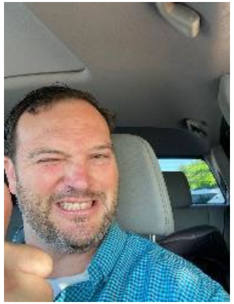
# The Improvement of U.S. Air Force Cyber Defense

Tony Franks
Professor of Cyberwarfare Studies
AF Cyber College

# Who am I?

- Legacy pilot: Active Duty, AF Reserves, Airlines
- AF Cyber College, 5 years
  - 4 years, military
  - Last year, civilian professor
  - Teaching MDTs, CPTs, cyber fundamentals to non-cyber career fields
- Converted over to 17D, Cyberspace Operations
  - AFSOC/A6
  - Stood up MDTs and Cyber Defense Correlation Cell
- Currently AF Reserve C-130 Vice Wing Commander
- Future: Air University's Blue Horizons Master's Program



# Rules of Engagement

- Air Force Cyber College presentations are protected by Academic Freedom.

- Presentation is speaker's opinion, not of Air University, Air Force, or DoD.

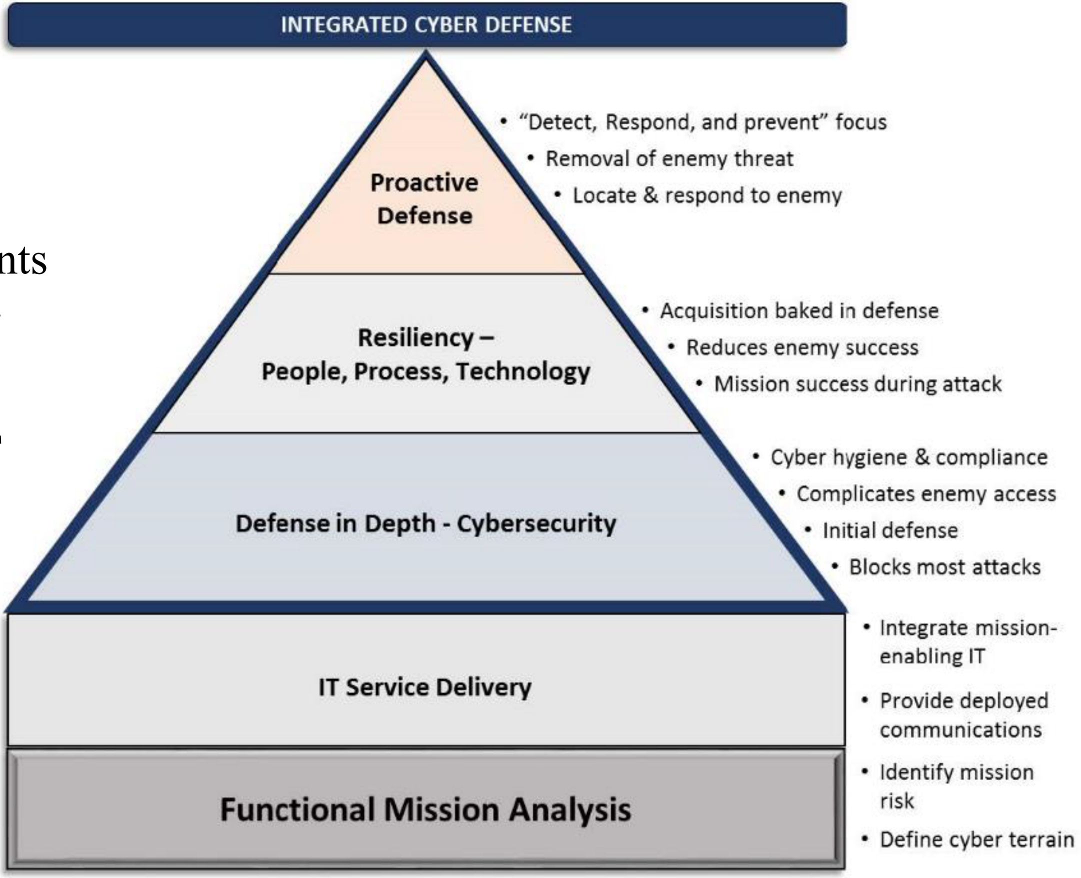
- Any comments made in this educational forum are safeguarded through non-attribution. A speaker's identity may not be associated with his/her comments without the speaker's express permission.

- For Q n A: attack the argument not the person.

# Where we are at

- 2016: Cyber Squadron Initiative
  - Mission Defense Team Creation
- 2016: NDAA 1647
  - CROWS, AFOTEC, CPT assessments
- 2018: ACC takes over AF Cyber
- 2018: Enterprise IT as a Service
- 2019: 16 AF combines 24/25 AF
- 2022: 84+ MDTs
- 2023: 19 MDTs funded (kinda)
- 2024: who knows

**What happened?**



INTEGRATED CYBER DEFENSE

**Proactive Defense**

- "Detect, Respond, and prevent" focus
- Removal of enemy threat
- Locate & respond to enemy

**Resiliency – People, Process, Technology**

- Acquisition baked in defense
- Reduces enemy success
- Mission success during attack

**Defense in Depth - Cybersecurity**

- Cyber hygiene & compliance
- Complicates enemy access
- Initial defense
- Blocks most attacks

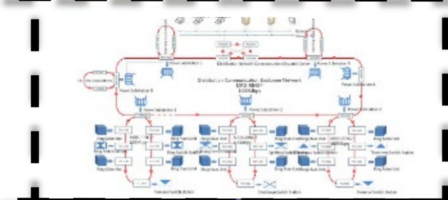
**IT Service Delivery**

- Integrate mission-enabling IT
- Provide deployed communications

**Functional Mission Analysis**

- Identify mission risk
- Define cyber terrain

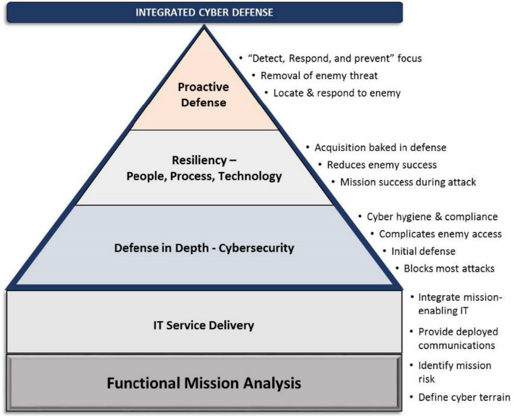
# Cyber Framework

| | Traditional Info Technology | Operational Technology | Platforms |
|---|---|---|---|
| Mission Level | | | |
| System Level | |  | |
| Component  Level | | | |

*Historically have been:* *Comm Squadron* *Civil Engineer Squadron* *Maintenance Squadron*

# What happened?

- Active Defense
  - We gave it to the wing commanders to own
    - No formal education
    - Not aware: wing has an MDT or what they do
  - Mission Defense Teams
    - Put them in MSG and Comm Squadrons initially
      - Additional duties, trouble tickets, no operational education
    - No expectation or timeline to IOC or FOC
    - No Formal Training Unit for an operational team
      - Communicators are normally Maintainers of the Network
      - Any operator takes 2 years to make
    - Not funded or billeted
    - No return on investment across the teams
      - Couple of slivers of hope, 10% ROI best case



INTEGRATED CYBER DEFENSE

Proactive Defense
- "Detect, Respond, and prevent" focus
- Removal of enemy threat
- Locate & respond to enemy

Resiliency – People, Process, Technology
- Acquisition baked in defense
- Reduces enemy success
- Mission success during attack

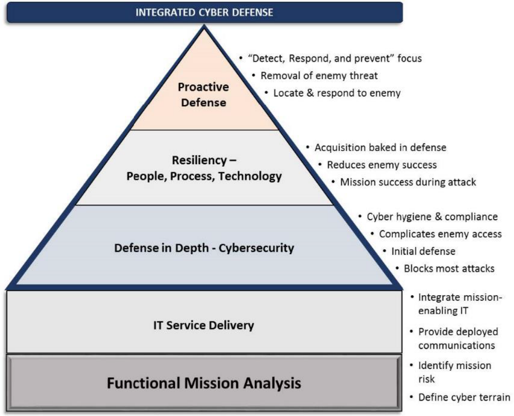
Defense in Depth - Cybersecurity
- Cyber hygiene & compliance
- Complicates enemy access
- Initial defense
- Blocks most attacks

IT Service Delivery
- Integrate mission-enabling IT
- Provide deployed communications

Functional Mission Analysis
- Identify mission risk
- Define cyber terrain

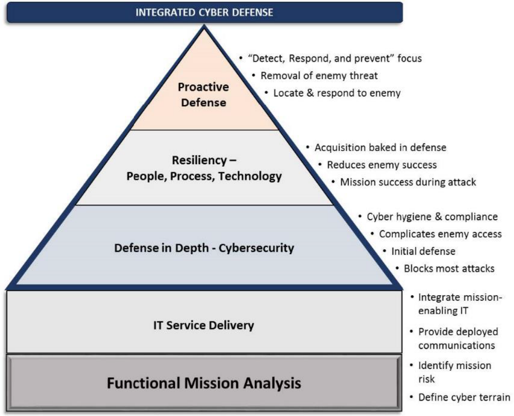
# What can we do?

- Active Defense
  - Secret sauce for the MDT:
    - Leadership buy-in
    - Wing mission integration: Ops, MX, Intel, MDT
  - COA 1: Give authority back to ACC
    - Hold teams accountable: 2 years to become FOC and show ROI
  - COA 2: Educate, Integrate, Operate
    - Educate wing commanders, not the job of the MDT
    - Educate MDTs with AF missions (FTU) and wing missions (MQT)
    - Integrate MDTs with wing exercises and deployments
    - Integrate PMO/SPO authorities with their weapon system MDTs
    - Operationalize MDTs
      - Risk assessments, prioritization, implementation, coordination


INTEGRATED CYBER DEFENSE
Proactive Defense
• "Detect, Respond, and prevent" focus
• Removal of enemy threat
• Locate & respond to enemy
Resiliency – People, Process, Technology
• Acquisition baked in defense
• Reduces enemy success
• Mission success during attack
Defense in Depth - Cybersecurity
• Cyber hygiene & compliance
• Complicates enemy access
• Initial defense
• Blocks most attacks
IT Service Delivery
• Integrate mission-enabling IT
• Provide deployed communications
Functional Mission Analysis
• Identify mission risk
• Define cyber terrain

# What happened?

- Resiliency
  - Misunderstanding of mission and risk
    - Risk = Threat acting upon Vulnerability
      - Includes consequence and likelihood
    - Risk assessment must involve entire system of systems
      - Server vs. HVAC upgrade
    - Vulnerabilities aren’t always acted upon
      - Intel not included in decision-making/prioritization
  - Never delegated PMO/SPO authorities
    - CSAF Action Order B: Bureaucracy



INTEGRATED CYBER DEFENSE

Proactive Defense

- “Detect, Respond, and prevent” focus
- Removal of enemy threat
- Locate & respond to enemy

Resiliency – People, Process, Technology

- Acquisition baked in defense
- Reduces enemy success
- Mission success during attack

Defense in Depth - Cybersecurity

- Cyber hygiene & compliance
- Complicates enemy access
- Initial defense
- Blocks most attacks

IT Service Delivery

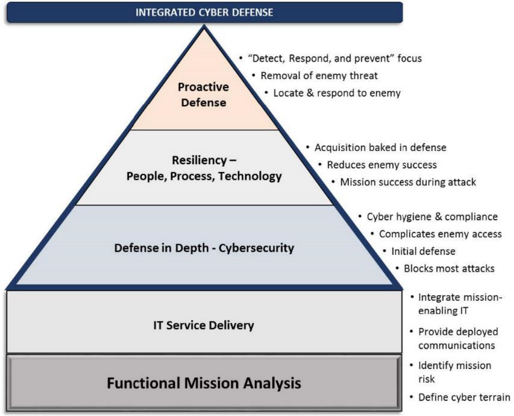
- Integrate mission-enabling IT
- Provide deployed communications

Functional Mission Analysis

- Identify mission risk
- Define cyber terrain

# What can we do?

- Resiliency
  - Understand mission first then risk to mission
    - Understand mission path (system of systems)
    - Fuse MDT, Ops, MX, Intel into risk assessment
      - Know your enemy
        - » China: IP theft
        - » Russia: Disruption (don’t draw early conclusions from Ukraine)
      - Know your systems
        - » 30 yr HVAC could be more of vulnerability than 5 yr server
    - Leaders own risk; support teams advise risk
      - Feed them information, prioritize, execute
      - Trade space to understand risk & where to take risk or improve systems
  - Acquisitions and Weapon System Authorities
    - Integrate teams, risk assess, appropriately delegate
      - Pivot faster than the enemy



INTEGRATED CYBER DEFENSE

Proactive Defense
- “Detect, Respond, and prevent” focus
- Removal of enemy threat
- Locate & respond to enemy

Resiliency – People, Process, Technology
- Acquisition baked in defense
- Reduces enemy success
- Mission success during attack

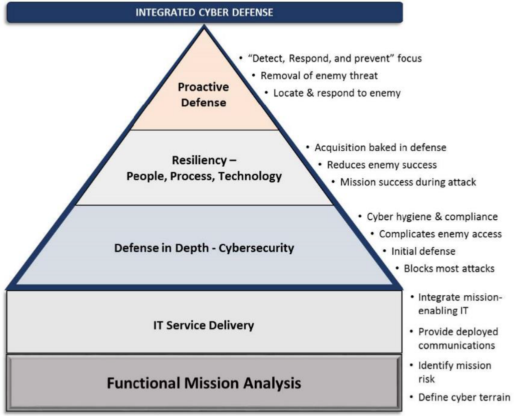
Defense in Depth - Cybersecurity
- Cyber hygiene & compliance
- Complicates enemy access
- Initial defense
- Blocks most attacks

IT Service Delivery
- Integrate mission-enabling IT
- Provide deployed communications

Functional Mission Analysis
- Identify mission risk
- Define cyber terrain

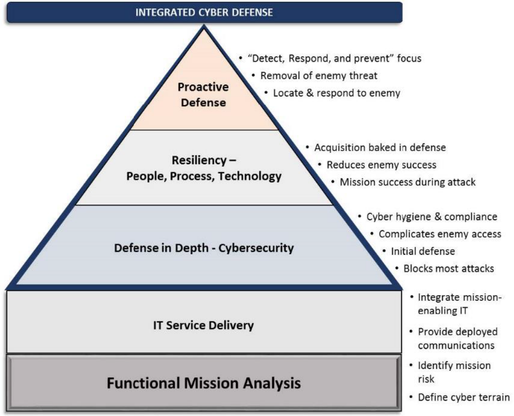
# What happened?

- Defense in Depth
  - Technology isn’t the answer
    - Zero Trust
    - Blockchain
  - Can’t divest it all
    - EITaaS can’t cover it all (classifications) and it’s too expensive currently
  - Know your enemy
    - Works by heuristics, AI/ML will not save the day
  - Better yet: know your troops
    - Compliance, insider threat vs. negligent user
    - No education revolution
      - MX hygiene that isn’t implemented or many know about


INTEGRATED CYBER DEFENSE
Proactive Defense
• “Detect, Respond, and prevent” focus
• Removal of enemy threat
• Locate & respond to enemy
Resiliency – People, Process, Technology
• Acquisition baked in defense
• Reduces enemy success
• Mission success during attack
Defense in Depth - Cybersecurity
• Cyber hygiene & compliance
• Complicates enemy access
• Initial defense
• Blocks most attacks
IT Service Delivery
• Integrate mission-enabling IT
• Provide deployed communications
Functional Mission Analysis
• Identify mission risk
• Define cyber terrain

# What can we do?

- Defense in Depth
  - Understand outcomes then match technology to it
    - Don’t chase it: form follows function
  - Enemy heuristics
    - Better integration of DODIN, NOS, Comm Sq with EITaaS
      - Divide and conquer contract with military (money balance)
      - Divide and conquer with overlapping fields of fire (delegate)
      - Comm Squadrons will have to stay linked at hip with MDTs
  - Education
    - Very cheap
      - Hygiene: change it up (Awareness 100, 200, 300, 400 series)
      - Classified education on risk to mission
      - Compliance (more importantly, why are they complying…mission failure)



INTEGRATED CYBER DEFENSE

Proactive Defense
- “Detect, Respond, and prevent” focus
- Removal of enemy threat
- Locate & respond to enemy

Resiliency – People, Process, Technology
- Acquisition baked in defense
- Reduces enemy success
- Mission success during attack

Defense in Depth - Cybersecurity
- Cyber hygiene & compliance
- Complicates enemy access
- Initial defense
- Blocks most attacks

IT Service Delivery
- Integrate mission-enabling IT
- Provide deployed communications

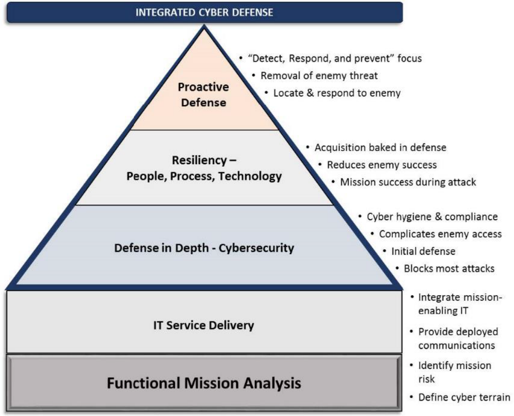
Functional Mission Analysis
- Identify mission risk
- Define cyber terrain

# Parting thoughts

- MDTs are for mission effectiveness not just cyber defense
  - AFSOC, 1 SOCS, AC-130J mission prep
    - Aircrew got efficiencies (less weight); MDT got effectiveness (less attack surface)
  - AFRC, 94 AW, C-130 tactical datalink
    - Fusion of entire team of teams, everybody got something out of it
  - AMC, 22 CS, mission & risk prioritization
    - Discovery of key nodes when entire wing got involved with assessment
    - Knew network so well without toolkit utilization

- Educate, Integrate, Operate
  - With any new capability involves understanding first
  - Slow is smooth, smooth is fast
    - Cyber TTX, 94 AW, creation of CP checklists

- Capture lessons learned but it must be seen by all
  - A2, 3, 4, 6
  - Information is there, but leadership must prioritize/integrate cyber defense mission



INTEGRATED CYBER DEFENSE

Proactive Defense
- "Detect, Respond, and prevent" focus
- Removal of enemy threat
- Locate & respond to enemy

Resiliency – People, Process, Technology
- Acquisition baked in defense
- Reduces enemy success
- Mission success during attack

Defense in Depth - Cybersecurity
- Cyber hygiene & compliance
- Complicates enemy access
- Initial defense
- Blocks most attacks

IT Service Delivery
- Integrate mission-enabling IT
- Provide deployed communications

Functional Mission Analysis
- Identify mission risk
- Define cyber terrain

# QUESTIONS

Improving cyber operations with thinking, not things.