AIR WAR COLLEGE

AIR UNIVERSITY

AIR FORCE MISSION DEFENSE TEAMS

NOT YOUR GRANDPARENT'S COMMUNICATIONS SQUADRON

by

Erick O. Welcome, Lieutenant Colonel, United States Air Force

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: David B. "Boz" Bosko, Colonel, United States Air Force

27 February 2019

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted but is the property of the United States government.

Biography

Lieutenant Colonel Erick O. Welcome is currently a student at the Air War College, Air University, Maxwell Air Force Base, Alabama. He entered the Air Force in 1990 as a graduate of Basic Military Training. After serving 10 years as an enlisted professional he later graduated from Southern Illinois University and received his commission from Officer Training School in 2000. He is a cyber operations officer who has served at the squadron, group, major command, and Joint Staff levels. This includes commanding the 451st Expeditionary Communications Squadron at Kandahar Airfield, Afghanistan, and the 460th Space Communications Squadron at Buckley AFB, Colorado. He attended Intermediate Developmental Education at the United States Army's Command and General Staff College at Fort Leavenworth, Kansas. Lieutenant Colonel Welcome holds a Bachelor of Science Degree in Industrial Technology from Southern Illinois University at Carbondale and a Master of Management-International Studies degree from the University of Phoenix.

Abstract

Air Force core mission areas are vulnerable to nefarious cyber activities and senior Air Force leadership has impressed upon the Air Force to rapidly strengthen organic defensive cyber operations at the base level. Adversaries have proven to deny, degrade and disrupt Air Force weapon systems that enable (1) air and space superiority; (2) intelligence, surveillance, and reconnaissance; (3) rapid global mobility; (4) global strike; and (5) command and control. What organic defensive cyber capability do base level communications unit have to guarantee mission assurance? This paper examines the effectiveness of Air Force Mission Defense Teams (MDT) that are designed to deliver mission assurance through base-level proactive and persistent defensive cyber operations. Through research, surveyed various in-garrison and deployed units that have employed MDTs and interpret their effectiveness based on the following areas; intelligence, tools, training and talent management. Will make recommendations to strengthen MDTs based on research, interviews, surveys and overall feedback from the field. Finally, the Air Force cannot afford to have gaps in defending weapon systems from nefarious cyber activities at the base level. Mission Defense Teams must have a robust cyber defense arsenal to enable the Air Force ability to achieve core missions.

Former U.S. President Obama indicated cyber-security among greatest challenges.
"Just as we're all connected like never before, we have to work together like never before, both to seize opportunities but also meet the challenges of this information age. It's is one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm."
Barak Obama, former President, United States of America[1]

Introduction

The United States Air Force lacks mature cyber Mission Defense Teams that are capable to effectively defend nefarious cyber activities that target Air Force weapon systems. Air Force weapon systems consist of aircraft, ground-based, space and missile defense systems which are heavily reliant on complex software and high interconnectedly to perform their missions.[2] Cyber capabilities enable several sophisticated features (e.g., electronic warfare, precision strikes, and communications) that allow the Air Force to have a competitive advantage over adversaries, but creates opportunities for adversaries to counter these advantages through cyberattacks.[3]

Adversaries that compose of nation states or a potential lone wolf actor constantly attempts to discover and exploit vulnerabilities in a satellite's ground station software, supporting systems or logistics systems in order to obtain intelligence or to disrupt or degrade operations. Air Force base-level communications squadron have historically provided traditional information technology services to include: unclassified and classified voice and data capabilities, Radar, Airfield and Weather Systems capabilities that support an operational wing.

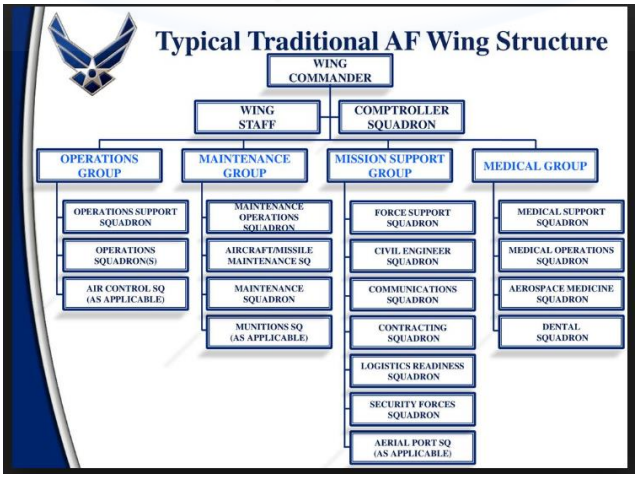
In order to better understand the Mission Defense Team construct, this paper will attempt to answer the question, **"Has Air Force Mission Defense Teams met Air Force Requirements?"** The goal of this paper is to 1) describe the pre-MDT state; 2) describe the desired MDT state; and then 3) provide recommendations to solve the gap between items 1 and 2 regarding MDT construct, intelligence support, training, talent and tools, and authorities. So, how did the Mission Defense Team effort start?

Pre-Mission Defense Team Posture

Pre-Mission Defense Team: Business Rules

Base or installation communications units in the past have generally focused on providing traditional information technology services to base users with a limited focus on mission assurance of weapon systems. These units were organized, trained and equipped to provided general services such as Non-classified Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), client services, basic voice and data capabilities and in some cases Radar, Airfield and Weather Systems (RAWS), formerly Air Traffic Control and Landing Systems (ATCALS). This communications culture cultivated an operation focused on network management and keeping "comms" green without clearly understanding how information technology affected operations. Additionally, communications squadrons are typically aligned under a Mission Support Group in a standard wing structure.[4]

Table 1. Air Force Typical Traditional Wing Structure per AFI 38-101[5]



Communications squadrons aligned under a Mission Support Group have typically focused on supporting the base's information technology requirements without strictly focusing on the core mission or providing proactive cyber defenses. This communications posture

created a mindset focused on network management and keeping "comms" green without clearly understanding how information technology affected mission assurance or enabled operations. This business practice evolved into how communications units have been operationally limited based on a lack of intelligence, cyber tools, training and talent to effectively defend the weapon system and guarantee mission assurance.

Pre-Mission Defense Team: Lack of Cyber Intelligence

Based on the creation of Air Force Network Operations Squadrons in 2007 base level communications units relied on these new organizations to provide as close to real-time intelligence to respond to nefarious cyber activities or vulnerabilities across the Air Force enterprise. However, vulnerabilities were not disseminated real-time, but more so on a scheduled basis to allow base units to apply patches and other remediation efforts to mitigate or remove vulnerabilities.

The impact of not having an organic intelligent capability to inform cyber defense tactics, techniques and procedures actions have proven to be costly and impacted operations. Per Major General Patrick Higby, former Director of Air Force cyber strategy and policy, most communications units did not understand how information technology affected day-to-day mission operations. General Higby eluded "when a circuit went out or a server crashed or a radio net went down, if a comm squadron commander went to their wing commander and said they just lost circuit x, y or z, the wing commander would ask what that meant for the mission; oftentimes the communications squadron commander did not have the full understanding of how communications affected operations."[6]

Pre-Mission Defense Team: Lack of Cyber Defense Tools

Communications squadrons are aligned under cybersecurity service providers and lack a robust suite of tools to perform cyber defense actions at the base level. The Air Force created this environment based on the Cyber Security and Control System (CSCS) weapon system. This weapon system was designed to provide 24/7 network operations and management functions and enable key enterprise services within Air Force unclassified and classified networks while providing defensive operations within those Air Force networks.[7]

The CSCS was an initiative to save resources, but more so focused on centralized command and control and less decentralized execution as several bases did not have tools to effectively operate, maintain and defend their base networks. In an effort to save money and manpower, a wing's cyber defense posture was limited to defensive cyber operations capabilities at the base level.

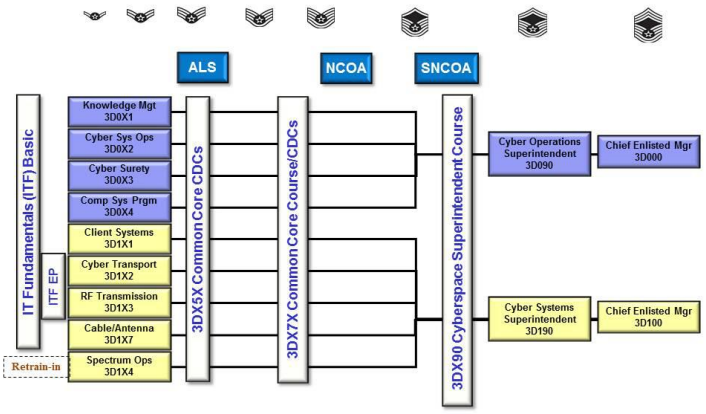
Local communications units focused on defending unclassified and classified voice and data networks that supported the base mission, but not necessarily an installation's weapon system. For example, a space wing may have a missile warning mission that is fueled by a particular weapon system where the local communications have no situational awareness of its defensive cyber operations posture. Additionally, there were not any organic cyber defense tools local units were authorized to use on the weapon system.

Weapon systems have no-fail mission networks that are isolated from a base's general service networks. These networks are not easily cleared to test defensive cyber operations tools due to the complexity of the weapon systems and lack of key cyber terrain knowledge. In addition to a lack of tools, there is a huge cybersecurity training gap of the MDT cyber workforce.

Pre-Mission Defense Team: Lack of Cyber Security Training

The majority of Airmen in the cyberspace support Career field (3DXXX) do not have the resident expertise to defend base networks as their training pipeline is designed to focus on managing information technology services supporting generic base missions. There is a major cyber defense training gap that prevents teams from focusing on providing mission assurance of Air Force weapon systems. Per the Air Force Career Field Education and Training Plan for Cyberspace Support, Airmen are charged to perform system analysis and design, programming, systems operation and maintenance, resource management and security management. In addition, these cyber Airmen execute activities for installing, maintaining, repairing, overhauling, deploying, and modifying cyberspace systems and equipment platforms. Finally, they conduct network warfare operations in garrison and at deployed locations by performing duties to develop, sustain, and enhance network and electromagnetic capabilities to defend national interests from attack and to create effects in the cyberspace domain to achieve national objectives.[8] There is a clear lack of defensive cyber operations training to educate base-level personnel to effectively defense base and weapon systems.

Table 2. 3DXXX Career Field Path – No Codified Defensive Cyber Operations Path[9]



Pre-Mission Defense Team: Lack of Cyber Security Talent

As discussed earlier, the majority of cyber support Airmen assigned to a typical wing are organized, trained and equipped to provide traditional information technology support and are not organized to defend base weapon systems. There is no dedicated defensive cyber operations force allocated specifically for base communications units. Airmen within the Air Force Cyberspace Defensive Operations (1B4X1) air force specialty code is designed to perform duties to develop, sustain, and enhance cyberspace capabilities to defend national interests from attack and to create effects in cyberspace to achieve national objectives.[10] Unfortunately, this high-demand, low-density asset is prioritized to support the Air Force's contribution to Cyber Mission Forces.

The Cyber Mission Force is United States Cyber Command's action arm, and teams execute the command's mission to direct, synchronize and coordinate cyberspace operations in defense of the nation's interests.[11] These teams are critical to the nation's defense by identifying and blocking adversary activities and maneuvering to defeat adversaries. While these missions are critical, several cyber-savvy Airmen have been allocated to support this mission.

The Air Force has roughly 2,500 cyber officers on active duty and those 2,500 officers must fill cyber mission force requirements, as well as Air Force cybersecurity requirements.[12] When it comes to retention rates in the Air Force, the cyber mission force is manned at 100 percent, meaning the 39 Air Force teams dedicated to USCYBERCOM will receive 100 percent of their staffing.[13] Additionally, there is a high demand for cyber professionals within the commercial sector and the Air Force has invested in and lost several cyber Airmen to opportunities in the civilian workforce.

The Department of Defense (DoD) faces tremendous challenges in recruiting and retaining trained and experienced cybersecurity professionals.[14] DoD's challenge is part of a larger worldwide shortfall for this high demand resource. According to the Global Information Security Workforce Study, cybersecurity professionals' manpower shortfall is on track to reach 1.8 million by 2022.[15] It is a fact that DoD pay lags behind the commercial industry – annual base pay for an E5 with four years of service is $32,000 and an O-3 with four years of service is $66,300 – based on the 2018 pay scale.[16] In contrast, the average civilian cyber penetration tester with four years of experience earns approximately $115,000[17]; DoD has an uphill battle to compete with industry. Retention will continue to be a key component hindering the Air Force from having a talented cyber workforce and achieving the desired state of full mission capable Mission Defense Teams.

Feedback from Strategic, Operational and Tactical Levels

Feedback from the Field: Not all MDTs Meeting Air Force Requirements

There is no better way of understanding how the Air Force Mission Defense Teams are postured without engaging the teams who are in the field accomplishing this important mission. As such, I reached out to various key players at the strategic, operational and tactical levels to better answer the question: "Are Air Force Mission Defense Teams meeting Air Force Requirements"? The overwhelming response is "not quite"; however, there are a few MDTs that are further along than others, but until the organizational culture shifts, MDTs will be limited in maximizing their effectiveness.

Feedback from the Field: Need to Change Culture

The old paradigm of base-level communications squadrons *only* being a service provider for an installation and not focusing on defending weapon systems is no longer. Per Major General Robert J. Skinner, Commander, 24th Air Force; Commander, Air Forces Cyber and Commander, Joint Force Headquarters-Cyber, "it all starts with changing the culture beyond a shadow of a doubt. Wing commanders and the entire wing structure must not only embrace and advocate for the MDT mission but also heavily invest in people and equipment to re-orient acceptance of this wing capability."[18] The successful MDTs have full support from their wing and group leadership, which allows units to take risks in other mission areas and focus on providing mission assurance of weapon systems. Currently, the AF IT workforce is tied to operations and sustainment of commodities and services limiting its ability to field an agile cyberspace workforce.[19] A key driver of advocating for a change of culture is for wing leaders to better understand their installation's cyber defense posture of their weapon systems through a Functional Mission Analysis (FMA).

An FMA identifies a wing's core mission's key cyber terrain and provides a methodology to analyze the unit's operational mission to understand how cyberspace systems contribute to mission success and how cyber vulnerabilities translate to mission risk. [20] Key terrain in cyberspace is found across traditional information systems, control systems, platforms, and weapon systems.[21] Most importantly, by understanding risks to core missions enables senior leaders to make informed decisions about the health of their networks and provides greater credibility to investing in Mission Defense Teams. The realization of crippling a wing's core mission due to a cyber incident provides base communication squadrons the justification they need for senior leaders to change the culture of a service-oriented environment

to one of mission assurance of weapon systems. Another gap preventing the fielding of an effective MDT is a lack of organic manpower. Good news is the implementation of the Enterprise Information Technology as a Service (EITaaS) initiative will enable units to provide manning for their MDTs.

Feedback from The Field: Must Provide Units with MDT Organic Manpower

Enterprise Information Technology as a Service initiative will selectively leverage the private sector to provide standardized, innovative, and agile IT services to the AF through the use of worldwide commercial business services and best practices.[22] This new approach will enable the utilization of the AF IT workforce to the cyberspace workforce.[23] The EITaaS initiative is a transformational effort that will free up a unit's military and civilian personnel to resource MDTs. Based on feedback from the field, units are still responsible of providing IT services across a particular base and must take risks in certain mission areas to allocate manpower towards MDTs until contractors are in place to accept IT-service responsibilities. The more effective MDTs have aggressively moved out with hiring contractors to operate on their MDTs which is a plus as contractors are hired with the required skillset to effectively employ cyber defense tactics, techniques and procedures. Hiring contractors will be based on wing leaders prioritizing wing requirements and investing dollars in the organization, training and equipping of MDTs to reach the desired state expeditiously.

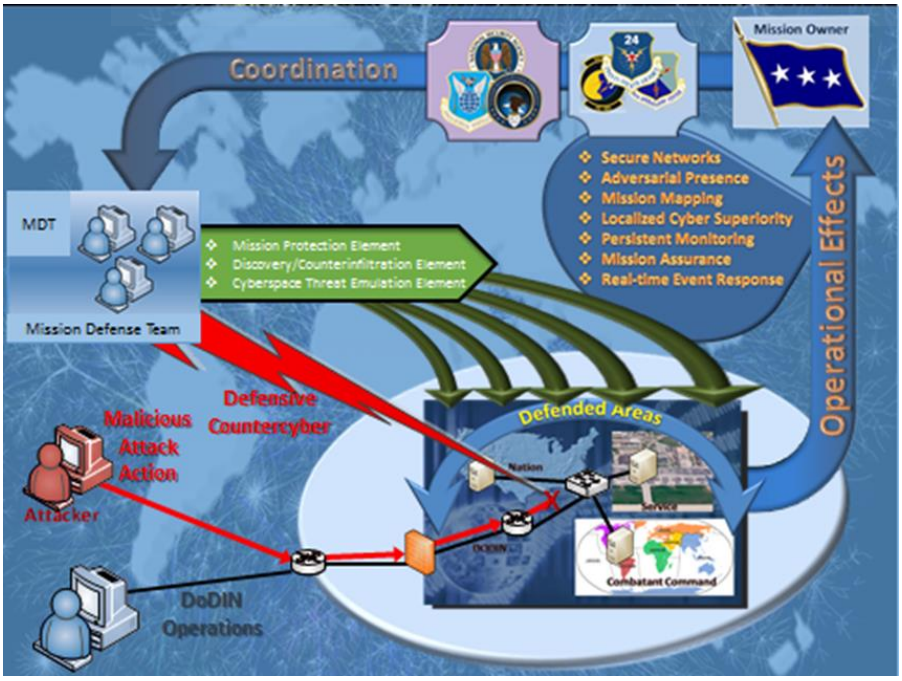
Mission Defense Team – Desired State

The Mission Defense Team end state is to produce specialized cyber teams across the Air Force whose primary mission will be to defend local installations and critical mission tasks from nefarious cyber activities.[24] This effort will take heavy investments by the Air Force in base communications units to ensure they are organized, trained and equipped to increase their

defensive cyber posture. Moreover, communicators will need to have an increased familiarization with the base's core mission.

Major General Robert "Bob" Skinner, Air Forces Cyber Commander eluded that if a wing has an F-16 unit that's responsible for offensive counter air or defensive counter air support, mission defense teams will need to understand those weapon systems and everything that goes into making those air sorties successful as a way to defend that mission from a cyber standpoint.[25] The days of only focusing on maintaining 1s and 0s and not understanding how computer systems affect core missions are long gone. Similar to the integration of operations and maintenance, cyber operators will need to spend countless hours understanding how the network and internet of things affect operations. At the core of how MDTs are envisioned are six desired effects; 1) **Mission Assurance** 2) **Identification of Advanced Persistent Threats** 3) Mission **Mapping to Identify Cyberspace Key Terrain** 4) Localized **Cyber Superiority** 5) Persistent **Monitoring and Characterization** 6) Adversary **Engagement**

Table 3. MDT Employment Operational View -1[26]



Mission Defense Team – Desired State: Mission Assurance

Ultimately Mission Defense Teams will be charged to deliver mission assurance of Air Force weapon systems through laser-focused employment of weapon and mission system defense capabilities. Future vulnerabilities and threats will continue to heighten which calls for proactive MDT tactics, techniques and procedures to counter those threats. This effort causes a rapid shift in focus from compliance and cybersecurity to a focus on cyber defense while enabling core Air Force missions and capabilities.[27] Additionally, intelligence will play a critical role in knowing what vulnerabilities are present or on the horizon and most importantly, how to respond to those threats.

Mission Defense Team – Desired State: Identification of Advanced Persistent Threats

It is imperative that future Mission Defense Team operations are driven by intelligence that is timely, accurate and actionable.[28] In order for MDTs to be effective in their tactics, techniques and procedures an organic base level intelligence cell will need to be a part of the MDT construct. Higher echelon intelligence organizations will need to link MDTs within with the Intelligence Community to not only inform mission planning but identify potential threats to defended systems.[29]

Receiving intelligence of threats to mission systems and more importantly understanding how weapon systems operate from a cyber lens is a critical piece to defending those weapon systems. MDTs will need to have the capability to find, fix, track, target and engage advanced persistent threats in the least amount of time possible. Mission Defense Teams will need to perform a Functional Mission Analysis and Network Characterization of weapon systems to identify key cyber terrain and dependencies related to the wing's operational missions. This

effort will assist MDT personnel to not only detect but to respond to nefarious activities or anomalies within the weapon system.

Mission Defense Team – Desired State: Mission Mapping to Identify Key Cyber Terrain

Teams will need to understand what "right looks like" to be effective in defending Air Force weapon systems. At its pinnacle, defensive cyber operations "hunting" is the search for key cyber terrain with a goal of understanding the link between cyber terrain and the mission it enables.[30] MDTs will need to fully immerse into operations to have an intimate understanding of how systems and networks affect weapon systems and by performing a thorough Functional Mission Analysis will provide the level of fidelity required.

Mission Defense Team – Desired State: Localized Cyber Superiority

Mission Defense Teams need to ensure cyber superiority at their localized sites to ensure mission assurance of selected weapon systems. It is well known that military superiority in the air, land, sea, and space domains is critical to the United States ability to defend its interests and protect United States values. Achieving superiority in the physical domains relies heavily on cyberspace; however, the United States military oftentimes risks yielding cyberspace superiority. [31] United States adversaries have exploited the speed, capacity of data and events in cyberspace, making the domain more hostile.

Maintaining local cybersecurity in a hostile environment is not an easy task and will call for an integrated partnership amongst base users. Cybersecurity is every user's business and a lack of cyber hygiene and discipline will cause grave effects to operations. In 2015 the Joint Staff's unclassified email was hacked by suspected Russian actors due to poor cybersecurity discipline.

Per open source reporting, Joint staff personnel received spear-phishing emails that were modified messages that appeared to originate from trusted associates. These emails contained embedded links to documents that caused malware to be downloaded on specific computer systems. This lack of user discipline prompted the Joint Staff to disconnect from the global unclassified email system for 11 days.[32] Maintaining cybersecurity of base networks will need a laser focus not only from Mission Defense Teams but also from every user accessing DoD information systems.

Mission Defense Team – Desired State: Persistent Monitoring and Characterization

Mission Defense Teams will need to have the ability to persistently monitor, have the ability to characterize nefarious cyber activities and enable base operations the option of fighting through a cyber disruption or attack. The adversary gets a vote and will execute various tactics, techniques and procedures to deny, disrupt, degrade, deceive and exploit mission system processing. Teams will need to understand how to leverage "Hunting" activities and techniques to integrate mission assurance and defensive cyber operations capabilities while defending key cyber terrain.[33] Close integration with Computer Network Defense Service Providers will be critical to for MDTs to be effective with persistent monitoring and characterization of the network. Teams will need to be well-versed on defensive cyber operations hunting through close integration with mission owners and understanding their respective cyber key terrain.

Mission Defense Team – Desired State: Increase Organic Manpower

As base communications squadrons transform into cyber squadrons, unit personnel will need organic manpower focused on defending weapon systems and more importantly possess the authorities required to process required cyber effects. Additionally, the integration of

intelligence personnel within cyber squadrons is paramount to ensuring cyber squadrons are intelligence driven.[34] Training will be a key enabler to ensure MDTs will have similar skills to Cyber Protection Teams.

Mission Defense Teams will need a codified training pipeline and continuous track to ensure personnel are capable of effectively employing defensive cyber operations. Per AFCYBER Commander, Major General Bob Skinner, "The Mission Defense Team is a cyber protection team "lite", we are very proud of our cyber protection team training and the more training we can provide our MDTs, the more successful they will become. Then we can really focus our cyber protection teams on greater threats that we will face with a peer competitor and peer adversaries."[35]

Mission Defense Team – Desired State: Adversary Engagement

One of the key attributes Mission Defense Teams needs to possess is the ability to not only engage adversaries but have the ability to defeat them without impacting operations. This effort will require appropriate manpower, training, intelligence and a suite of cyber tools that can be tailored to specific cyber operations. Cyber operations must be codified into several weapon system exercises to include red teaming to adequately posture MDTs to be ready when adversary engagement is probable or imminent.

During a 2018 wing exercise at Tyndall Air Force Base a Mission Defense Team was tested to validate protecting weapon systems in a dynamic security environment in which potentially unknown cyber vulnerabilities could impact operations. The exercise objective was to assist the Air Force to create a process that would inform cyber analysts to determine if a software glitch inside an aircraft was an isolated failure or if other aircraft across the world were experiencing the same issue.[36] This operational focus by Air Force communications units is a

transformational shift of being a base information technology service provider to focusing on mission assurance.

Recommendations

Actions to Solve Gap between MDT Current and Desired End State

The Air Force must prioritize Mission Defense Teams and invest in their overall development; specifically, intelligence, cyber tools, talent, and training. These four areas are critical to closing the gap between MDT current and desired end state. Integration with the Intelligence Community to better understand potential threats and vulnerabilities is a critical first piece to creating robust DCO teams. Per Colonel Dave Bosko, Air Force Cyber College Instructor, "not only is cyber a consumer of intelligence, but cyber is also a producer of intelligence artifacts."[37] In addition, there are several agencies and organizations that MDTs can leverage to maximize their utility. The Air Force Cyber College is a tremendous resource that offers units to various resources to strengthen their MDTs.

The Air Force Cyber College located at Maxwell Air Force Base, Alabama creates concepts, theory, strategies and force development for national cyber endeavors.[38] Per Col Bosko, "the leadership within the college is actively engaged with supporting MDTs by meeting with wing leadership, providing functional mission analysis cyber training and partnering with the Cyber Resilience Office of Weapon Systems". Air Cyber College leaders have been instrumental in elevating the priority levels of support for MDTs.

The Air Force Cyber College team met with several wing commanders to highlight the need to defend weapon systems and hammer home vulnerabilities found within those systems and potential operational impacts. The college is comprised of rated and non-rated senior officers and civilians from various backgrounds and experience. Through direct engagement

with wing leaders, the college has helped squadron commanders with their MDT advocacy and resource challenges. These visits are complimented due to the Functional Mission Analysis performed at each base to highlight key cyber terrain and cybersecurity strengths and weaknesses of weapon systems.

In Fiscal Year 2018 the AF Cyber College administered Functional Mission Analysis-Cyber (FMA-C) training to 650 personnel while supporting a total of 2,040 graduates. In addition, the college provided guidance and education to Air War College, Air Command and Staff College and Squadron Officer School students. The FMA-C course bridges the gap between network operations and the five core missions of the Air Force.[39] Students learn critical and strategic thinking skills and apply them according to the Functional Mission Analysis methodology to address mission assurance beyond compliance.[40] Students will begin the transition to a warfighting mindset necessary to "fight the network" as a weapon system.[41] Another key organization MDTs need to leverage is the Cyber Resilience of Weapons Systems.

In January 2018, the Air Force announced the creation of the Cyber Resiliency Office for Weapons Systems (CROWS), which was declared fully operational in October 2018.[42] CROWS integrate activities across the Air Force to ensure that weapon systems maintain mission-effective capabilities despite cyber adversities.[43] The ultimate goal is to overhaul the Air Force culture so that cyber resiliency becomes an integral part of the technology acquisition process.[44] The Air Force needs to pursue the notion of having weapon systems that have cybersecurity “baked in” versus battling with a long and arduous cyber acquisition timeline to bolster weapon system cybersecurity.

The CROWS team began by exploring a couple of mission threads, including aerial refueling. For example, a cyber attacker could infiltrate an aircraft’s computer systems and

change the rendezvous point, causing the aircraft to miss a chance for refueling.[45] Or, a base-level attack could shut down the so-called fuel farm, preventing a mission commander from launching aircraft.[46]

Ultimately, Air Force officials would like to see a major transformation of the service's acquisition culture to focus more on cybersecurity.[47] CROWS need to be closely integrated with industry as they are charged for the development, testing, and maintenance of weapon systems. There needs to be a proactive approach built into the acquisition process to ensure systems contain an appropriate cybersecurity baseline and the tolerance to accept additional cybersecurity tools. In order to effectively employ tools, the Air Force needs to codify what type of MDT Weapon system will be used.

Mission Defense Teams were initially provided an MDT-Toolkit that did not properly equip MDT operations with the capability to engage advanced persistent threats, but more so the capability to find, fix, track, target and assess those APTs.[48] The Air Force needs to provide an MDT baseline weapon system similar to the Cyberspace Vulnerability Assessment/Hunter (CVA/H) weapon system.

The CVA/H system includes capabilities designed to engage adversaries but the majority of MDT personnel are not certified weapon system operators and are not afforded the option to use the CVA/H. This limiting training factor creates a huge gap with maximizing the utility of our MDT and causes for the creating of an MDT weapon system that is fully mission capable to not only identify and assess adversaries but engage them directly. Training is a core enabler to ensure unit personnel who transition from traditional IT service delivery functions to defensive cyber operations have the expertise required to provide mission assurance of the wing's mission.

Mission Defense Team training will need a combined effort between cyber and intel organizations to fully prepare our MDTs to operate in a contested, degraded and operationally-limited environment. Per Major General Skinner, "we need to have the right capacity at the 39th Information Operations School (Hurlburt Field, FL) and Keesler Air Force Base while spending the right amount of time at Goodfellow AFB to leverage our intel school".[49] The 39th Information Operations is the Air Force's premier information operations and cyber formal training unit and conducts qualification and advanced training to provide mission-ready Information Operations and Cyber Warfare operators for all Air Force Major Commands.[50] One of the most important MDT needs is manpower, units need to aggressively work the implementation of EITaaS to have dedicated military and civilian to allocated to defensive cyber operations for the purpose of mission assurance.

Base level communications squadrons must take calculated risks with day-to-day IT service delivery tasks while smartly organizing, training and equipping MDTs. Wing commanders will play a critical role by supporting these units by providing "top cover" during the transformation from communication squadrons to cyber squadrons. For example, customer wait times to fix unclassified systems where there is not an operational impact will drastically increase. Having support from wing leadership will allow units to focus on transforming their units and posturing their MDTs. In addition, there must be a seamless transition between EITaaS contractors and unit personnel to prevent operational impacts with day-to-day business. Also, contractors will need to sustain the integrity of unclassified and classified systems while maintaining Air Force cybersecurity standards.

Conclusion

Based on feedback from senior leaders and units in the field, not all Air Force Mission Defense Teams are meeting AF requirements. In order to meet this requirement will take a concerted and focused effort at all levels to ensure "ITTT": Intelligence, Tools, Training, and Talent are aggressively being worked to support MDTs. However, the AF is leading the way in transforming communications squadrons into cyber squadrons. This effort will pivot unit personnel from providing IT service delivery capabilities to focusing on defending cyber key terrain of a base weapon systems. Understanding the terrain is a key enabler to maximizing the utility of MDTs.

Intelligence drives or should drive operations and allow AF MDTs to posture their defense capabilities based on threats or future threats. Without cyber intelligence, MDTs will be limited in maximizing their cybersecurity posture. Cyber and intelligence organizations must continue their partnership and the 24th Air Force transition to Air Combat Command will help strengthen this partnership. Per Secretary of the Air Force Heather Wilson, "this move [24th Air Force] will drive faster decisions as we fight by realigning the cyber operations and intelligence, surveillance and reconnaissance missions under the same command."[51]Based on timely and relevant intelligence, you will need personnel who are trained to operate existing and future MDT weapon systems.

Mission Defense Team training needs to remain at the forefront and be prioritized at the wing level to ensure funds are allocated towards this effort. Training will need to consist of initial skills training along with a codified pipeline that will enable the required throughput. Most importantly, manpower is the bedrock of creating effective MDTs while helping units transition to cyber squadrons.

Communications units must continue to take calculated risks with daily operations while attempting to organize, train and equip their MDT workforce. The Air Force awarded $120 million dollars in September 2018 to support the EITaaS initiative which will help accelerate unit military and civilian personnel to focus on defensive cyber operations.[52] Most importantly, the Air Force must change organizational cultures and eliminate paradigms of how business used to be accomplished. The time is now to transform into a new way of leading and thinking that will posture our Mission Defense Teams to enable mission assurance across the Air Force.

Notes

[1] Payton Guidon, "US President Obama says cyber-security among greatest challenges", Independent, 13 Feb 14. https://www.independent.co.uk/news/world/americas/us-president-obama-says-cyber-security-among-greatest-challenges-10045950.html (accessed 15 Dec 18)

[2] Don Snyder, James D. Powers, Elizabeth Anne Bodine-Baron, Bernard Fox, Lauren Kendrick, and Michael H. Powell, "Cybersecurity of Air Force Weapon Systems", RAND Corporation, 2015, RR1007. https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9800/RB9835/RAND_RB9835.pdf (accessed 15 Dec 18)

[3] Ibid.

[4] Air Force Organization, AFI 38-101, Figure 3.3, page 26, 31 Jan 17. https://static.e-publishing.af.mil/production/1/af_a1/publication/afi38-101/afi38-101.pdf, (accessed 20 Nov 18).

[5] Air Force Policy Directive, Organization and Unit Designations, 24 May 18, https://static.e-publishing.af.mil/production/1/af_a1/publication/afpd38-1/afpd38-1.pdf, (accessed 15 Dec 18).

[6] Mark Pomerleau, "Air Force to begin cyber squadron roll out" 6 Feb 18, https://www.fifthdomain.com/dod/air-force/2018/02/06/air-force-to-begin-cyber-squadron-roll-out-in-2018/ (accessed 15 Dec 18).

[7] https://www.afspc.af.mil/News/Article-Display/Article/1036711/50-scs-learning-cyber-defense/

[8] Career Field Education and Training Plan, Cyberspace Support, AFSC 3DXXX, 1 Sep 14. https://static.e-ublishing.af.mil/production/1/saf_cio_a6/publication/cfetp3dxxx/cfetp3dxxx.pdf (accessed 15 Dec 18).

[9] Ibid.

[10] Career Field Education and Training Plan, Cyber Warfare Operations, 15 Jul 18, https://static.e-ublishing.af.mil/production/1/saf_cio_a6/publication/cfetp1b4x1/cfetp1b4x1.pdf (accessed 15 Dec 18).

[11] U.S. Cyber Command Public Affairs, "Cyber Mission Force achieves Full Operational Capability", 17 May 18, https://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/ (accessed 15 Dec 18).

[12] Mark Pomerleau, "Holding on to the Air Force's cyber workers", 20 Jun 18, https://www.fifthdomain.com/dod/air-force/2018/06/20/holding-on-to-the-air-forces-cyber-workers/ (accessed 15 Dec 18).

[13] Ibid.

[14] Ibid.

[15] Arthur MacDougall and Michael Meyers, "Pentagon faces array of challenges in retaining cybersecurity personnel", https://thehill.com/opinion/cybersecurity/391426-pentagon-faces-array-of-challenges-in-retaining-cybersecurity-personnel (accessed 15 Dec 18).

[16] United States Air Force Military Pay Chart, https://militarybenefits.info/2018-military-pay-charts/ (accessed 15 Dec 18).

[17] Cyber Penetration Tester Salaries in the United States, https://www.indeed.com/salaries/Penetration-Tester-Salaries (accessed 15 Dec 18).

[18] Major General Robert J. Skinner Interview, Commander, 24th Air Force; Commander, Air Forces Cyber and Commander, Joint Force Headquarters-Cyber, 30 Jan 19.

[19] Dennis Richer and Jarvis Croff, "Mission Defense Team Military Utility Assessment Final Report", 05 Sep 18, Page 7.

[20] Major General Patrick Higby and Lt Col Steven Wieland, "Cyber Squadron Enabling Concept, 15 Mar 18.

[21] Ibid, page 11.

[22] Dennis Richer and Jarvis Croff, "Mission Defense Team Military Utility Assessment Final Report", 05 Sep 18, Page 7.

[23] Ibid.

[24] Mark Pomerleau, "Air Force to begin cyber squadron roll out" 6 Feb 18, https://www.fifthdomain.com/dod/air-force/2018/02/06/air-force-to-begin-cyber-squadron-roll-out-in-2018/ (accessed 15 Dec 18).

[25] Ibid.

[26] HQ AFSPC Mission Defense Team Concept – DRAFT, 02 Feb 16.

[27] HQ AFSPC Mission Defense Team Concept – DRAFT, 02 Feb 16.

[28] Major General Patrick Higby and Lt Col Steven Wieland, "Cyber Squadron Enabling Concept, 15 Mar 18.

[29] Ibid.

[30] HQ AFSPC Mission Defense Team Concept – DRAFT, 02 Feb 16.

[31] Ibid.

[32] Martyn Williams, "Joint Chiefs of Staff emails targeted by Russian hackers", 6 Aug 15. https://www.computerworld.com/article/2960806/malware-vulnerabilities/joint-chiefs-of-staff-emails-targeted-by-russian-hackers.html (accessed 15 Dec 18).

[33] HQ AFSPC Mission Defense Team Concept – DRAFT, 02 Feb 16.

[34] Major General Patrick Higby and Lt Col Steven Wieland, "Cyber Squadron Enabling Concept, 15 Mar 18.

[35] Mark Pomerleau, "Air Force begins to roll out special cyber defense teams", 27 Dec 18, https://www.airforcetimes.com/dod/air-force/2018/12/27/air-force-begins-to-roll-out-special-cyber-defense-teams/ (accessed 15 Dec 18).

[36] Mark Pomerleau, "New Air Force cyber teams debut at exercise", 28 Jun 18, https://www.fifthdomain.com/dod/air-force/2018/06/28/new-air-force-cyber-teams-debut-at-exercise/ (accessed 15 Dec 18).

[37] Colonel David Bosko, Air Force Cyber College, Advisor Meeting, 08 Feb 19

[38] Air Force Cyber College Mission Brief, dated 4 Feb 19.

[39] Air University, Air Force Cyber College, https://www.airuniversity.af.edu/CyberCollege/FMAC, accessed 15 December 2019

[40] Ibid.

[41] Ibid.

[42] George I. Seffers, "Cyber Resiliency a Feather in CROWS Flight Cap", The Cyber Edge, 1 Jul 18, https://www.afcea.org/content/cyber-resiliency-feather-crows-flight-cap (accessed 15 Dec 18).

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] Ibid.

[47] Ibid.

[48] HQ AFSPC Mission Defense Team Concept – DRAFT, 02 Feb 16.

[49] Major General Robert J. Skinner Interview, Commander, 24th Air Force; Commander, Air Forces Cyber and Commander, Joint Force Headquarters-Cyber, 30 Jan 19.

[50] Hurlburt Field, 39th Information Operations Fact Sheet, 15 Aug, 2012, https://www.hurlburt.af.mil/About-Us/Fact-Sheets/Fact-Sheets/Article/204540/39th-information-operations-squadron/ (accessed 15 Dec 18).

[51] Secretary of the Air Force Public Affairs, "Air Force transfers cyber responsibility to ACC, 7 June 18, https://www.af.mil/News/Article-Display/Article/1544072/air-force-transfers-cyber-responsibility-to-acc/ (accessed 27 Feb 18).

[52] Billy Mitchell, "Air Force awards $121M in Enterprise IT-as-a-Service 'experiments', 27 Sep 18, https://www.fedscoop.com/air-force-eitaas-att-microsoft-121-million/ (accessed 15 Dec 18).

Bibliography

Air Force Organization, AFI 38-101, Figure 3.3, page 26, 31 Jan 17. https://static.e-publishing.af.mil/production/1/af_a1/publication/afi38-101/afi38-101.pdf, (accessed 20 Nov 18).

Air Force Policy Directive, Organization and Unit Designations, 24 May 18, https://static.e-publishing.af.mil/production/1/af_a1/publication/afpd38-1/afpd38-1.pdf, (accessed 15 Dec 18).

Air University, Air Force Cyber College, https://www.airuniversity.af.edu/CyberCollege/FMAC, accessed 15 December 2019

Bosko, David (Col), Air Force Cyber College, Advisor Meeting, 08 Feb 19

Career Field Education and Training Plan, Cyberspace Support, AFSC 3DXXX, 1 Sep 14. https://static.e-ublishing.af.mil/production/1/saf_cio_a6/publication/cfetp3dxxx/cfetp3dxxx.pdf (accessed 15 Dec 18).

Career Field Education and Training Plan, Cyber Warfare Operations, 15 Jul 18, https://static.e-ublishing.af.mil/production/1/saf_cio_a6/publication/cfetp1b4x1/cfetp1b4x1.pdf (accessed 15 Dec 18).

Cyber Penetration Tester Salaries in the United States, https://www.indeed.com/salaries/Penetration-Tester-Salaries (accessed 15 Dec 18).

Guidon, Payton, "US President Obama says cyber-security among greatest challenges", Independent, 13 Feb 14. https://www.independent.co.uk/news/world/americas/us-president-obama-says-cyber-security-among-greatest-challenges-10045950.html (accessed 15 Dec 18)

Headquarters Air Force Space Command, Mission Defense Team Concept - Draft, 2 Feb 16.

Higby, Patrick (Maj Gen) and Lt Col Steven Wieland, "Cyber Squadron Enabling Concept, 15 Mar 18.

Hurlburt Field, 39th Information Operations Fact Sheet, 15 Aug, 2012, https://www.hurlburt.af.mil/About-Us/Fact-Sheets/Fact-Sheets/Article/204540/39th-information-operations-squadron/ (accessed 15 Dec 18).

MacDougall, Arthur and Michael Meyers, "Pentagon faces array of challenges in retaining cybersecurity personnel", https://thehill.com/opinion/cybersecurity/391426-pentagon-faces-array-of-challenges-in-retaining-cybersecurity-personnel (accessed 15 Dec 18).

Mitchell, Billy, "Air Force awards $121M in Enterprise IT-as-a-Service 'experiments', 27 Sep 18, https://www.fedscoop.com/air-force-eitaas-att-microsoft-121-million/ (accessed 15 Dec 18).

Pomerleau, Mark, "Air Force begins to roll out special cyber defense teams", 27 Dec 18, https://www.airforcetimes.com/dod/air-force/2018/12/27/air-force-begins-to-roll-out-special-cyber-defense-teams/ (accessed 15 Dec 18).

Richer, Dennis and Jarvis Croff, "Mission Defense Team Military Utility Assessment Final Report", 05 Sep 18, Page 7.

Secretary of the Air Force Public Affairs, "Air Force transfers cyber responsibility to ACC, 7 June 18, https://www.af.mil/News/Article-Display/Article/1544072/air-force-transfers-cyber-responsibility-to-acc/ (accessed 27 Feb 18).

Seffers, George, "Cyber Resiliency a Feather in CROWS Flight Cap", The Cyber Edge, 1 Jul 18, https://www.afcea.org/content/cyber-resiliency-feather-crows-flight-cap (accessed 15 Dec 18).

Skinner, Robert (Maj Gen) Interview, Commander, 24th Air Force; Commander, Air Forces Cyber and Commander, Joint Force Headquarters-Cyber, 30 Jan 19.

Snyder, Don, James D. Powers, Elizabeth Anne Bodine-Baron, Bernard Fox, Lauren Kendrick, and Michael H. Powell, "Cybersecurity of Air Force Weapon Systems", RAND Corporation, 2015, RR1007. https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9800/RB9835/RAND_RB9835.pdf (accessed 15 Dec 18)

United States Air Force Military Pay Chart, https://militarybenefits.info/2018-military-pay-charts/ (accessed 15 Dec 18).

Williams, Martyn, "Joint Chiefs of Staff emails targeted by Russian hackers", 6 Aug 15. https://www.computerworld.com/article/2960806/malware-vulnerabilities/joint-chiefs-of-staff-emails-targeted-by-russian-hackers.html (accessed 15 Dec 18).