Cultivating Cyber Warriors from the Ground Up

A Case Study in Building a Mission-Focused Cyber Defense Force

Cyber Workforce - Framing the Problem

Deterrence by Resilience. Denying the benefits of aggression also requires *resilience* – the ability to withstand, fight through, and recover quickly from disruption. The Department will improve its ability to operate in the face of multi-domain attacks on a growing surface of vital networks and critical infrastructure, both in the homeland and in collaboration with Allies and partners at risk. Because the cyber and space domains empower the entire Joint Force, we will prioritize building resilience in these areas. Cyber resilience will be enhanced by, for example, modern encryption

2022 National Defense Strategy

The Department must also expand its cyber workforce with various roles and develop talent to securely build, operate and maintain its digital and critical infrastructures and protect and defend our data against cyber adversaries at home and abroad. However, there is a recognized shortage of skilled cyber personnel that could potentially impact operational readiness across the Department and put national security at risk. Despite the vast expansion of cyber educational and experiential opportunities, the Nation's cyber talent pipeline remains limited.

2023-2027 DoD Cyber Workforce Strategy

The Department is collaborating with other government agencies, industry and academia to address the cyber talent pipeline challenge. While working collaboratively with these entities, the DoD faces fierce competition within the labor market to secure the necessary highly skilled experts from the Nation's finite talent sources. In light of this competition, the Department must foster an environment of innovation coupled with cutting-edge technology to produce and enable a world-class workforce ready to meet all current and future cyber challenges.

2023-2027 DoD Cyber Workforce Strategy

412 TW Organic Cyber Defense

- **FY 16 Mission Defense Team 'Pathfinder unit' – encountered initial difficulties**
  - MDT Pathfinder team didn't have a place in the CS org structure
  - Staffing turnover left only 1.5 people working on MDT
  - **No AF direction**

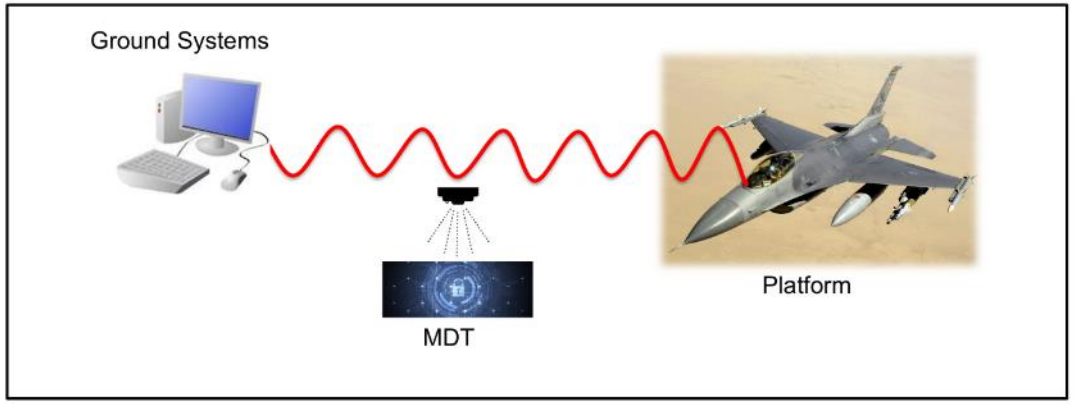
- **In Spring 2017, 412 CS/CC 'rebooted' the effort**
  - Increased manning of full-time personnel + Flight Chief personal oversight

- **In FY23, transitioned from MDT to local wing-tasked cyber defense cell**
  - Built out improved monitoring suite using non-program office hardware
  - Continued mapping 412 TW key cyber terrain and supporting assets
  - Baselined and characterized of local enclave traffic to identify patterns of behavior
  - Expanded cyber monitoring capabilities by developing AI tools to assist cyber analysts

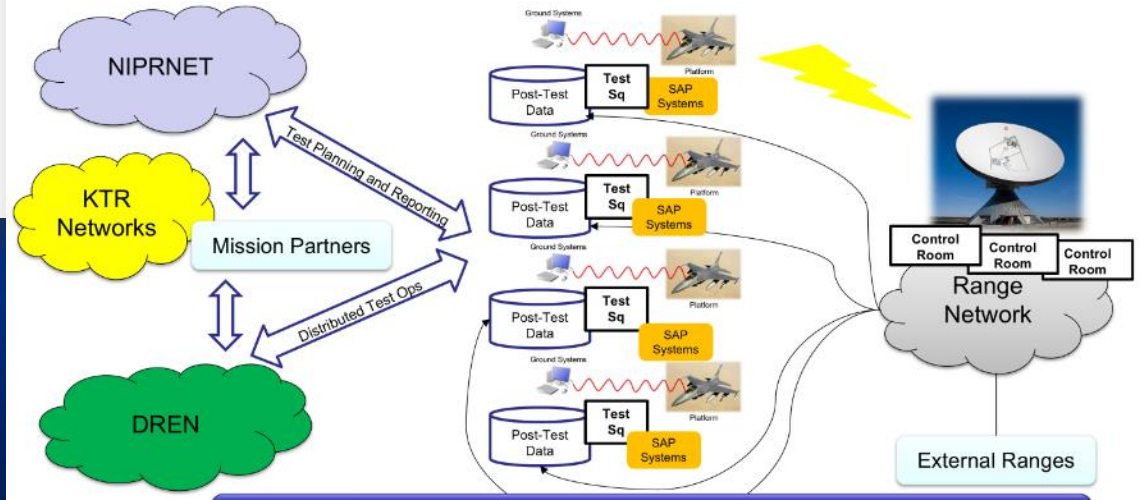
One Size Doesn't Fit All

'Traditional' MDTs

- **MDT 1.0 concept was inherently platform specific**
  - Focus is defending a discrete weapon system or capability



Cyber Defense at Edwards AFB



Cyber Defense of Test and Evaluation is Inherently Complex

..and the threats are equally complex

- Nation State Intrusion Campaigns
- APT Phishing / Social Engineering
- Supply Chain Threats
- Foreign Intelligence Agents
- Domestic Conspiracy Theorists
- Insider Threats
- Lack of Preparedness

What Does This Look Like in Practice?

Hunt

- **Search and Respond**
  - Detect threats in the defended terrain; detect adversary tradecraft that evades existing network defense capabilities. Coordinates incident response with local defenders, then, within the defended terrain, engages and eliminates adversary capabilities.

Survey

- **Scan, Plan, and Evaluate**
  - Performs **mission mapping** and MRT-C **analysis**

Secure

- **Penetrate and Assess**
  - **Validates improvements** made to the defended enclave from a relevant threat actor perspective; supports development of threat-relevant **countermeasures**

REDCORE is a 17-member team focusing on defending 412 TW cyber terrain. REDCORE obtains intel support from AFTC/XP2 as needed and has an ongoing relationship with AFOSI/PJ Detachment 7

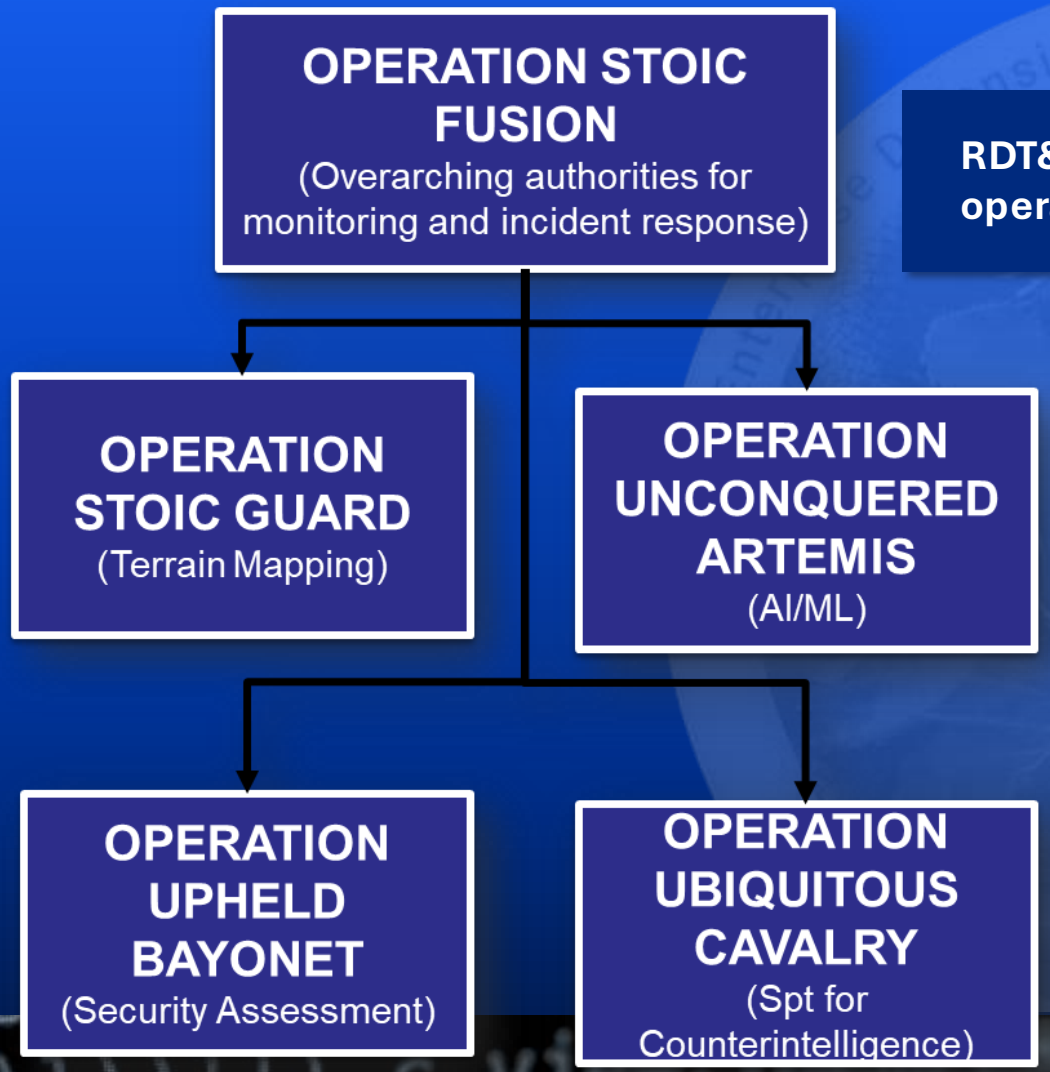
Mission

Actively defend 412 TW cyber terrain against known and unknown threats, ensuring the T&E mission execution remains agile, ready and right

Vision

World-class Cyber Warriors Providing Agile and Innovative Defense for The World Leader in Developmental Test and Evaluation

Cyber Defense Operational Concept



RDT&E Defensive Cyber Operations Response Element (REDCORE) operational concept to reflects unique mission needs:

OPERATION STOIC FUSION

On-going monitoring, hunting and incident response missions

OPERATION STOIC GUARD

Squadron-by-squadron mapping of 412 TW key cyber terrain and supporting assets

OPERATION UNCONQUERED ARTEMIS

Expand cyber monitoring capabilities by developing AI tools to assist cyber analysts

OPERATION UPHELD BAYONET

Perform security assessments to identify vulnerabilities in key cyber terrain

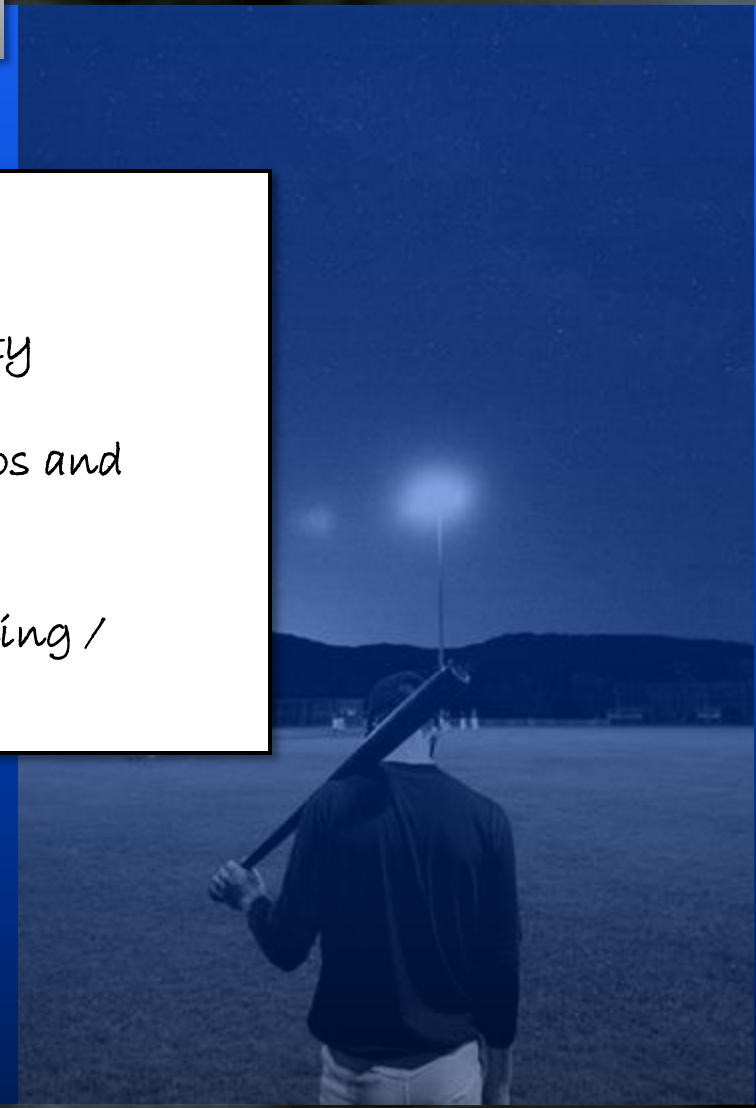
OPERATION UBIQUITOUS CAVALRY

Support counterintelligence operations

Key Skills for Cyber Defenders

- Years of experience
- Technical Expert
- Advanced certifications
- Multiple 6-figure salary

- Motivated
- DIY mentality
- OK with chaos and uncertainty
- Enjoys learning / research



You Don’t Need to Buy What You Can Build!

Where Do I Find These People?

Air Force Civilian Intern Programs

AFCS

- Premier College Intern → Palace Acquire
- Many owe Scholarship for Service time
- Motivated, educated
- **Centrally funded**
- **Think outside the 'AF box'**

Junior Enlisted Workforce

- Your 'fast-burning' junior airmen
- Wish they were doing the 'cool cyber stuff' they learned about in tech school
- **Looking to exceed expectations**

Does It Work?

For our civilian cyber defense analysts:

- 65% were recruited via AF career programs
- These programs have provided a stable pipeline for qualified, energetic new civilian airmen

AFCS

Our Cyber Warfare Training Program for junior enlisted is new for 2025, but already:

- Three airmen completed 4-month cyber defense tours
- Different specialties (Cyber Surety, Servers, Netman)
- Structured training plan designed by former civ interns

All have exceeded expectations and successfully contributed to active missions after a very short time

Recruiting & Retaining Cyber Talent

Even in a remote, isolated location where recruiting and retention has traditionally been very difficult:

- **~50% of PCIP summer interns choose to return full time as PAQs**
- **~60% of PAQs outplaced into permanent cyber defense positions**
  - The other 40% are serving as AF civilians in our unit or other units

Key Recruiting Factors

Based on interviews with staff who have completed internships, reasons for coming back full time included:

- **Ability to contribute to real-world missions / Sense of purpose**
  - Freedom to innovate, try new things
  - Dynamic work environment
- **Teammates & positive work environment**
  - Support for advanced training and self-improvement
  - Not already being an expert was OK
- **SFS service commitments & tough job market**

Key Retention Factors

Based on interviews with staff who have completed internships, reasons for remaining as permanent civilians:

- **Saw impact of contributions / able to "build something worthwhile"**
  - Focused on "something bigger than profit margins"
  - Pace of work kept them engaged
- **Young dynamic workforce / peer group**
  - Liked being around other mission-focused people
  - Collaborative innovation opportunities
- **Working with world-class weapon systems and tech**
- **Staying was an 'easy' / 'comfortable' choice**

Where Do You Start?

- **Start with a few motivated Airmen (officer/enlisted/civilian)**
  - We began with only four people
  - Carving some of your fastest burning folks ‘out –of-hide’ is an initially painful investment
- **Find the cyber defense mission inherent in your local cyber terrain**
  - What can’t the enterprise do for you?
  - What keeps your wing cc / director / etc. up at night
- **Give the team top-cover and freedom to innovate**
  - Initially feels like an expensive ‘science project’; embrace the chaos
  - Invest in training!
- **Leverage AF Civilian Career Program to find motivated junior workforce**
  - For summer interns, need at least 3-5 to form a ‘tribe’
  - The overhead / planning time ultimately pays off

Takeaway: Changing the Mindset

- We are **already** at war in Cyberspace
- You are **already** responsible for defending your mission
- Centralized efforts will **never** address all your needs
- **Resources are available** to get after the problem, it just takes work and prioritization
- **If a thing is worth doing, it is worth doing badly**

"**Activity in war** is movement in a resistant medium. Just as a man in water is unable to perform with ease and regularity the most natural and simplest movement, that of walking, so in war, with ordinary powers, one cannot keep even the line of mediocrity."

Carl von Clausewitz: ***On War, Book 1 Chapter 7***

Questions?