AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

BEYOND THE BARRIER: CYBER DEFENSE FOR C2ISR WEAPON SYSTEMS

By

S. ANDREW BAILEY, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Philip O. Warlick II, Colonel, USAF

9 March 2018

DISCLAIMER

Biography

Major S. Andrew "Loaf" Bailey entered the Air Force in 2004 after receiving his commission from the 305th ROTC Detachment at Louisiana Tech University. He is a senior Air Battle Manager with more than 1,600 total flying hours in the E-3B/C/G and E-2C aircraft including 257 combat hours. He completed Undergraduate ABM Training at Tyndall AFB, FL and is a graduate of the Navy Fighter Weapons School (TOPGUN). He has completed two assignments at Tinker AFB, OK including instructing at the E-3 Formal Training Unit as well as an exchange assignment as an instructor with the US Navy's Carrier Airborne Early Warning Weapons School at NAS Fallon, NV. He is currently a student at the Air Command and Staff College at Maxwell AFB, AL.

Acknowledgements

I would like to take the opportunity to thank all of the people who took time out of their busy schedules to offer suggestions or review the various revisions of this paper. Specifically, Lt Gen VeraLinn "Dash" Jameson, Brig Gen David "Trout" Gaedecke, Col Phil Warlick, Col Doug Hayes, Mr. Mike Ivanovsky, Mr. Rich Scher, Col William "Data" Bryant, Lt Col Mario "Z" Zuniga, Lt Col Kelly Shelton, Maj Rebecca Schmidt, Maj Nick Amato, Maj Brent "Goat" Roper, Capt Glen Pfieffer, and countless others who have provided background information, guidance, and/or feedback along the way. Most of all, I would like to thank my wife and daughter for their constant support and for allowing me to have the time necessary to complete this project.

Abstract

There has been a great deal of emphasis on cyber defense in recent years and several academic studies have been conducted which focused on protecting the Department of Defense Information Networks (DODIN). However, US weapon systems are also at risk from cyber-attack. Because of this risk, aircrew, maintenance, and intelligence personnel require increased training and the platforms require system upgrades to mitigate these vulnerabilities.

Aircrew and unit intelligence personnel should be aware of threats that face their weapon systems in cyberspace. Awareness would start by incorporating cyber threats, as well as friendly vulnerabilities, into initial weapon system training. Additionally, MAJCOM squadron, group, and wing commander courses should provide cyber threat training similar to the training the Le May center provides to general officers.

The Air Force has recognized the need to protect weapon systems in the cyber domain and has begun to establish Mission Defense Teams (MDT) to provide front-line cyber defense to operational wings. These programs are in their infancy, but there have been some success stories that can provide best practices for units as they bring their respective MDTs online. Some of these best practices include integration contracts established within the parent wing as well as attempts to standardize training.

Finally, weapon systems should reduce cyber vulnerabilities through hardware and software upgrades to already fielded assets. These include MDT toolkits made available for in-flight operations as well as installation of Intrusion Detection Systems (IDS) that would alert the operator that anomalies are present within the system. The operator could then review the affected systems and isolate that network and/or sensor in order to contain the vulnerability and minimize mission impact.

Table of Contents

List of Acronyms

ACC	Air Combat Command
ACNS	Air Control Networks Squadron
AIT	Aircrew Intelligence Training
ATC	Authority to Connect
ATO	Authority to Operate
AWACS	Airborne Warning and Control System
CAF	Combat Air Forces
C2ISR	Command, Control, Surveillance, and Reconnaissance
CCP	Cyber Campaign Plan
CNA	Computer Network Attack
CNE	Computer Network Exploitation
CO	Cyberspace Operations
CONOPS	Concept of Operations
CPT	Cyber Protection Team
CROWS	Cyber Resiliency Office for Weapon Systems
CS-I	Cyber Squadron Initiative
DCO	Defensive Cyberspace Operations
DDoS	Distributed Denial of Service
DODIN	Department of Defense Information Networks
FY	Fiscal Year
IC	Intelligence Community
ISO	Isochronal Inspection
LOA	Line of Authority
MAJCOM	Major Command
MDT	Mission Defense Team
MWS	Major Weapon System
OCO	Offensive Cyberspace Operations
OPE	Operational Preparation of the Environment
OS	Operating System
PPR	Pre-Planned Response
SAF/CIO	Secretary of the Air Force / Chief Information Officer
SMP	Strategic Master Plan
STAN/EVAL	Standards and Evaluations
TTP	Tactics, Techniques, or Procedures
USAF	United States Air Force
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command

Introduction

Cyber protection of weapon systems is necessary in order to avoid introducing unnecessary risk to multidomain command and control, a capability that will be critical in a battle against a peer competitor. Many systems are interconnected and a risk to one system is a risk to all systems participating in the network.[1] The interconnectedness of weapon systems rely on cyberspace and this domain is capable of affecting the physical domain.[2] The Air Force should use a three-pronged cyber defense initiative consisting of aircrew and intelligence operator training, improved Mission Defense Team (MDT) integration, and system hardware and/or software upgrades to ensure cyber domain protection for C2ISR assets. Doing so will help increase the resilience of our weapon systems and allow them to be safely interconnected to achieve the benefits of multidomain command and control.

This paper will begin by providing a background in the problem area as well as an explanation of the problem significance. There are multiple echelons within the Department of Defense Information Networks (DODIN) and this paper will provide an overview of the entities that support US weapon systems in the cyber domain. It will then discuss training options for intelligence and operations personnel to ensure adequate cyber protection. Next, the paper will identify Mission Defense Team (MDT) integration best practices. As more and more MDTs come online, these practices can ensure smooth integration within the respective wing. Finally, the paper will explore upgrade options that would make the system more resilient and resistant to cyber-attack or exploitation.

This paper assumes very little knowledge of cyber operations and intended for weapon system operators, maintenances, and intelligence professionals. Increased cyber awareness and vulnerability mitigation are important across the board – from the unit level specialist to the

Wing Commander. However, much of the literature assumes a great deal of knowledge in the subject area. The Problem Background and Problem Significance sections of this paper are intended to frame the problem for personnel, like myself, whose respective training and experience does not include a large amount of cyber operations. Furthermore, the paper was written for the Intelligence, Surveillance, and Reconnaissance (ISR) Research Task Force and therefore Command, Control, and ISR (C2ISR) assets are the focus; but the findings apply equally to other Air Force weapon systems.

Problem Background

News coverage of cyber attacks in Estonia and Georgia put the cyber domain in the national focus and highlighted the need to protect government and civilian networks from attack. In Estonia, a month-long barrage of Distributed Denial of Service (DDOS) attacks was used to shut down numerous government, media, and banking websites – causing the country to shut itself off from the Internet beyond its borders.[3] The attack used over one million computers from around the world employing software "bots" to attack the computer infrastructure.[4] This attack demonstrated the vulnerability from perpetrators in cyberspace.[5]

Developed countries and militaries employing sophisticated computer networking capabilities are especially vulnerable to computer network attacks (CNA) and computer network exploitation (CNE). According to a 2009 *Military Periscopes* Special Report, "the United States has been subjected to a constant stream of cyber assaults, from scans of military and government networks, to attacks aimed at stealing critical data… and the U.S. military takes the threat seriously."[6] The military established US Cyber Command as a sub-unified combatant command under US Strategic Command (USSTRATCOM) in 2009 and that command is in the final stages of upgrading to its own combatant command – US Cyber Command (USCYBERCOM).[7]

Additionally, the Air Force has pushed for a leading role and created the 24th Air Force at Lackland AFB, TX, which functions as the service's cyber component.[8]

Cyberwarfare can allow countries or non-state actors to threaten a stronger country without the need to build a comparable military. One concern of this type of warfare is the ability to attribute a CNA or CNE to a specific state or non-state actor.[9] Air Force leadership has recognized this characteristic of cyberwarfare and called for increased focus in the 2015 Strategic Master Plan (SMP). The plan states, "Many actors are emboldened by the perception of anonymity, particularly in the cyberspace domain." The SMP lists the following counter-threat focus areas:[10]

- Enhance integrated, multidomain ISR to detect, monitor, and attribute threats
- Increase the ability to share and release integrated, multi-domain ISR
- Develop new response options ranging across domains
- Improve our ability to apply levels of deterrence and coercion

The aforementioned focus areas require effective ISR in order to be successful. These capabilities are extremely important, but they are at risk unless the Air Force implements the three pronged weapon system cyber defense initiatives.

ISR can be a deterrence in and of itself by affecting the behavior of adversaries who believe (or know) they are under surveillance.[11] Deterrence is important, but the service also seeks to conduct Defensive Cyber Operations (DCO) in order to mitigate vulnerabilities as well as prevent attacks in progress. In fact, Joint Publication 3-12, *Cyberspace Operations (CO)* describes employing CO as the ability to gain freedom of maneuver for the joint force in cyberspace and to deny freedom of action to adversaries.[12] To accomplish this, JP 3-12 states that successful execution of CO requires "integrated and synchronized offensive, defensive, and DODIN operations, underpinned by effective and timely Operational Preparation of the Environment (OPE)."[13] Protection of C2ISR weapon systems falls within the DCO mission. JP

3-12 describes DCO as using "passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems." [14]

DODIN defense uses several different types of hardware and software in order to provide network situational awareness to cyber defenders. Network administrators can be overwhelmed with a large amount of separately derived information that can actually decrease situational awareness.[15] Some of these include hardware sensors, anti-virus software, Intrusion Detection Systems (IDS), network-mapping tools, and monitoring software.[16] Many of these tools use scripted responses to identify attacks and alert cyber defenders; however, network sensor information is often disjointed and the analysis of data can be overwhelming.[17] To counter this problem; researchers at the Air Force Institute of Technology have begun to incorporate computer automation to aggregate data from heterogeneous network sensors and software tools.[18]

Many networks rely on a host of sensors to identify intrusion and/or assess system performance since a change in performance could identify a CNA. Correlating security events from many different types of sensors can create a more holistic view and provide greater situational awareness.[19] Traditional IDSs monitor network traffic for cyber threats and notify the system administrator. Technological advancements now allow the IDS to fuse the network sensors with other sensors that monitor physical systems controlled by (or through) the network. An example would be a sensor that identifies an out of the ordinary gas leak that could cause an explosion if not recognized. The intent of the preceding CNA example could cause cascading effects on the operations located in proximity to the explosion. The example also highlights the

need for a cyber defense initiative like the three-pronged attack to ensure our systems are combat effective when called upon to defend the country.

Problem Significance

The majority of scholarly research in DCO focuses on protecting a computer network, but protecting military weapon systems can take advantage of the same principles. The Air Force has started to focus on weapon system protection due to the possible cyber impact on mission success.[20] Col William Bryant, the Deputy Air Force Chief Information Security Officer, wrote in *Air & Space Power Journal* that weapon systems are at risk of attack through cyberspace because "any physical connection that passes data or has an antenna with a processor behind it is a potential pathway for an attacker. Examples include maintenance and logistics systems, software-defined radios and datalinks, and other cyber physical systems that operators can connect to platforms, such as pods or weapons." [21] The recently created AF Cyber Resiliency Office for Weapon Systems (CROWS) is in the process of establishing a cyber campaign plan (CCP) to include cyber defense in the acquisition process for new weapon systems. However, the CCP also addresses vulnerabilities in previously fielded weapon systems and identifies the need for these steps by stating: [22]

> Many legacy weapon systems were developed during a period of cooperative networked environments with limited understanding of the cyber vulnerabilities of weapon systems and their impact on mission success. New weapons systems require design guidance to be cyber secure and resilient. In order to mitigate cyber threats, the AF must identify mission-critical cyberspace assets and ensure they can continue to operate in cyber-contested environments.[23]

The three primary areas of concern for the CCP are acquisitions, operations, and infrastructure. The remainder of this paper will focus on operations and the protection of previously fielded weapon systems. The CCP references the Cyber Squadron Initiative (CS-I)

which is led by the SAF/CIO. The CCP offers seven Lines of Authority (LoA) to help mitigate vulnerabilities; two of which protect fielded weapon systems. LoA 6, *Assess and Protect Fielded Fleet*, establishes a program to identify and mitigate cyber vulnerabilities across the entire enterprise. [24] LoA 7, *Provide Cyber Intelligence Support*, will help identify and mitigate adversary threats as well as deliver knowledge and products to the broader intelligence community. [25] This LoA will provide a baseline knowledge that unit level intelligence professionals can draw upon when implementing the training portion of the three pronged cyber defense initiative discussed later.

Air Combat Command (ACC) is the lead command for weapon system cyber protection and recently produced a pre-decisional draft Weapon System Assurance Service Provider (WASP) concept of operations (CONOPS) in response to the CCP's direction to mitigate vulnerabilities to fielded weapon systems. The CONOPS highlights the need for weapon system protection by stating, "The Air Force cannot "fly, fight, and win in air and space" without extending cyber defense to MWS [major weapon systems]." [26] The 24th Air Force is the Cyberspace Security Service Provider (CSSP) responsible for protecting the Air Force Network (AFNET) and ACC, via the WASP, is closing the gap and extending CSSP services to its

weapon systems as shown in Figure 1. Conversely, 25th Air Force has its own SSP that manages Intelligence Community (IC) assets.

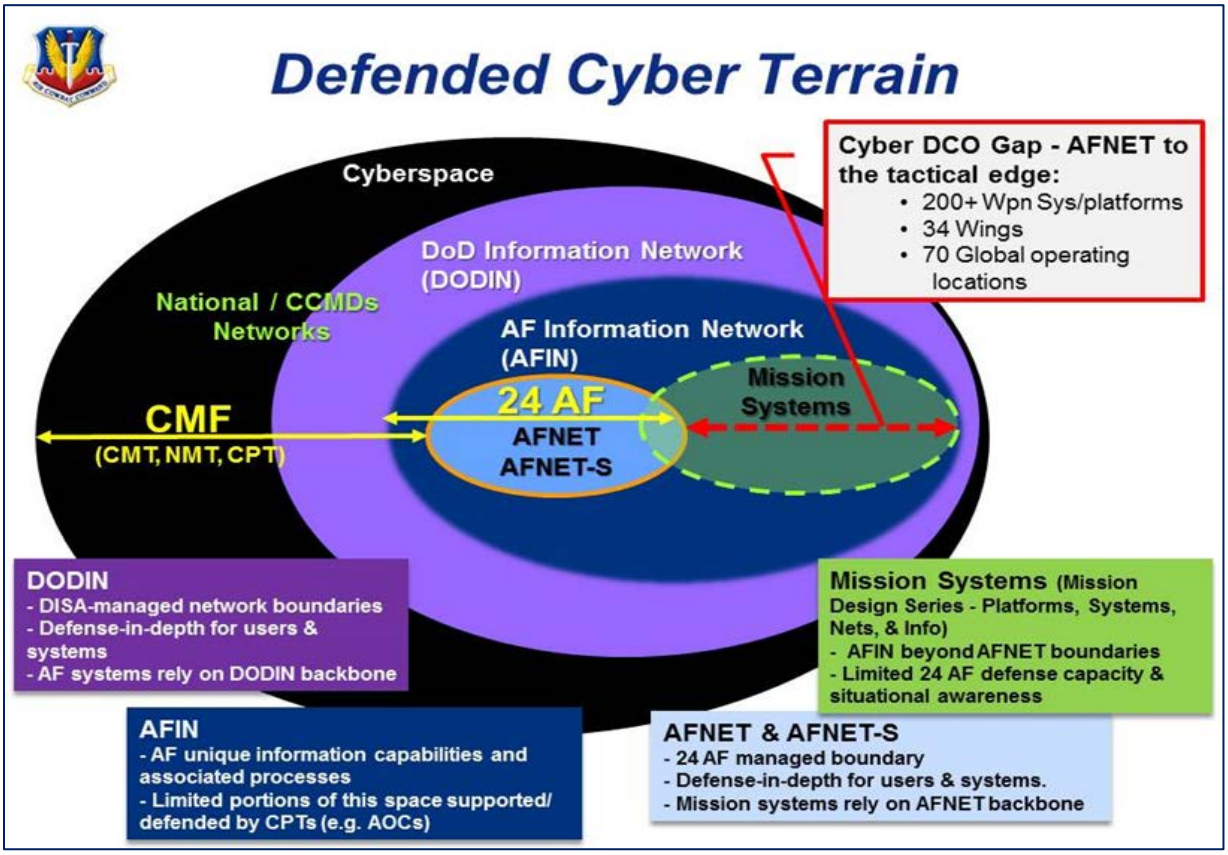

Figure 1: Cyber Terrain. Source: 2017 ACC WASP CONOPS (DRAFT)

The CONOPS establishes the organizational framework to ensure cyber protection down to the squadron level and provides *Figure 1* to represent the gap in DCO at the tactical edge (weapon systems.)

A Mission Defense Team (MDT) is the unit-level contact point for weapon system cyber protection and reports to the assigned Wing Commander. The MDT leverages mandates of the Cyber Squadron Initiative to convert communications squadrons into cyber operation squadrons in order to provide a "holistic cyberspace mission."[27] The ultimate goal of these MDTs is to provide mission assurance, which is defined as "a process to protect or ensure the continued function and resilience of capabilities and assets…critical to the performance of DoD Mission

Essential Functions in any operating environment or condition."[28] The MDT is the first line of defense for the weapon system and can coordinate with higher echelon Cyber Protection Teams (CPTs) for help. Some use the analogy of the MDT being the fire alarm monitor while a CPT is the firefighter brought in from the outside to fight the fire.[29] However, these are relatively new and have not fully developed tactics, techniques, and procedures (TTPs). Additionally, weapon system operators and maintenance personnel are not fully aware of cyber threats to their respective weapons systems and are in need of training to close the information gap. The Air Force can overcome these challenges using the three-pronged cyber defense initiative for previously fielded weapon systems that consists of training, MDT integration, and system upgrades.

Training

The Air Force Chief of Staff sponsored a study in 2013 where the Air Force Research Institute reviewed training and development of USAF cyber forces. The study recommended the establishment of "a short course in cyber hygiene with course objectives of achieving analysis-level understanding of common cyber threats as part of all officer and enlisted accessions programs."[30] Carnage Mellon's *Insider Threat Blog* describes cyber hygiene as "the most common baseline cyber practices that… organizations use in their cybersecurity programs."[31] The accessions level training recommendation would help ensure the culture of cyber awareness within the force by providing basic cyber hygiene skills to all personnel. This training can help provide a reason behind seemingly annoying user protocols. Aviators may be more likely to follow required procedures if they understand the vulnerability caused to the DODIN if they cut corners. Even though this was a good step, the training need not stop at the accessions level.

The annual Air Crew Intelligence Training (AIT) program should incorporate cyber threats into academics and testing. AIT ensures crewmembers have a solid understanding of the adversary's capabilities and the way in which those capabilities and limitations drive tactical employment, and the same concept should hold true for cyber threats. The aircrew and unit intelligence personnel should be aware of threats that face the weapon systems in the cyber realm. Training can start by incorporating cyber threats, as well as friendly vulnerabilities, into initial weapons system training. The academic phase would be an ideal time to introduce cyber threats and vulnerabilities to new aircrew and would help bring about a paradigm change by instilling a basic understanding of cyber risk, leading to mitigation techniques that are more diligent. Understanding why a mitigation step is necessary may increase the likelihood that the operators will comply with the guidance. Additionally, understanding the "why" may have a positive impact on cyber hygiene.[32] Aircrew may not even be aware of the vulnerabilities inherent in a system built before cyber exploitation was a concern. These training programs can also be implemented at various leadership levels.

Senior leaders within the operational squadrons, groups, and wings would benefit from increased cyber awareness training opportunities. The Le May Center currently offers a two-day Cyberspace Operations Executive Course for senior flag officers.[33] However, MAJCOMs should take some of the key concepts regarding the importance of cyber hygiene within an organization and present them during respective squadron, group, and wing commander preparation courses currently offered. Unit leadership who understand cyber vulnerabilities can help create a culture of good cyber hygiene within their respective units.

Front line operators would also benefit from additional training opportunities. In his Air War College paper, Lt Col Jason Settle advocates, "Growing a dedicated cyber course" in order

to help instill a "culture of cyber awareness".[34] He goes on to suggest that a unit like the 57th Adversary Tactics Group at Nellis AFB, NV would be well suited to develop such a course and provide academic courses and/or mobile training teams.[35] These opportunities should be used to train operators and aircrew on cyber operations basics. Once equipped, the operator would be a valuable resource in assessing system vulnerability since they are well versed in the operation of their respective weapon system. The 57th threat academics are a valuable resource to operators to help understand the enemy they may face and cyber threats should be no different. Once the educational and training cornerstone is established, the next portion of the three-pronged initiative is to improve MDT integration within its respective combat wing.

Integration

The MDT was designed to be the front line cyber defense entity for weapon systems, but the program is still in its infancy. Several of these teams have been set up in newly configured cyber squadrons and are in the process of developing TTPs. This section will offer some best practices developed by the 552d Air Control Networks Squadron (a pathfinder unit) which was the first to connect, using a temporary Authority to Operate (ATO), a MDT to an aircraft. Other MDTs exist around the Combat Air Forces (CAF), but most are working through the process to receive the ATO from their respective representative. The issue that is causing delays is due to a concern about the MDT's ability to make changes to the connected weapon system's software configuration. A concern at the Air Force Headquarters staff level is that an inexperienced MDT operator can cause damage to the weapon system while performing his/her defense mission and therefore information officers must be cautious when granting ATOs.[36] However, MDTs will continue to mature and will continue to demonstrate their competence, which in turn will build trust with granting authorities.

A unique hurdle for IC platforms is the need to obtain an ATO from the IC Authorization Official. For example, the RC-135 Rivet Joint has not yet obtained the required IC ATO and thus cannot employ their MDT toolkits. The MDT toolkit would have access to equipment used by national intelligence systems and thus must be approved for use by the IC's authority at 25th Air Force. The challenge is that two separate ATOs are necessary. An ATO for the mission system requires 24th Air Force approval, while 25th Air Force must provide approval for any of their networks and/or systems that interface with the MDT via the onboard mission computer. This approval process is necessary in order to allow networks to fuse information, but it is an arduous process and future studies may be necessary to make the process more efficient.

Once ATO approval occurs, wings will need to develop an implementation plan. The 552d ACNS found it helpful to develop familiar terms to enable better dialogue between cyber defenders, operators, and maintenance personnel. For example, a "Sortie" is the process of connecting the MDT toolkit to an aircraft for a "scan". The ACNS conducts mission planning and debriefing on each sortie, which is in line with the aircrew's battle rhythm. Once common terms were established, the 552d Air Control Wing incorporated the MDT into the scheduling process. Each week, MDT representatives attend the 552d Operations Groups' scheduling meeting along with operations squadron and maintenance representatives. The group developed the process of conducting MDT sorties in conjunction with Isochronal Inspections (ISO) and refer to the process as a "Cyber ISO." This allows access to the aircraft while maintenance personnel are performing inspections, which reduces the amount of time the aircraft is out of the flying lineup.

A respective wing can tailor the MDT's crew composition for a specific mission because a higher authority does not dictate it. The 552d also utilizes a mix of cyber operators,

maintenance personnel, and mission system operators to staff the MDT. This allows a full range of knowledge and experience to ensure optimal employment of the toolkit. Follow on plans and recommendations include developing a Standards and Evaluations (STAN/EVAL) process for MDT crews. The intent is to develop "crew positions" within the MDT and a training program to ensure a baseline knowledge and experience prior to conducting MDT sorties unsupervised. This training will also provide ATO granting authorities with assurance that MDT operators have proved an ability to use the system properly during a STAN/EVAL examination.

Another area for improvement of the MDT is to integrate the whole weapon system defense structure into that of the IC, which has been involved in defensive cyber operations for many years. MDTs and CPTs rely on the WASP to obtain new threat libraries and to push system issues and anomalies up for further analysis and dissemination. In order to ensure the most up to date information, the CONOPs require updates to ensure WASP coordination with the IC is required and it meets IC Directive 503 (cyber compliance) requirements.[37] Doing so would ensure platforms within ACC and the IC meet all the certification requirements from both communities. Working to create MDTs that mirror the capability of USCYBERCOM CPTs would aid standardization, as well as ensure the most up to date threat information is available to the lower echelon teams. Training and integration can be affected in the relatively short term, but the next step is to make upgrades to existing weapon systems to make them more cyber resilient.

Upgrades

Weapon systems provide a unique challenge in terms of DCO as it is often a conglomeration of different types of sensors. Some of these sensors operate with one another and some are stand-alone. Some of the systems consist of off the shelf technology or proprietary

systems that developed thirty years or more ago and not fully integrated into the system's network. These multiple systems each present their own cyber vulnerabilities that require risk mitigation initiatives.

Weapon systems can also apply some traditional network protection methods. The first step would be to utilize the MDT Toolkit connected to the weapon system on operational and training missions. The toolkit could monitor the system during the mission and allow the data to be collected for post mission analysis. The crewmember running the software would be able to take action if the toolkit found any anomalies. Since the crewmember would not necessarily be a cyber operator, they could have a set of preplanned responses (PPR) to use. Detailed planning, threat analysis, and system design knowledge would be required to develop these PPRs, but could prove invaluable for any DCO action needed during the mission. The objective of these PPRs is to allow a graceful degradation of the weapon system versus an instant soft kill. A thorough understanding of the system limitations and threat tactics are necessary to prevent an over-reaction to an attack that would likely create the effect the enemy seeks.

The MDT Toolkit is a starting point in terms of DCO during operations, but the next step would be to incorporate Intrusion Detection Systems with heterogeneous sensors into the weapons system. This would be a massive undertaking, as it would involve obtaining funding for major modifications to the weapon system. However, there are critics to this approach who argue that these systems will not work because they attempt to predict the future based on the past. The argument assumes that all attacks use completely new code that is not detectable by an IDS. Senior leadership within the communities would be required to assess the risk vs reward ratio when considering such an option and this calculation could prove to be too great of an investment for the given risk. Because these systems are currently funded, it can be inferred that

senior leadership sees technology such as IDS and MDTs as a viable solution for the near future. It is true these will not prevent all attempts to exploit US systems, but they have the potential to increase the amount of time and resources a would-be opponent must expend to do so. The aforementioned system upgrades provide near term solutions that are viable options for fielding, but the Air Force also needs long-term solutions.

The long-term goal is to create more secure systems. Doctor Kamal Jabbour of the Air Force Research Laboratory, during a speech given to the Air Force Cyber College, discussed the possibility of producing mission systems that are more resilient. The idea would be to write system code that can account for "untrusted system components, operators, and data."[38] According to Dr. Jabbour, AFRL tested this concept on a small scale already and large-scale expansion is feasible.[39] In fact, Dr. Jabbour referenced the Boeing 787 and the steps taken to ensure data integrity within the system, even with untrusted components.[40]

Another way to protect assets is to develop systems that do not rely on a traditional operating system (OS). Rather, the Air Force should develop systems that use a stripped down version of an OS such as Linux.[41] The kernel would be void of any root or administrator access and only preprogrammed applications would be able to be run. Instead of patching or updating software on the system, the whole operating system, with embedded software, would be updated when needed and would take away many of the vulnerabilities of a system. According to Rich Scher of Microsoft Azure, the systems will always have some vulnerability, but the goal is to require threat actors to "put forth tremendous resources, massive intelligence collection efforts, and risk attribution in order to produce an attack."[42] These steps would also reduce the risk of a "zero day attack" where malware has been loaded onto the system that "exploits a vulnerability that as of yet has no formulated solution."[43] This argument may seem to be contrary to the push

for open architecture designs, but can be overcome by solid planning efforts. The idea is to harden the system itself, but this does not limit the system from external updates. The owning cyber squadron would be able to upload completely new disk images containing all the software and coding needed to complete a mission. It would remove the ability to change underlying operating system parameters during a mission while not precluding system updates.

Dr. Jabbour recently proposed that future systems would have software built only to support a specific mission that is an even more secure option than the previous Boeing 787 example. He described fielding a "blank" Unmanned Aerial Vehicle (UAV) that had no operating system or code installed. Prior to each mission, operators would create a mission profile and program the UAV for the mission. The programming would include mission parameters, but it would also include an operating system and all associated mission software, written in a coding language that "did not exist ten minutes prior."[44] This would minimize the risk of cyber-attack and increase mission assurance.

Dr. Jabbour does not claim this system would be "unhackable", however he said it would provide mission assurance for a specified period. He went on to advocate the need for senior leaders to think of mission assurance as finite. Leaders and developers must build systems that can withstand cyber-attack for a specified amount of time in order to develop realistic assumptions. Mission assurance is in need of a paradigm shift since a determined adversary will most likely find a way to exploit our technology. However, we can build systems that can withstand a contested environment for a period and "time" is the domain that we must focus on in the future. Col William D. Bryant, the Deputy Air Force Chief Information Security Officer echoes this view by stating, "Cyberspace operators need to move beyond the concern of how to best secure their systems against attack to focus on how to design their system to continue

working after their defenses fail."[45] This would include building heterogeneous networks incorporating multiple operating systems to help improve the chance of mission assurance even if in a degraded state. Doing so balances resiliency and efficiency and allows leaders an opportunity to calculate risk assessments.

Finally, hardware and software upgrades may be able to reduce risk, but they should not do so at the expense of severe impact on system performance. What good is a secure system that is combat ineffective due to multiple layers of security protocols that the hardware was not designed to support? System performance considerations are necessary when developing modifications to existing weapons systems and ensure the platform has adequate computing power to enable continued operations.

Conclusion

Although Air Force weapon systems are regarded as the tip of the spear in traditional warfare, they also represent an inherent vulnerability to the larger C2ISR network. Many of our platforms have connections to multiple data sources that present a ready target for attacks with the intent to disrupt the overall network. The only way to allow multidomain data fusion is to ensure we do our due diligence to defend the networks at all levels, especially the major weapon systems. The Air Force should implement a combination of aircrew and intelligence as a short-term solution and can expand existing training venues extended to a wider audience across multiple levels. MDT integration will continue to improve and cyber operators are codifying TTPs, which will make the entire enterprise more effective. These pathfinder units are making great strides each day to ensure mission assurance. Additionally, close integration with the IC will also ensure the most current information is available at the front line. Furthermore, system upgrades may be able to reduce cyber-attack risk while still allowing effective combat

employment. The upgrades include short, near, and long-term solutions ranging from buying more MDT toolkits to producing system with blank software suites built for a specific mission. The three lines of effort in this paper will help achieve the cyber campaign plan's goal of protecting fielded weapon systems and achieve a level of mission assurance that is required of the weapon systems respective combatant commanders.

Endnotes

1 Office of the Director of National Intelligence, *Intelligence Community Directive Number 503: Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*, 15 September 2008. 3

2 Col William D. Bryant, "Mission Assurance through Integrated Cyber Defense," *Air & Space Power Journal* (Winter 2016): 5.

3 Cushman, Jeremiah, "Foreign Hackers Focus On Military Targets," Military Periscope Special Reports, 1. Military & Government Collection, (August 2009), EBSCOhost. 2.

4 Ibid.

5 Ibid.

6 Ibid.

7 U.S. Strategic Command, "U.S. Cyber Command (USCYBERCOM), 30 September 2016, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/

8 Cushman, "Foreign Hackers Focus On Military Targets", 2.

9 Ibid.

10 Office of the Secretary of the Air Force, Strategic Master Plan, May 2015. 38.

11 "USAF Strategic Master Plan", news release, Secretary of the Air Force Public Affairs, 21 May 2015, http://www.af.mil/Portals/1/documents/Force%20Management/Strategic_Master_Plan.pdf?timestamp=1434024300378 41.

12 Joint Publication 3-12 (R), Cyberspace Operations, 5 February 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf. I-6.

13 Ibid. II-2.

14 Ibid.

15 Capt Raulerson, Evan L., "Modeling Cyber Situational Awareness Through Data Fusion," Masters Thesis AFIT-ENG-13-M-41 (Air Force Institute of Technology: Wright –Patterson Air Force Base, OH), 2013. 19.

16 Ibid. 5.

17 Ibid.

18 Ibid.

19 Zuech et al., "Intrusion detection and Big Heterogeneous Data: a survey," Journal of Big Data 2, no. 3 (2015): https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ve

d=0ahUKEwixvKqk2I_WAhVE0oMKHZ-bDGgQFggrMAA&url=https%3A%2F%2Fjournalofbigdata.springeropen.com%2Farticles%2F10.1186%2Fs40537-015-0013-4&usg=AFQjCNGVj7_14pG-Pg1xesj9g4aUBj6UZg. 1.

20 Air Force Cyber Resiliency Office for Weapon Systems, AFLCMC/EN-EZ, Air Force Acquisition Cyber Campaign Plan Charter for Weapon System Resiliency, 30 Jun 2017, (emailed from HAF/A8X Cyber Dominance Panel.) 4.

[21] Col William D. Bryant, "Mission Assurance through Integrated Cyber Defense," *Air & Space Power Journal* (Winter 2016): 7.

22 Ibid.

23 Air Force Cyber Resiliency Office for Weapon Systems, Air Force Acquisition Cyber Campaign Plan Charter for Weapon System Resiliency. 1.

24 Ibid. 16.

25 Ibid.

26 Air Combat Command, *Weapon System Assurance Service Provider (WASP) Concept of Operations (CONOPS) – Pre Decisional Draft*, 28 July 2017, (emailed from HAF/A8X Cyber Dominance Panel.) 1.

27 *Cyber Squadron Initiative: Functional Concept* Draft Version 3. March 2017 (emailed from 752 OSS/ADO.)

28 Air Combat Command, *Weapon System Assurance Service Provider (WASP) Concept of Operations (CONOPS) – Pre Decisional Draft*, 28 July 2017, (emailed from HAF/A8X Cyber Dominance Panel.) 5.

29 Lt Col Kelly Shelton, Commander, 552 Air Control Networks Squadron, Tinker AFB, OK, interview, 16 Nov 17.

30 Panayotis A. Yannakogeorgos and John P. Geis II, The *Human Side of Cyber Conflict: Organizing, Training, and Equipping the Air Force Cyber Workforce (Montgomery AL: Air University Press, 2016, xv).*

31 Charles M. Wallen, "Cyber Hygiene: 11 Essential Practices," *Insider Threat (Blog)*, Software Engineering Institute: Carnegie Mellon University, 15 Nov 2015, https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html

32 Lt Col Mario Zuniga, Deputy Commander, 552 Operations Group, Tinker AFB, OK, interview, 16 Nov 17.

33 Yannakogeorgos and Geis, The *Human Side of Cyber Conflict, 173.*

34 Lt Col Jason R. Settle, "Cyber Threat Awareness for the Warfighter," (Air War College: Montgomery AL), 2016. 7.

35 Ibid.

36 Hayes, Col Douglas P., HAF/A2, Chief Information Officer, HQ DoD, Washington, D.C., interview, 7 March 2018.

37 Office of the Director of National Intelligence, Intelligence Community Directive Number 503: Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation, 15 September 2008. 2.

38 Dr. Kamal Jabbour, Senior Scientist, Information Assurance, Air Force Research Laboratory. Address. Air Force Cyber College, Maxwell AFB, AL, 15 Nov 17.

39 Ibid.

40 Ibid.

41 Richard Scher, Chief Information Security Officer for High Security Clouds, Microsoft Azure, San Antonio, TX, interview, 20 Nov 17.

42 Ibid.

43 Maj Brent D. Roper, 752 OSS/ADO, Tinker AFB, OK, email to author, 29 Nov 17.

44 Dr. Kamal Jabbour, Senior Scientist, Information Assurance, Air Force Research Laboratory. Address. Air Force Cyber College, Maxwell AFB, AL, 8 Feb 18.

45 Col William D. Bryant, "Resiliency in Future Cyber Combat," (working book chapter emailed to author, Washington DC, Headquarters Air Force, 2018). 10.

Bibliography

Air Combat Command, Weapon System Assurance Service Provider (WASP) Concept of Operations (CONOPS) – Pre Decisional Draft, 28 July 2017, (emailed from HAF/A8X Cyber Dominance Panel.)

Air Force Cyber Resiliency Office for Weapon Systems, AFLCMC/EN-EZ, Air Force Acquisition Cyber Campaign Plan Charter for Weapon System Resiliency, 30 Jun 2017, (emailed from HAF/A8X Cyber Dominance Panel.)

Bender, Lt Gen William J. and Col William D. Bryant, "Assuring the USAF Core Missions in the Information Age," *Air & Space Power Journal* (Fall 2016): 4-8.

Brant, Col William D., "Defending the Virtual Walls: Active Cyber Defense of Weapon Systems," *ITEA Journal of Test and Evaluation* 37, no. 3 (September 2016): 236-240.

Bryant, Col William D., "Mission Assurance through Integrated Cyber Defense," *Air & Space Power Journal* (Winter 2016): 5-17.

Bryant, Col William D., "Resiliency in Future Cyber Combat," (working book chapter, Washington DC, Headquarters Air Force, 2018): 10.

Bryant, Col William D., "Suring the Chaos," *Joint Forces Quarterly* 88 (1st Quarter 2018): 28-33.

Coleman, Jillian, "The Future of Cybersecurity," The Tinker Take Off, 21 October 2016. http://journalrecord.com/tinkertakeoff/2016/10/21/the-future-of-cybersecurity/

Cyber Squadron Initiative: Functional Concept Draft Version 3. March 2017 (emailed from 752 OSS/ADO.)

Courville, Lt Col Shane P., "Air Force and the Cyberspace Mission: Defending the Air Force's Computer Network in the Future," Occasional Paper No. 63 (Air War College: Maxwell AFB, AL) 2007.

Cushman, Jeremiah, "Foreign Hackers Focus On Military Targets," Military Periscope Special Reports, 1. Military & Government Collection, (August 2009), EBSCOhost

Daley, Tom, "Integration into Cyber Security Management System," Final Technical Report AFRL-IF-RS-TR-2005-353 (Air Force Research Laboratory: Rome, NY) 2005.

Gaedecke, Col David, SAF/CIO, A3C/A6C, HQ DoD, Washington, D.C., to the author, e-mail, 31 August 2017.

Hayes, Col Douglas P., HAF/A2, Chief Information Officer, HQ DoD, Washington, D.C., interview, 7 March 2018.

Jabbour, Dr. Kamal, Senior Scientist, Information Assurance, Air Force Research Laboratory. Address. Air Force Cyber College, Maxwell AFB, AL, 15 Nov 17.

Jabbour, Dr. Kamal, Senior Scientist, Information Assurance, Air Force Research Laboratory. Address. Air Force Cyber College, Maxwell AFB, AL, 8 Feb 18.

Joint Publication 3-12 (R), Cyberspace Operations, 5 February 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

Lyons, 2 Lt Katherine B., "A Recommender System in the Cyber Defense Domain," Masters Thesis AFIT-ENG-14-M-49 (Air Force Institute of Technology: Wright –Patterson Air Force Base, OH), 2014.

Mixon, Col Clinton, Commandant, Air Force Cyber College, Maxwell AFB, AL, to the author, e-mail, 13 September 2017.

Moises Sudit et al., "High Level Fusion in the Cyber Domain," Final Technical Report AFRL-IF-RS-TR-2005-376 (Air Force Research Laboratory: Rome, NY) 2005.

Office of the Director of National Intelligence, *Intelligence Community Directive Number 503: Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*, 15 September 2008.

Painter, LCDR Matthew, Student, Air Command and Staff College, Maxwell AFB, AL, to the author, e-mail, 25 September 2017.

Pfieffer, Capt Glen, Chief, Airborne Networks Requirements, Tinker AFB, OK, to the author, e-mail, 22 September 2017.

Raulerson, Capt Evan L., "Modeling Cyber Situational Awareness Through Data Fusion," Masters Thesis AFIT-ENG-13-M-41 (Air Force Institute of Technology: Wright –Patterson Air Force Base, OH), 2013.

Rizer, Lt Col Scott W., "Sun Tzu in Cyberspace," OMB No. 0704-0188 (Air War College: Maxwell AFB, AL) 2008.

Roper, Maj Brent D., 752 OSS/ADO, Tinker AFB, OK, email to author, 29 Nov 17.

Scher, Richard, Chief Information Security Officer for High Security Clouds, Microsoft Azure, San Antonio, TX, interview, 20 Nov 17.

Settle, Lt Col Jason R., "Cyber Threat awareness for the Warfighter," (Air War College: Maxwell AFB, AL) 2016.

Shelton Lt Col Kelly, Commander, 552 Air Control Networks Squadron, Tinker AFB, OK, interview, 16 Nov 17.

U.S. Strategic Command, "U.S. Cyber Command (USCYBERCOM), 30 September 2016, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/

"USAF Strategic Master Plan", news release, Secretary of the Air Force Public Affairs, 21 May 2015, http://www.af.mil/Portals/1/documents/Force%20Management/Strategic_Master_Plan.pdf?timestamp=1434024300378.

Wallen, Charles M., "Cyber Hygiene: 11 Essential Practices," *Insider Threat (Blog),* Software Engineering Institute: Carnegie Mellon University, 15 Nov 2015, https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html

Welsh III, Gen Mark A., "Global Vigilance, Global Reach, Global Power for America," Air and Space Power Journal 28, no. 2 (March – April 2014): http://www.airpower.maxwell.af.mil/digital/pdf/articles/2014-Mar-Apr/SLP-Welsh.pdf

Zuech et al., "Intrusion detection and Big Heterogeneous Data: a survey," Journal of Big Data 2, no. 3 (2015): https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwixvKqk2I_WAhVE0oMKHZ-bDGgQFggrMAA&url=https%3A%2F%2Fjournalofbigdata.springeropen.com%2Farticles%2F10.1186%2Fs40537-015-0013-4&usg=AFQjCNGVj7_14pG-Pg1xesj9g4aUBj6UZg

Zuniga, Lt Col Mario, Deputy Commander, 552d Air Control Group, Tinker AFB, OK, interview, 16 Nov 17.