SITUATION

In 2006 the United States Air Force developed and established doctrine naming "Cyberspace" as the fifth war fighting domain (along with land, sea, air, and space) and implement the first cyber command structure. Finally, in 2009 after the United States Cyber Command (**USCYBERCOM**) was established as a sub-unified combatant command, the **24th Air Force** was stood up to spearhead all USAF cyberspace operations. But it quickly became apparent that the pipeline for trained "cyber warriors" was incredibly thin.

To aid in the recruitment of cyber-security professionals, programs like CyberPatriot, established in 2009, were created and offered practical cyber exercises to middle and high school cadets. To date CAP continues to provide more than one third of the teams in the All Services division. But until 2014, no strategic vision was in place to adequately educate and train CAP members nor provide practical applications to skills learned. Beginning with the first cyber NCSA in 2014, the development of a "Cyber Program" has been underway with a primary focus on the cadet program. But CyberPatriot doesn't equal CAP's Cyber Program and in order to build successful cadets, we need senior member mentors with the proper skills and experience applicable to defensive cyber operations.

BACKGROUND

During the fall 2015 Board of Governors meeting, the National Cadet Cyber Programs team briefed CAP's potential role in defending U.S. national cyber infrastructure and aid in building the next generation cyber workforce. A request to establish a research or "TIGER" team was granted and chartered to study the following topics:

- Research how CAP can contribute to USAF's "Total Force" in a cyber defense capacity
    - Use programs like GREEN FLAG and Surrogate Remotely-Piloted Aircraft as a template
- Review CAP's current cyber-security posture regarding:
    - Configuration management of national, regional, wing level networks
    - Authorities overseeing information assurance of corporate and volunteer assets
- Develop a conceptual design for a senior Cyber Programs officer
- Expand on Cyber Programs education and training within the cadet program and include:
    - Review current USAF recruiting requirements for enlisted personnel and tailor training to prepare cadets for a possible USAF career
    - Develop cyber training modules for cadet encampments and advanced training academies like Cadet Officers School and Regional Cadet Leadership School
    - Expand cyber training into unit activities and cadet program achievements

EXTERNAL MISSION RESEARCH

The purpose of external mission research is to establish relationships with those organizations that execute defensive cyber operations and determine if CAP could provide qualified personnel that can aid in their missions. The overall goal was to establish a baseline of possible missions CAP could perform and build a member education and training program based on the requirements set forth by the mission originator.

The TIGER TEAM lead contacted multiple organizations to include: Headquarters Air Force / A6 (Communications) and Thomas Shubert, the Assistant Deputy for AF Auxiliary, Education and Development Programs, Office of the Secretary of the Air Force. While discussions with HAF is important to our relationships, we feel that discussions the direct leadership with the Operations Directorate (A3) would be more relevant to enumerating potential cyber missions. The justification for this is that while cyber bridges both communications and operations, cyber defensive operations traditionally falls under A3. Furthermore, it would be beneficial to CAP to also have a formal and in-depth discussion with the top USAF cyber officer, Lieutenant General Kevin McLaughlin, USCYBERCOM Deputy Commander.

It is our recommendation that while it may be 2-5 years before CAP can execute an external cyber related mission; we should continue to explore this topic with proper USAF leadership. Discussions with organizations like HAF/A3, USCYBERCOM, 24th and 25th Numbered Air Forces will aid in developing requirements for a proper training program.

Finally, a concern in CAP members participating activities like the “Hack the Pentagon Bug Bounty” in an official capacity could be considered “offensive cyber operations” or combative in nature. “Bug bounties,” vulnerability / compromise assessments, hunt actions are considered Defensive Cyberspace Operations (DCO) under Joint Publication 3-12: *Cyberspace Operations* where it states “DCO also includes actively hunting for advanced internal threats that evade routine security measures.” We feel that as a Title 10 noncombatant entity, CAP is within its power to perform these types of operations as long as a proper “Authority to Operate” is clearly outlined.

INTERNAL MISSION RESEARCH

Securing CAP’s information technology infrastructure and data is paramount. CAP members have increasingly becoming reliant on technology that tracks our members, inventory, personnel records; even our G1000 “glass cockpit” systems use sophisticated GPS tracking and instrumentation. But unfortunately, our policies and hierarchy haven’t not kept up with the technology.

Currently CAP’s corporate Director of Information Technology (DIT) is the interim Chief Information Officer (CIO). But in a traditional corporate environment, the IT directorate is focused on developing, maintaining, and disposing of IT resources, while the CIO is charged with ensuring

the security of systems and their data. It is a recommendation that the DIT be given the title Chief Technology Officer and a someone with formal cyber-security education be appointed as the CIO.

Infrastructure auditing, security assessments and incident response are normal cyber defensive operations within an organization. Many senior members within CAP serve in cyber-security roles within their own day to day jobs and carry credentials to prove their skills. It is a recommendation that a team of qualified personnel be developed to perform these roles according to the needs of the corporation. This would be at no cost to the organization and various collaboration tools could be used to keep in constant contact with remote auditors and responders. It is imperative that CAP establishes ability to properly secure its own information technology infrastructure before we look to conduct missions externally.

SENIOR MEMBER CYBER PROGRAMS OFFICER

The current Information Technology Officer specialty track primarily focuses on Information Technology, not cyber operations. Frankly security should not be an afterthought or secondary to the availability of IT systems. Furthermore, CAP needs to formally develop a cadre of senior members with the proper education and experience to mentor cadets interested in cyber security.

It is our recommendation that a formal Cyber Programs specialty track be developed with training requirements, certifications, and practical applications similar to SAREXs. Furthermore, a system would need to be developed to track senior members with the proper skills to execute various defensive cyber operations on order by the commander. It should be noted that these senior members should already have formal education in computer science, engineering or cyber security. This program is designed to hone our senior member's skills.

Finally, these senior members would aid in promoting the Cyber Program within the cadet program. Cyber Programs officers would use their training and experience to perform cyber activities at the squadron level, mentor cadets through the new Cyberspace module within the Aerospace Education program, inform cadets of upcoming cyber activities, and coach cyber defense competitions like CyberPatriot.

CYBER PROGRAM WITHIN THE CADET PROGRAM

Recently the USAF approved a recruitment program to offer sign-on bonuses to members with various cyber security certifications. Cadets interested in enlisting in the 3DX or 1BX career fields would be offered thousands of dollars for certifications like the Network or Security Plus certifications. The cost of a cadet attending the Cyber Defense Training Academy for two years is $100. This program will put a cadet on track to obtain a certification for under $500 dollars; significantly less than a cadet attending a flight academy for $1000-1500 for only a solo credit.

The overall cost to cadets and parents could aid in invigorating CAP cadet recruitment and help bring more diverse cadets and members into the career field.

Currently our team is developing a unit activity program called the "Tuesday meeting" cyber activity book that would aid squadron commanders to develop a cyber program within their own unit with little resources from NHQ. Furthermore, we are working on an encampment module to familiarize cadets with the cyber program during their first influential CAP activity. We are also working on a new AE module focused on educating our cadets in cyberspace operations. This module will be a requirement for all cadet officers to accomplish during their road to their Spaatz achievement. Finally, we are developing NCSA curriculum to put our cadets on track to achieve a CompTIA Security+ or Network+ certification within a few years of training and little cost to the cadet and parent.

NEED FOR A CYBER PROGRAMS DIVISION

The CAP organization currently places the Cyber Team under Cadet Programs at the National Headquarters. This placement was optimum for the fledgling organization, however, as the program has matured, CAP National Headquarters should consider establishing a Division or Branch within the Operations Directorate to provide focused operations support. This division would enable CAP to more fully explore opportunities in support of Emergency Services and provide greater voice for the program outside of Cadet Programs. This organization should be led by a Civil Air Patrol Colonel or Lieutenant Colonel.

We appreciate the opportunity to conduct research on behalf of the Civil Air Patrol Board of Governors regarding a formal cyber program. We hope that our recommendations will aid CAP in developing a viable program that will continue to build better members and aid in securing our national cyber infrastructure.