24 AF
Operationalizing Cyber

Montgomery IT Summit

Art “Wally” Wachdorf
24 AF/CA
Foundational Principles

- Only operational domain that is man-made
- Physical Domain (A place, Not a mission)
- Where Operations are conducted (Like Land, Sea, Air & Space)
- Integrate operations conducted across domains (don’t integrate domains)
- It’s About Mission Assurance (not Network Assurance)

"Cyberspace is not a mission, it is a place where operations are conducted ... and is about assuring the mission, not about assuring the network”
– Maj Gen Dick Webber, AFNS, 20 Nov 09
Unclassified

The Battle has Come to Cyberspace

• Who
  • Individual hackers
  • Organized crime
  • Transnational groups
  • Nation states

• What
  • Known vulnerabilities
  • Attack applications vice OS
  • DoD contractors (attack seams)
  • Reverse engineer anti-virus
  • “Spear” phishing (targeted)
  • Supply chain

“Make no mistake about it, the fight is on in cyberspace”
- Gen C. Robert Kehler
24th Air Force

CC, Maj Gen Webber

624 OC, Col Diaz

67 NWW, Col Shwedo
688 IOW, Col Skinner
689 CCW, Col Giorlando
770 ISRG(P), Lt Col Hamrick
24 AF Mission: Extend, operate and defend the Air Force portion of the DoD network and to provide full spectrum capabilities for the Joint warfighter in through and from cyberspace

- Network Operations
- Information Operations
- Combat Communications
- 4,300 Active Duty & Civilians
  - Full Spectrum Network Ops
  - Maintenance
- 11,000 ARC

Mission Assurance for Joint Operations
Establish, plan, direct, coordinate, assess, command & control cyber operations and capabilities in support of Air Force and Joint requirements

Operational Orders
- CyOD
- AF-CTO
- CCO
- MTO

Current 624 OC Personnel: 90 (Military, Civilians)
624 OC FY10 Billets: 196
1. Identify critical mission elements and supporting infrastructure
1. Identify critical mission elements and supporting infrastructure
2. Assure infrastructure availability
3. Focus intelligence collection on mission support

1. Identify critical mission elements and supporting infrastructure
2. Assure infrastructure availability
3. Focus intelligence collection on mission support

Intelligence community

AF Circuit

Creech AFB

3. IC providing mission related Intel

2. Hot Back-up

2. Back-up circuit – single point of failure
1. Identify critical mission elements and supporting infrastructure
2. Assure infrastructure availability
3. Focus intelligence collection on mission support
4. Actively defend critical links, information, and infrastructure
Strategy Based Architecture

Crown Jewels
- DAL
- TBMCS
- TACC
- JSPOC
- Mission critical systems

Core Systems
- Email
- AF Portal
- MyPay
- Trusted partners

Self Managed Systems
- PMO
- Recruiters
- Red Cross

Virtual Technology

Access denied

Must Evolve From Perimeter Defense
Partnerships

• Seamless integration of Intel and Cyber
  • AFISRA and 24AF
  • Relationships with National Communities and AF

• AFOSI
• Joint
• Coalition
• Industry
• National Laboratories
QUESTIONS?
AFNET Macro View

- Standardize / minimize AF Gateways (CITS Blk 30)
- Intrusion Protection System (IOP) at Gateways (Dynamic Defense)
- Intrusion Detection System (ASIM) at each base (known threats)
- Monitor and alert (HBSS) at each machine (CITS Blk 35)
- Cyber C2 weapon system (CCS) (CITS Blk 40)
- Single trouble ticket & IT inventory tracking system
- Theater deployable communication integration
- Move to a single AF forest