USAF Mission Defense Teams (MDT) Overview

Lt Col Emmanuel “Manny” Matos
ACC/A6OI
Overview

• The Strategic Environment
• The Threat
• The Response – Cyber Squadron Initiative
  • Initial Concepts
  • Cyber Squadron Transformation
• The Target – Weapon System’s MRT-C
• The Solution – Mission Defense Teams
  • MDT Core Functions
  • MDT Operations Cycle
  • MDT Force Package Composition
  • MDT Realignment - Proposed
• Necessary Partnerships
• Way Forward
Strategic Environment

Revisionist nation states such as Russia & China seek to shape the world consistent with their authoritarian model.

Russia, China, and rogue regimes desire to leverage cyberspace in an asymmetric manner to degrade US military combat capability and erode the power gap with their own militaries.

The US must deter these adversaries from attacking US military power projection through cyberspace.

End State

Air Force can project power with minimal interference from cyber attacks.

Ways

Consolidate organic cyber defense capabilities into Mission Defense Teams below the wing level.

Means

Field MDTs with standardized crews, training, equipment, and experts on local cyber terrain.
“...air superiority is not an American birthright. It’s actually something you have to fight for and maintain.”

- General Goldfein

“We must take into account the plans and directions of development of the armed forces of other countries...our responses must be based on intellectual superiority, they will be asymmetric, and less expensive.”

- Vladimir Putin
Threat Targeting

What They See
Mission Assurance of the Core AF Missions

- Warfighting and support systems reside within the cyberspace domain
- Without freedom of action within cyberspace, our ability to accomplish the five core missions is threatened
- Most Air Force weapons and support systems were designed to operate in a permissive cyberspace environment
- Cyberspace is contested; the presence of a maneuvering enemy in cyberspace requires mission assurance

- Mission Assurance (MA) - A process to protect or ensure the continued function and resilience of capabilities and assets—including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains—critical to the execution of DoD mission-essential functions in any operating environment or condition.

DoD Directive 3020.40

Today’s Communications Squadrons are not trained, organized, or equipped to assure core missions in a contested environment
Cyber Squadron Initiative (CS-I)

- Establish active cyber mission assurance capability for wings and equivalent
- Provide wing commanders and equivalent cyber situational awareness for informed risk decisions
- Formalize 24 AF supported/supporting role to mission commanders when additional cyber actions are required
- Ensure cyber “trade space” decisions made by programs are incorporated into risk decisions
- Integrate cyber into mission owner program requirements and system upgrades

Goal: Provide commanders with mission-tailored Cyberspace Mission Assurance capabilities to enable AF core missions
CS-I PAD D15-03 Timeline

In the News

- Air Force launches new task force to focus on cyber threats, Cyber Defense, Apr 2015
- Innovative cyber program protects critical Tyndall assets, 325th FW Public Affairs, Oct 2016
- The Future of Cybersecurity, Tinker Take-Off, Oct 2016
- Base level cyber squadron takes flight, 482nd CS, Nov 2016
- AF Fights Attacks With New “Cyber-Squadrons”, Warrior Maven, Nov 2017

Authority / References

- CORONA Top 2015 Tasker #1, June 2015
- SECAF/CSAF Strategic Guidance for 2016, 4 February 2016
- VCSAF Memorandum “Operating In, Thru, and From Cyberspace,” 29 June 2016
- Air Force Enterprise Information Technology as a Service (EITaaS) Concept of Operations (CONOPS), 9 March 2018
- Air Force Cyber Squadron Enabling Concept, 15 March 2018
- United States Air Force Cyber Squadron Support Construct Enabling Concept, 13 March 2019
Initial Concepts

Cyber Squadron Major Competencies

Cyber Squadron Enabling Concept (15 Mar 2018)
the Cyber Squadron “What”

Cyber Squadron Support Construct
Enabling Concept (13 Mar 2019)
Above-the-wing Support to MDTs
Objective Structure

Wings with a Cyber Squadron

Cyber Squadron Enabling Concept, SAF/CIO, 15 Mar 2018

Host wings without a Cyber Squadron
**Squadron Transformation**

**Communications Squadron**
- Primary role: IT Service provider
- AFNET (NIPR/SIPR)
- Compliance culture
- Success metric: uptime, tickets
- Information Assurance
- Provide vital IT services
- In garrison & expeditionary
- No Comm, no bomb

**Cyber Squadron**
- Primary role: Mission assurance
- AFIN ops/Wing’s weapons platform
- Risk management culture
- Success metric: sortie generation
- Cyber defense & cyber security
- Integrator of vital IT services
- In garrison & expeditionary
- No Comm, no bomb
Mission Defense Team (MDT)

**WHAT:**

BLUF: MDTs are the basic unit of employment for Cyber Squadrons.
- MDTs are Wing-Level Cyber Mission Assurance teams
- MDTs will be the Cyber Terrain SME and provide persistent monitoring and defense of Key Terrain in Cyberspace.
- 1 MDT crew will consist of: 9 Pax
  - 3 MDT Crews required for standard employment
  - MDTs are not Cyber Protection Team (not OPCON to CYBERCOM)

<table>
<thead>
<tr>
<th>Host</th>
<th>Net</th>
<th>MX</th>
<th>Intel</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

**HOW:**

Wheel of Access: Mission Assurance Process:

**WHO:**

- Currently: USAF has 84 Pathfinder MDTs
  - Pathfinders are “out-of-hide” implementations of MDT construct
  - MDTs have access to Cyber Vulnerability Assessment/Hunting Tool (CVA/H) but are application limited
  - 95% of MDTs are in local Comm Squadrons
- MDT Training Pipeline Goal is 1K per FY
  - 1st MDT Class started 5 Aug 19 (20pax) @ 223 COS
  - 2nd MDG Class starts 21 Aug 19 (20pax)
- Required Future AFSC (1D7) and UTC in works

Current MDTs are Manning and Training Limited; Post PAD 15-03 Approval and MAJCOM PPLAN IOC/FOC established
Mission Defense Teams defend the Wing’s primary weapon systems against threats in, through and from cyberspace. Related to the assigned weapon system, mission defense teams will:

- **Identify** the terrain critical to weapon system performance, tie into the sensor grid
- **Protect** and harden nodes and LOCs critical to the mission success
- **Detect** the mission area and deploy/task additional sensors
- **Respond** to blunt or deny adversarial efforts at disrupting or observing the wing mission through cyberspace
- **Recover** wing missions to ensure mission success
- **Ensure** Airmen are able to compete and preserve Air Power in the steady state operational environment
- **Ensure** Airmen are ready to fight and win in a contested operational environment
- **Ensure** Unit leadership understands and is provided options to mitigate threats in, through, and from cyberspace
Weapon System > Mission Relevant Terrain – Cyber (MRT-C)

Wheel of Access
#1 Provide Access and SME level support to MDTs.
- A4 has inherent understanding of most Mission Support Systems as well as weapon system operations
- SME Support critical to Functional Mission Analysis-Cyber (FMA-C);
- FMA-C must be an ongoing process as operating environments change

#2 Identifying POCs supporting MDTs at the Wing-level
- MDT elements need Mx/Logistics SMEs supporting their vulnerability mitigation efforts

#3 Assist in the development of Pre Approved Actions for MDTs to employ during an identified incident

#4 Partner with MDTs during initial and evolving knowledge exchange
- MDTs help with cyber hygiene best practices and the Logistics and Maintenance community help MDTs understand system functionality, TTPs, etc.

#5 Assist in identifying risk to system and COA creation for Wing Commander’s decision selection during incident
Way Forward

For CS-I/MDT:
- CSAF PAD 15-03 Signature (ECD Fall 2019)
- Cyber Squadron Implementation Planning via MAJCOM Program PLAN (PPLAN) – Probable A4 shaping period
- Complete MDT Concept of Operations and Concept of Employment
- Resourcing – Finalize FY22 Planning Choice, Begin FY22 POM

For A4 community
- Awareness of threats to WS Mission Support Systems
- Involvement in cyber survey and securing efforts lead by MDTs
- Advocacy with PMO/SPO Authorizing Officials for system Access and Vulnerability mitigation.
Questions?

MDT Intelink (UNCLASS): https://intelshare.intelink.gov/sites/accwfi/MDT/_layouts/15/start.aspx#
MDT Intelink (SECRET): https://intelshare.intelink.sgov.gov/sites/accco
CS-I/MDT Crosstalk Bi-Weekly Teleconference (240) 612-2079 - MSgt Jonathan McCullar (DSN 575-1954)