It Starts with a C: But it's not the CCRI

AN INVESTIGATION INTO AIR FORCE CYBERSECURITY CULTURE

By:
Aidan Chandra, Divya Ganesan and Akshay Gupta

Our Team and Purpose

AIDAN CHANDRA
EE & HISTORY '24

DIVYA GANESAN
CS & POLITICAL SCIENCE '25

AKSHAY GUPTA
ECON & CS '24

COL JAMES MICHAEL HARRINGTON
OUR MENTOR

We are a team of undergraduates at Stanford University. In 2022, we participated in the Hoover Institution's National Security Affairs Mentorship program, a program that matches selected National Security officials with students. Throughout the year we had the opportunity to build a strong relationship with our mentor Col James Michael Harrington through weekly meetings and discussions. In one such meeting, Col Harrington raised his frustrations with the Air Force's Command Cyber Readiness Inspection (CCRI) which he had to deal with as a Cyber Airman. Interested in learning more, we set out on a 10 week research project to learn more about the challenges surrounding the CCRI. We hope as outsiders and students, our view may provide guidance and learnings that can shift current thinking. The following report consolidates our learnings and central takeaways.

Table of Contents

The Question

Based on our conversations with Col Harrington and initial research our team came up with the following research question:

How can the Air Force improve the policies or processes around cyber readiness to reduce the amount of time, effort and resources spent preparing for the Command Cyber Readiness Inspection?

Our pairing hypothesis was as follows:

The Air Force may need better visibility tools to help limit the time, resources and effort spent preparing for the Command Cyber Readiness Inspection.

source:https://www.acc.af.mil/News/Article-Display/Article/200933/air-forces-northern-readies-for-cyber-inspection/

Methodology

10

weeks

2

iterations

8

interviews

Over a 10 week period we conducted a total of 8 interviews with all different levels of cyber airmen. We talked to Flight Commanders, Squadron Commanders technicians. We realized quickly that while our initial question was centered around the CCRI, most interviewees chose to talk about training overall. Thus, our line of questioning evolved in weeks 3-5 to surround the types of **training** airmen received. We heard a common theme: while all airmen received basic training, only the most motivated or top airmen would get extra training or choose to do extra learning. Investigating the purpose of training brought to us our final iteration of questions surrounding neither the CCRI, nor training but underlying culture around cybersecurity in the Air Force.

Interview Highlights

"Airmen need a way to build their benches"

"We need more cyber ninjas"

"I think it may actually be the internal motivation behind the training"

So through interviews we heard ...

- It’s not just about the **exam** itself.
- It’s not necessarily about **training** either.

... rather there exists a challenge around

culture.

Findings

We found that in the **status quo**, Air Force culture around cybersecurity is:

fearful of risk

confused

lacking of incentive structures

Findings

These cultural characteristics compound with **attributes** inherent to cyber:

fearful of risk

non-kinetic

confused

lacking of incentive structures

the churn

Findings

The status quo Air Force culture around cyber is

Fearful of risk - employees fear demotion or poor performance reviews when updating software or changing anything.

Members are often **confused** - technicians are often multi-tools rather than surgical instruments, doing many tasks without clear delineation..

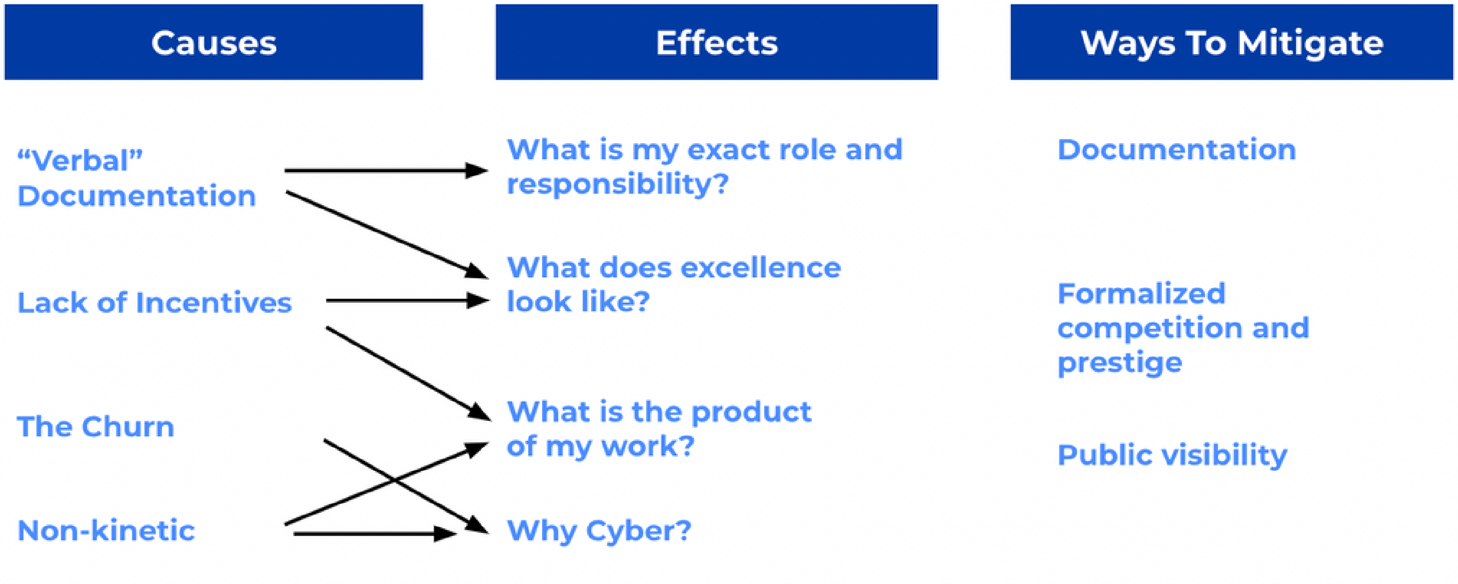
.

Finally, cyber in the Air Force lacks **incentive structures** - airmen in cyber do not have extrinsic objectives to work towards.

These cultural attributes are worsened by the churn and the non-kinetic nature of cyber. Airmen are constantly re-familiarizing themselves between bases and we simply cannot easily see the tangible product of work in cyber, especially when it is preventative or not public facing. We thus understand the problem through this **working model** [see next page]

Findings

In our working model, we organized causes, effects and mitigation methods into separate categories. It's worth noting that "The Churn" and the "Non-Kinetic" causes are structural or inherent, and not necessarily cultural. Rather, these elements combine with cultural elements to cause some unique and difficult problems. However, we firmly believe that these problems - due in part to non-cultural elements - can still be addressed and mitigated. A stronger culture of documentation, formalized competition and prestige specifically for cyber, and more opportunities for public visibility will help solve many Air Force culture issues, specifically within cyber.



Causes

"Verbal" Documentation

Lack of Incentives

The Churn

Non-kinetic

Effects

What is my exact role and responsibility?

What does excellence look like?

What is the product of my work?

Why Cyber?

Ways To Mitigate

Documentation

Formalized competition and prestige

Public visibility

Solutions

Given our model of the challenges in Air Force culture around cybersecurity, we see three central solution areas:

Changing the public narrative around cyber

Creating internal competition

Developing policies and protections for cyber airmen

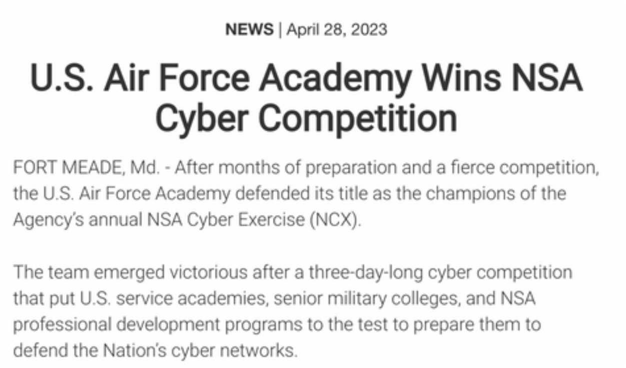
1) Public Narrative

If you ask any pilot in the Air Force if they are the best, their answer will probably be yes. But ask the same of a cyber airman? The answer is more likely to be: "I'm not sure." What would it look like for there to be a blockbuster about cyber that motivates talent and excellence with the same affect as Top Gun? How could we envision a superhero in cyber space in the same ways that we see ones in physical space? Changing the public narrative through media is one manner of shifting an internal Air Force narrative. This starts as small as thinking about how the Air Force markets itself to new recruits and more. Onboarding teams should celebrate and showcase exemplary talent to create visions for what success looks like.

Solutions

Internal competition have the potential to accomplish the same goal: showcasing and modeling a vision of cyber talent while motivating ambition in the space. Other federal agencies in Intelligence and more (as seen to the right) create opportunities for cyber-curious students to achieve, collaborate and learn key, applicable skills. In our Stanford careers, we have found competition to be a key learning experience. Divya helped form Stanford's first all girls cybersecurity team, in a personal sense finding new ambition and curiosity about the field. The Air Force has key opportunities to promote fun and competitive cyber challenges modeling CISA and the NSA to solidify cyber as a valued part of the Air Force mission.

2) Competition



NEWS | April 28, 2023

U.S. Air Force Academy Wins NSA Cyber Competition

FORT MEADE, Md. - After months of preparation and a fierce competition, the U.S. Air Force Academy defended its title as the champions of the Agency's annual NSA Cyber Exercise (NCX).

The team emerged victorious after a three-day-long cyber competition that put U.S. service academies, senior military colleges, and NSA professional development programs to the test to prepare them to defend the Nation's cyber networks.

3) Cyber Airmen Protection

Currently, cyber airmen, specifically technicians, feel an undue burden of liability when executing cyber tasks. This includes software updates, strategic decisions and more. Yet, risk-taking and preemptive movement is key to cyber success. In order for cyber airmen to continue to develop new skills, and try new strategies, they must be ensured protection for their actions while also committing to the training that allows them to make smart decisions regarding risk taking.

Conclusion: It Starts with a C but it's culture not the CCRI

Exploration

10 weeks of interviews told us the problem with the CCRI was more about culture.

↓

Analysis

We characterized the current Air Force culture as fearful, confusing, and lacking incentives.

↓

Problem Solving

We see potential solutions in changing public narratives, creating internal competitions, and more protection for cyber airmen.

Acknowledgements

Given our findings, we hope there will be room to collaborate in the future on planning internal competitions and more. Our most initial recommendation is that the Air Force collects **correlation data** between training and unit's CCRI scores to quantify the power of culture change.

That being said, we would like to **thank all** of our interviewees, Col Harrington, and the NSAF mentorship program.