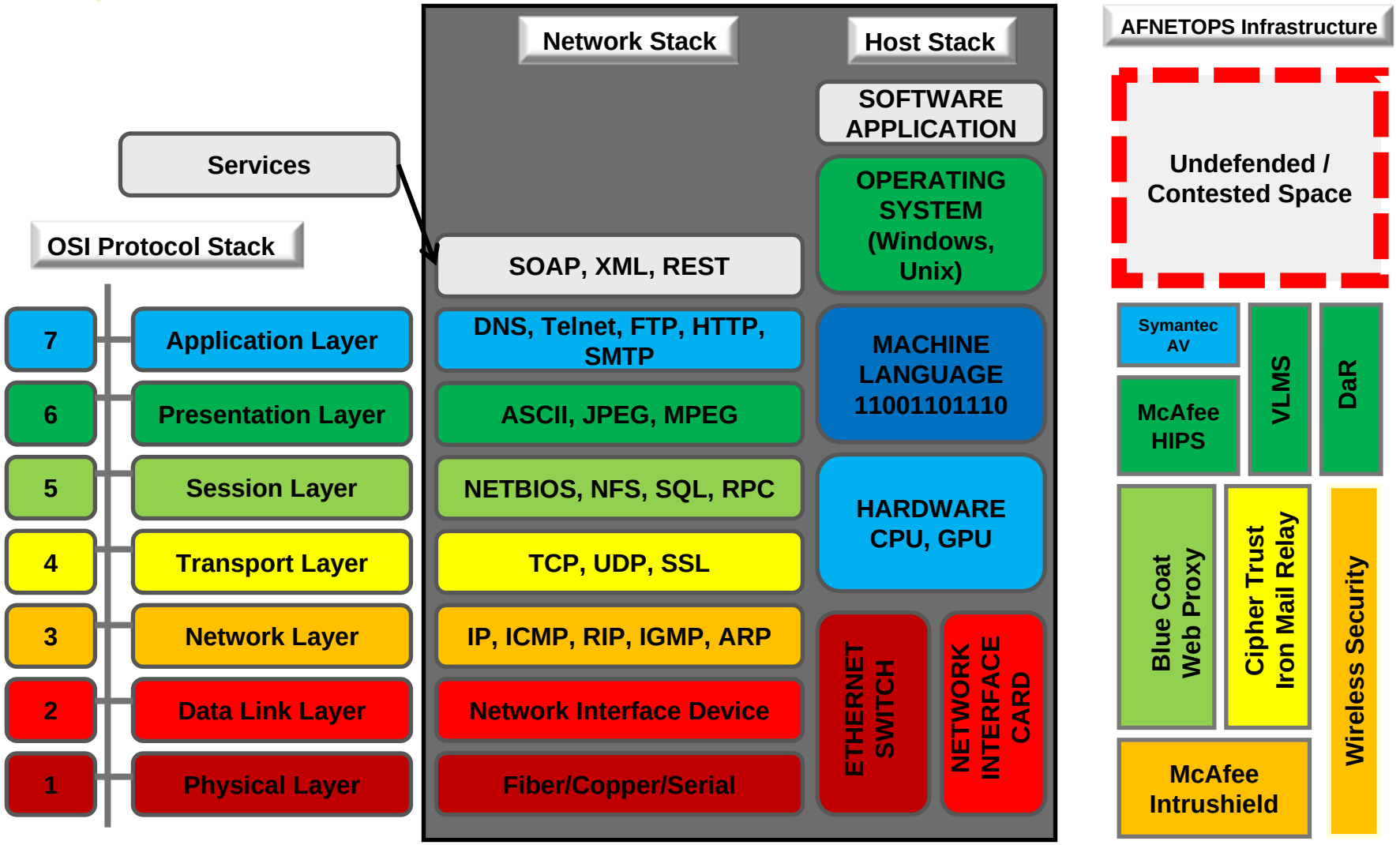
The Fix?
Sprawl Is Not The Answer…



- State of current practice is to spread out the load:
  - Adding proxies (doesn't solve the problem)
  - Firewall "helpers" (limited view of traffic)
- All this structure is costly to buy, maintain, and operate

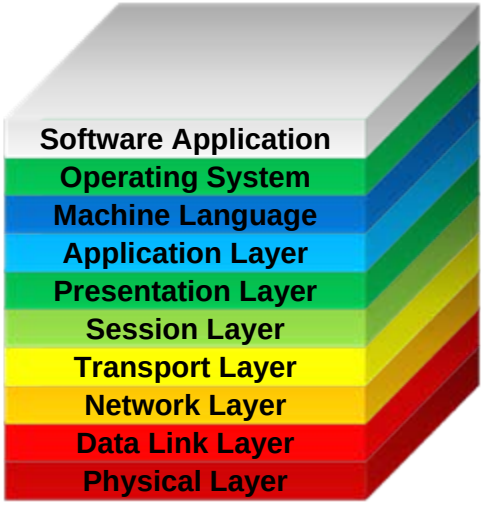
Point Solutions…add complexity and will not scale

Where are we Putting our Defenses Today?



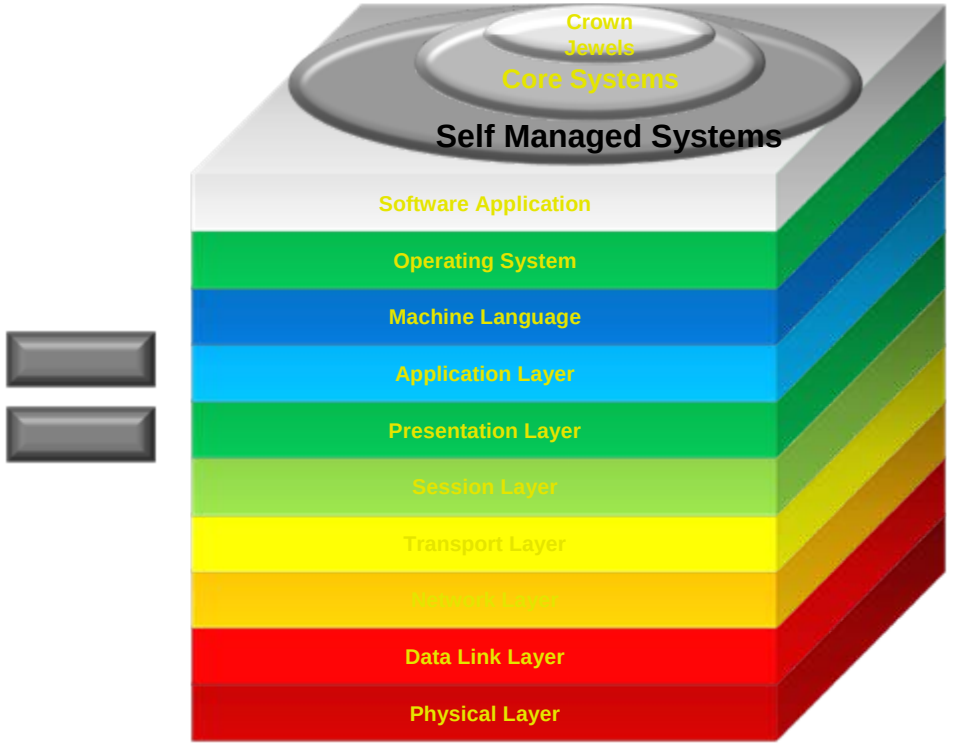
How do we Implement?

- **Firewalls are effective at Layers 2, 3 & 4 - need to address the higher layers**
- **Need to implement *more* real-time code/packet inspection technology to address the entire cyber terrain:**
  - **Application Identification: *Identify the application***
    - ***Application Protocol Detection/Decryption/Decoding***
    - ***Heuristics & Signatures***
  - **User Identification: *Identify the user***
    - ***Fingerprinting***
    - ***Detect Malware Beacons***
  - **Content Identification: *Scan the content***
    - ***Identify and block data ex-filtration***
    - ***Identify and block malware***



Need to Apply Protection Equally to External and Internal Threats

What should replace Defense in Depth?
A New Cyber 'Terrain' Map

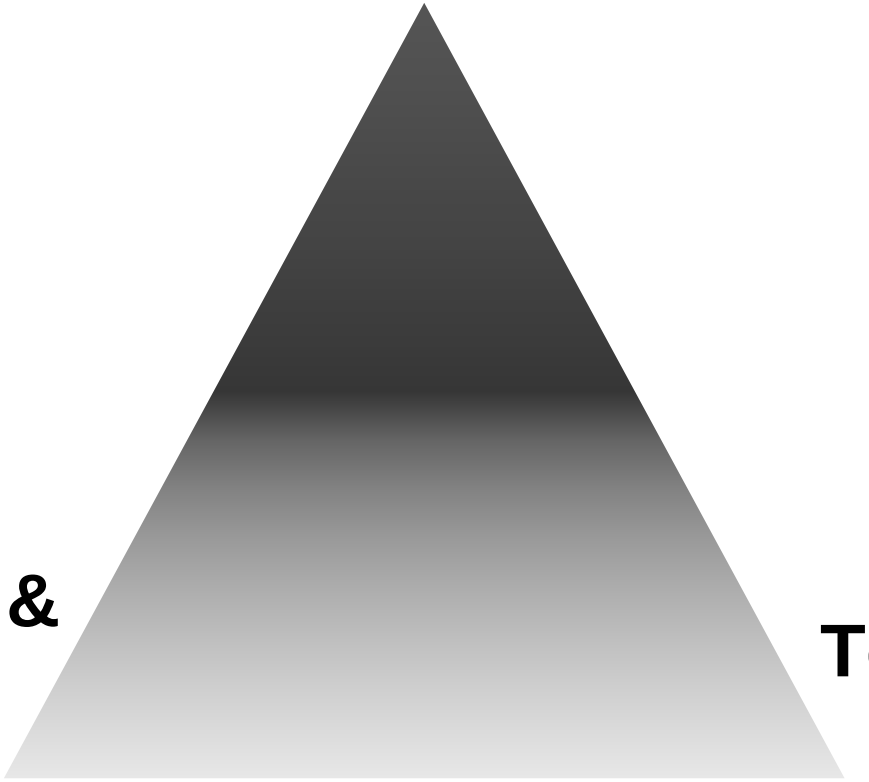


Cyber 'Terrain' Map:

- **Addresses both the path of data in and out of the net (network layers 2, 3, & 4) as well as the what happens after data arrives (network layers 5 & above)**

Triangle of Sustainment

Talent Management



Organization & Processes

Technology

Organization & Processes

- 24th Air Force & Associated Wings
- COCOM, MAJCOM & Base Presence
- Identified our Assets (Map the Net)
- 40 Assessments and 80 Tests

Talent Management

- **73 Air Force Specialty Codes**
- **Cyber Warrior Training**
- **Supported 15 Major Exercises**
- **Total Force**

Technology

- **Deployed Information Operations Platform**
- **Delivered 129 Capabilities**
- **Remote Assessments**
- **Cyber Modeling and Simulation**

Protecting and Advancing the Cyber Domain

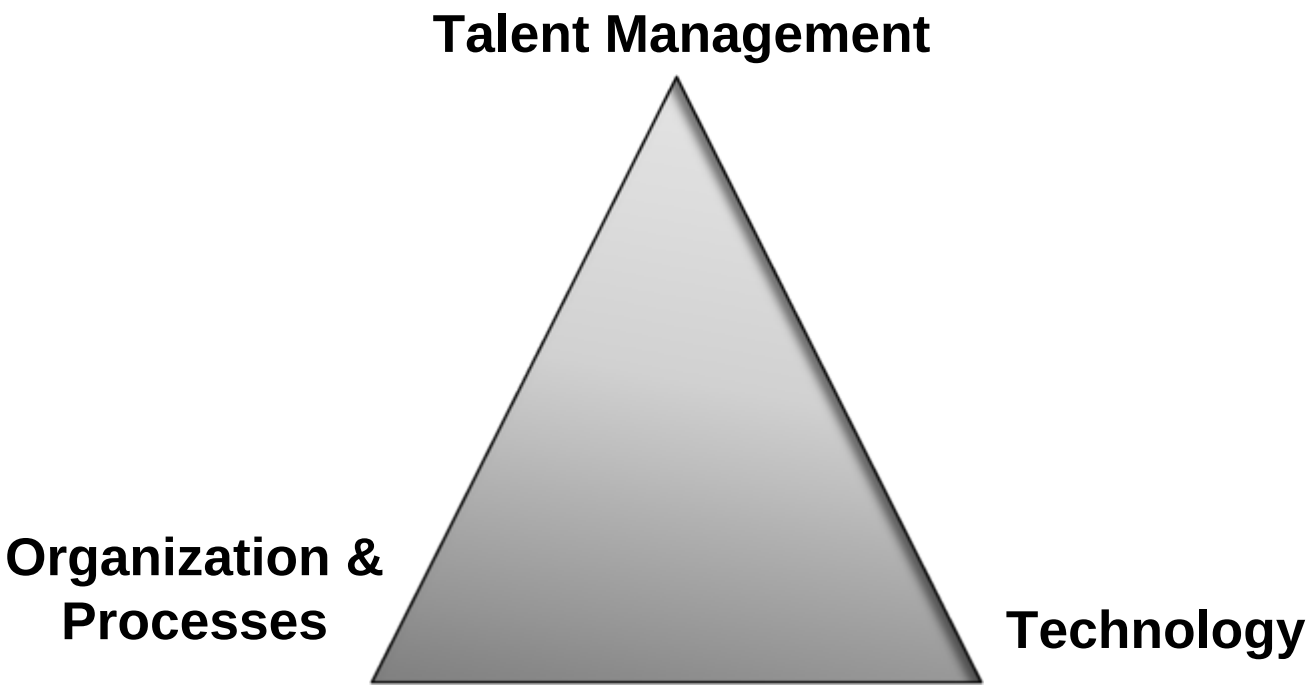
688 IOW Built for the Fight

- Cyber Focused Exercises
- Partnership with Industry
- Industrial Control System Host Based Security System Tactics
- Real-Time Net-A/Net-D Capabilities
- Emissions Security
- Mission Qualification Training
- Hunter Team Concept

2010 Air Force Outstanding Unit Award Recipient

Summary

- Cyber Domain Critical to the War-Fighting Effort
- Importance of Cyber Integration & Sustainment
- 688 IOW Armed and Ready



Questions

BACKUP

Protecting and Advancing the Cyber Domain

Integration

Assessments

Innovation

Training

Operational Engineering

Test/Evaluation

Tactics

Real-Time Ops Support

Integration

- National Capital Region
- Cyber Focused Exercises
- Total Force

Protecting and Advancing the Cyber Domain

Integration

Assessments

Innovation

Training

Operational Engineering

Test/Evaluation

Tactics

Real-Time Ops Support

Innovation

- Cooperative Research and Development Agreements
- Partnership with Industry
- National and Air Force Laboratories

2010 Air Force Outstanding Unit Award Recipient

Protecting and Advancing the Cyber Domain

Integration

Assessments

Innovation

Training

Operational Engineering

Test/Evaluation

Tactics

Real-Time Ops Support

Operational Engineering

- Continued Progress on ICS
- Map the Net
- Radio Frequency Interference Mitigation

Protecting and Advancing the Cyber Domain

Integration

Assessments

Innovation

Training

Operational Engineering

Tactics

Test/Evaluation

Real-Time Ops Support

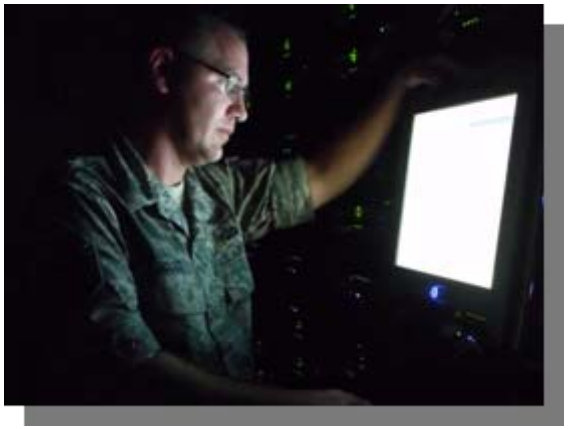
Tactics

- Establish New Pools of Expertise
- Integrate CNO throughout AFTTP
- Publish AFTTP 3-1.NWO

Protecting and Advancing the Cyber Domain

Real-Time Ops Support

- Real-Time Net-A/Net-D Capabilities
- Information Operations Platform
- ACCM HBSS Module



Protecting and Advancing the Cyber Domain

Integration

Assessments

Innovation

Training

Operational Engineering

Test/Evaluation

Tactics

Real-Time Ops Support

Test and Evaluation

- Operationally Test AF Cyber Capabilities
- Build Relationship with External Partners
- Emissions Security

688th Information Operations Wing

Integration

Assessments

Innovation

Training

Operational Engineering

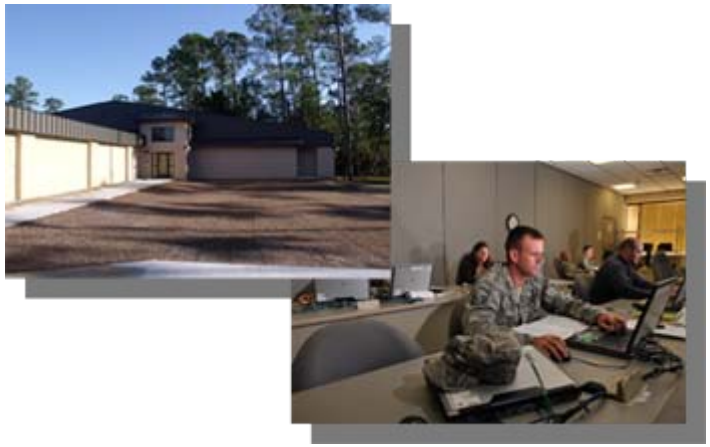
Test/Evaluation

Tactics

Real-Time Ops Support

Training

- Expand MQT Course Builds
- Build Weapons Instructor Prep Course
- Collaboration with AFIT and AETC on Life-Cycle Training



2010 Air Force Outstanding Unit Award Recipient

688th Information Operations Wing

Assessments

- Partnering
- System Vulnerability Missions
- Hunter Team Concept

For Internal Threats: Anti-Exfiltration

Internet

DoD GIG

AF GIG

Base Network

Stop Exfil of:

- C2 from implants
- User Data
- Operational Data

Real-Time Code Inspection

Application Security

Anti-Virus

HIPS

Web Proxy

Mail Relay

IDS/ IPS

Fire-Walls

SOFTWARE APPLICATION

OPERATING SYSTEM (Windows, Unix)

MACHINE LANGUAGE 11001101110

HARDWARE CPU, GPU

Ethernet Switch

Network Interface Card

For External Threats: IPS at All Layers

Internet

DoD GIG

AF GIG

Base Network

IPS at all layers in the network "Topography"

Real-Time Code Inspection

Application Security

Anti-Virus

HIPS

Web Proxy

Mail Relay

IDS/ IPS

Fire-Walls

SOFTWARE APPLICATION

OPERATING SYSTEM (Windows, Unix)

MACHINE LANGUAGE 11001101110

HARDWARE CPU, GPU

Ethernet Switch

Network Interface Card