

Pivoting to Weapon System Cyber Defense

By

Trevor R. Groves, Capt, USAF

A Research Report Submitted to the Faculty

Advisor: Sarah E. Kinzer, Lt Col, USAF

December 4, 2021

"Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Air University, the United States Air Force, the Department of Defense, or any other US government agency."

Abstract

There has been a tremendous amount of focus and effort spent on cyber defense internal to service component's business systems inside the DoD's Fiscal Year 2022 budget.¹ Additionally, the Air Force has been trying to implement *Pathfinders* in Cyberspace Squadrons and focus more on Defensive Cyberspace Operations (DCO) capabilities since 2016.² In March 2020, the Secretary of the Air Force and Chief of Staff signed the Cyber Squadron-Initiative Program Action Directive (CS-I PAD), enabling Communication Squadrons to transform into Cyberspace Squadrons and operate with integrated cyber defenses using Mission Defense Teams (MDT). These MDTs are charged with providing mission assurance to installation commander's weapon systems. Finally, I propose that we must to pivot immediately into a more focused and funded approach at fielding new cyberspace squadrons faster with strategic integrated deterrence and cooperation against rising adversaries.

¹ "DoD IT Cyberspace Activities and Budget Overview." *DoD CIO*, 2021. June 8. https://www.cape.osd.mil/content/SNAPIT/files/FY22/DoD%20Budget%20Overview_FY22PB_DoD-CIO_DCIO-RA-RPB_20210607.pdf.

² Staff Sgt McRae, Jannelle. "Cyber Squadron Initiative: Arming Airmen for 21st Century Battle." *United States Air Force*, 2017. May 5. <https://www.af.mil/News/Article-Display/Article/1174583/cyber-squadron-initiative-arming-airmen-for-21st-century-battle/>.

When was the last time you had your social media accounts hacked, your identity stolen, or witnessed a gas shortage because of a cyber-attack on a pipeline? The Air Force must realize we are not in a peacetime situation in cyberspace, prioritize and accelerate funding within DCO, and pivot Communications Squadrons from a Communications Service Provider (CSP) role to a Cyberspace Squadron using MDTs to provide mission assurance and cyber defense of core weapon systems.

We are constantly under attack and are not in a peacetime continuum having to beat adversaries out of our systems and implement measures to decrease our risk posture.³ Over the past year our nation has been at the bleeding edge with cyber criminals taking down pipelines⁴, nation-state actors reading our emails⁵ and even inserting sophisticated supply-chain level malware within network monitoring software.⁶

Examining deep within the landscape of the Air Force weapon systems' information technology, we tend to get insights to that show a large number of vulnerabilities and can extrapolate potential mission risks that are not properly defended.⁷ Interestingly enough, one misconfigured device or crack in the security posture is simply a toe-hold needed to infiltrate an

³ "Significant Cyber Incidents." *Center for Strategic and International Studies*, 2021. December 4. <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>.

⁴ Williams, Brad D. "Colonial Pipeline Cyberattack Follows Years of Warnings." *Breaking Defense*, 2021. May 10. <https://breakingdefense.com/2021/05/pipeline-cyberattack-follows-years-of-warnings/>.

⁵ Temple-Raston, Dina. "China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying." *NPR*, 2020. August 26. <https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying>.

⁶ Williams, Jake. "What You Need to Know About the SolarWinds Supply-Chain Attack." *SANS*, 2020. December 10. <https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/>.

⁷ "Cybersecurity Framework." *NIST*, 2021. December 4. <https://www.nist.gov/cyberframework>.

entire installation.^{8 9} Today we have administrators operating mission systems across undefended and non-monitored networks within the Air Force Network (AFNet). Imagine if the desired Blue Force effects of our National Instruments of Power can be denied, disrupted, degraded, destroyed, or manipulated (D4M) because of a pilot module system vulnerability? This “system” operating inside the Air Force Information Network typically has no oversight or traditional cyber defender inside their accredited encrypted boundaries.¹⁰

The oversimplified scenario alludes to the constant issue of who’s watching the internal weapon system’s boundaries. Do Accrediting Officials and operational Commanders truly understand the risk of operating a weapon system with a critical vulnerability that the enemy has previously exploited? Our Air Force weapon systems’ ecosystem is just as connected and administrated as any other commercial network through multiple platforms but lacks the prioritization and funding it deserves in defensive cyberspace.

Recently, the Department of Defense (DoD) published the Fiscal Year 2022 Defense Budget that outlines many cyber expenditures and strategic focus areas¹¹. While there was an overall decrease in Air Force manning due to Space Force divestitures and lack of priority on the Cyber Squadron Initiative, cyber operations remain a continued focus area while the end strength has been reduced.¹² “Looking forward, the Services will focus growth in advanced capabilities like cyber, electronic warfare, and special operations, which are needed to contend with our most

⁸ Heller, Michael. “Pentagon Hack Possible due to Bad Vulnerability Management.” *TechTarget*, 2017. February 2. <https://www.techtarget.com/searchsecurity/news/450412235/Pentagon-hack-possible-due-to-bad-vulnerability-management>.

⁹ Williams, Brad D. “NSA Renews Focus On Securing Military Weapons Systems Against ‘Capable’ Rivals.” *Breaking Defense*, 2021. October 7. <https://breakingdefense.com/2021/10/nsa-ups-focus-on-securing-weapons-systems-amid-capable-multipolar-rivals/>.

¹⁰ Ibid

¹¹ “DoD IT Cyberspace Activities and Budget Overview.” *DoD CIO*, 2021. June 8. https://www.cape.osd.mil/content/SNAPIT/files/FY22/DoD%20Budget%20Overview_FY22PB_DoD-CIO_DCIO-RA-RPB_20210607.pdf.

¹² Ibid., 8

capable, potential adversaries and fulfill the Interim National Security Strategic Guidance...¹³”.

This strategic guidance must focus Commanders on proper spending and support to get after critical cyber dependencies, not only business systems but weapon systems used for strategic integrated deterrence.

In accordance with the CS-I PAD¹⁴, MDTs are cut from existing manpower while administratively and operationally assigned to installations, in order to enable local commanders with an accurate cyber risk picture.¹⁵ Commanders armed with a precise cyber risk picture are able to determine the appropriate mission assurance level required to operate these weapon systems. The systemic and programmatic approach to using existing manning under the CS-I PAD is weighed heavily on Communications Squadron Commanders to transform teams of people through a lengthy process that remains largely unfunded and disapprovingly undervalued.

Commanders must accept a larger risk to traditional CSP roles for the installations and transition over to employing an MDT organically. Communication Squadrons provide bases with support their Wing Commanders and Major Commands mission sets. From telephony, printers, computers, communication security and even SharePoint, the Communication Squadron is interconnected to every part of the base. They know what’s connected and where it communicates when monitoring their base networks. This is of strategic value and importance when creating an MDT to characterize the mission terrain in cyberspace.

¹³ “DoD IT Cyberspace Activities and Budget Overview.” *DoD CIO*, 2021. June 8. https://www.cape.osd.mil/content/SNAPIT/files/FY22/DoD%20Budget%20Overview_FY22PB_DoD-CIO_DCIO-RA-RPB_20210607.pdf.

¹⁴ Staff Sgt McRae, Jannelle. “Cyber Squadron Initiative: Arming Airmen for 21st Century Battle.” *United States Air Force*, 2017. May 5. <https://www.af.mil/News/Article-Display/Article/1174583/cyber-squadron-initiative-arming-airmen-for-21st-century-battle/>.

¹⁵ Underwood, Kimberly. “Defensive Teams Help Protect the Air Force Mission.” *AFCEA*, 2019. October 1. <https://www.afcea.org/content/defensive-teams-help-protect-air-force-mission>.

Col Bryant, the Deputy Air Force Chief Information Security Officer in 2016, wrote in the *Air & Space Power Journal* that our weapon systems are at a great 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.”¹⁶ We must have local cyber defenders intimately familiar with the weapon systems and understand where the enemy would target. It is critical that we must accomplish our core cyber missions to Identify, Protect, Detect, Respond, and Recover, because the fastest cyber adversaries out there are Russian actors with the ability to compromise and maneuver within 18 minutes and 49 seconds in cyberspace.¹⁷

Lastly, knowing the time our adversaries take to compromise systems can give us a couple solutions and creative ideas we can implement at little to no cost and right away. We must prioritize network connected weapon systems with integrated cybersecurity tools to lend a quick win solution for MDTs that do not have operational toolkits yet. Typically, Information System Security Owners (ISSO) and Information System Security Managers (ISSM) have full access to these networks but lack manning for 24/7 monitoring. MDTs should be given at a minimum read-only access to these network monitoring tools to provide the much need manpower and expertise required to watch these platforms.

Integrating MDTs using the weapon system’s cybersecurity tools with operational Commanders provide a foundational degree of cooperation. Connecting their ISSOs and ISSMs with an MDT will also lower risk to inadvertent operational impacts when something looks

¹⁶ Col Bryant, William D. “Mission Assurance through Integrated Cyber Defense,” *Air & Space Power Journal* (Winter 2016): 7.

¹⁷ Cimpanu, Catalin. “You Have around 20 Minutes to Contain a Russian APT Attack.” *ZDNET*, 2019. February 19. <https://www.zdnet.com/article/you-have-around-20-minutes-to-contain-a-russian-apt-attack/>.

suspicious and requires blocking or modification of the system. The team has to be connected to ensure we can defeat the adversary and continue integrated deterrence.

In 2015, a published RAND study mentioned that we must “create a group of experts in cybersecurity who can be matrixed as needed within the life-cycle community, making resources available to small programs and to programs in sustainment”¹⁸ MDTs are the foundational yet simple cyber defensive force, just waiting to be integrated amongst weapon systems. We must realize our strengths and connect our forces.

In conclusion, the Air Force must realize we are fighting in cyberspace every day and it is of utmost significance to make a priority to fund defensive cyberspace operations. To make a significant effort at transitioning tactical leaders that are intimately familiar with weapon systems to Cyberspace Squadrons with MDTs.

¹⁸ 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](https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9800/RB9835/RAND_RB9835.pdf) (accessed 15 Dec 18)