CYBERWORX™

AIR FORCE CYBERWORX REPORT 17-001
Functional Mission Analysis for the Air Force Cyber Squadron Initiative

Lucille McMinn

MICHAEL V. CHIARAMONTE, Lt Col, USAF
Senior Designer & Facilitator

LUCILLE R. McMINN, Capt, USAF
#FMA4CSI Project Lead

Jeff Collins

JEFFREY A. COLLINS, Col, USAF
Director of AF CyberWorx

DESIGN PROJECT CONDUCTED
13 FEB – 17 FEB 17

Produced with input from numerous units including SAF/CIO A6, AF/A3, AFSPC A2/3/6, Air University, the Air Force Institute of Technology, the Joint Space Operations Center, 1 CBCS, 137 CS, 38 EIG, 39 IOS, 434 CS, 50 SCS, 52 CS, 53 EWG, 56 ACOMS, 673 CS, 721 CS, 744 CS, 752 OSS, and 92 COS. Designed by USAFA Officers and our valuable partners in Industry.

Air Force CyberWorx™
2354 Fairchild Dr, Ste 2N300
USAF Academy, CO 80840
AFCyberWorx@usafa.edu - @AFCyberWorx - (719) 333–4278

UNCLASSIFIED - Distribution A: Approved for public release; distribution unlimited

Introduction to AF CyberWorx

CyberWorx is a dynamic organization partnering Airmen, industry, and academia to reimagine how technology might enrich and protect our nation, businesses, and lives. As a human-centric design center, we seek out unique ways to connect Air Force warfighters with current and future technology in meaningful ways. We look to transfer, license, and share promising prototypes, solutions, and knowledge with our partners to create value for both the warfighter and the economy as this is the best way toward operational advantage.

Design Thinking @AFCyberWorx

Design thinking is a common sense, human-centric problem solving method embraced by innovation leaders in industry, but is often overlooked in the government sector. The CyberWorx design thinking process is a transdisciplinary method that breaks down silos of standard organizational structures. Organizations naturally form structures based on specializations to facilitate deep expertise, but these structures often impede creativity, collaboration, and knowledge sharing vital to innovation. CyberWorx deliberately reaches across specialties to bring diverse perspectives to a problem in a non-threatening environment. This evokes ideas that would otherwise be missed or stifled. The transdisciplinary design approach teases out meaningful solutions that are intuitive and desirable to Airmen.

> The CyberWorx design thinking approach deliberately breaks through the military's hierarchical and mission silos to find hard-hitting answers.

Air Force CyberWorx offers facilitated design thinking sessions that bring stakeholders, industry and academic experts together to develop solutions to hard problems. These sessions are tailored to best meet AF needs with differing lengths based on time sensitivity and CyberWorx capacity. One method, which maximizes solution agility and the educational benefit to warfighters and industry partners, is to offer a design sprint where the week-long design project answers a challenge being worked for AF stakeholders. The goal of such a design sprint is to develop low fidelity prototypes that clearly convey the desired Airman experience and the technical and policy developments needed to bring that experience to fruition. These projects help refine the requirement by seeking the right problem to solve and finding meaningful, forward-looking solutions by exploring a wide range of possible answers to the design problem.

Background: Operational Success

> "A B2 bomber departs the runway to engage targets with precision weaponry – the safety and success of that weapon system is dependent on intel, maintenance, medical, and flight planning systems, onboard diagnostics and navigation networks to name but a few cyber dependencies…"
> – Lt Col Billy Pope

The Air Force's base-level Communications Squadrons are engaged in a cultural and technological transformation through the Cyber Squadron Initiative (CSI). Once focused solely on delivering government-run information services and hardware maintenance, Communications Squadrons today are sharpening their focus to include active cyber defense and mission assurance as core competencies to enable operational advantages and out-maneuver our adversaries in cyberspace.

While CSI covers a broad mission set, Functional Mission Analysis (FMA) and Mission Defense Team (MDT) capabilities are vital means toward success in enabling active cyber defense of Air Force missions and algorithmic responses to intrusions and other breaches endangering information dominance. Unfortunately only a handful of the CSI units in FY16 saw their MDTs successfully execute, implement and sustain an FMA process. The #FMA4CSI design sprint brought together over 40 experts from government and industry to focus on this shortcoming and ways to accelerate the needed transformation, uncover lessons learned, and distill a plan to revector or to harden the CSI support structure.

Highlighted during the sprint was that FMA is not simply a cyber tool; FMA within CSI is about understanding how cyber impacts the AF missions and how using FMA to tailor cyber defenses assures operational missions and decision superiority for Airmen. Cyber FMA will present cyber to the base and wing commanders in terms of mission assurance and mission impact. Cyber FMA is in support of a commander delivering warfighting capability to our nation.

Problem Statement

How might we best provide robust, repeatable processes and training for conducting, saving, and sharing the results of FMA to enable successful expansion of the CSI to all bases for mission success of the AF? At the base level where these systems are employed to produce and enable airpower effects, FMA emerges as a critical competency to posture missions against expanding cyber vulnerabilities. FMA is a process units use to identify and codify cyber dependencies associated with Air Force missions at the base level. When accompanied by complementary intelligence to inform adversary capabilities and intent, FMA products highlight the key terrain in cyberspace these units must actively defend. The current version of FMA training is academically focused and difficult to put into practice for base cyber warriors to identify, codify, and protect their key terrain in cyberspace.

Leveraging FMA effectively transitions the communication mission to the cyber mission by reconstructing units to provide cyberspace operations in terms of standard mission planning and execution processes that have been well understood and practiced by the ops and planning communities (A3/5).

Figure 1: Participants held a Q&A session with the former CTO of Google as part of the design research phase. Key insights from industry leaders help shape the team's design effort.

Participants

The design project tapped over 40 people from the Air Force, joint cyber protection team members, CSI pathfinder units, as well as industry partners. Differing perspectives and cognitive diversity provided unique value, distinct from military members and government civilians. The CyberWorx design thinking approach deliberately breaks through the military's hierarchical and mission silos to find hard-hitting answers.

Theme Discovery

The early stages of a design project and the design thinking methodology call for analyses of the users' work environment, their desires, and their dislikes to inform and revise the initial problem statement. As part of the design process, the participants spent time delving into the various facets of the challenge to ensure they understood the challenge and were working on solving the right problem. This included research interviews with commanders, operators, subject experts, and industry leaders. These observations, experiences, and views provided an unparalleled view of the problem not achievable within a homogeneous group.

Leveraging the unique group, the design team explored both reshaping the vision for FMA and addressing underlying problems hindering the execution of FMA within the pathfinder MDTs. When considering how to overcome these issues, the team identified four key themes, divided here into two groups based on current issues and future sustainment needs:

- ***Solving current issues our CSI pathfinders are facing***
  - *FMA data standardization and collaboration*
  - *Top Cover through formalized FMA program*
- ***Creating future CSI/FMA Leaders***
  - *Talent management*
  - *Training pipeline*

The design sprint participants spent significant time developing personas (users) who would have existing stories within the #FMA4CSI framework and whose stories could be improved through proposed advances. Crafting these stories and working to design better ones exposed the individual and interpersonal reliance of FMA applications. Clearly, not every cyber professional will have the aptitude and desire to go into the FMA field; additionally a successful FMA-to-execution cycle relies on mission owners and operational leaders to buy-in to the FMA process and commit resources to drive the cyber defense outcomes needed for operational success in a digital-age war fight.

The themes formed the foundation of multiple proposals to include both short- and long-term solutions that are best explained via a hypothetical story starring SSgt Sara Super, a seasoned MDT technician at the 50th Network Ops Group (NOG).

Solving Current Issues

FMA Data Standardization and Collaboration

The first major impediment to FMA success within the CSI is a lack of useful collaboration tools between units, amplified by the lack of data and language standards for the FMA process. CSI's need an easy way to collaborate, share ideas and rapidly build off each other's successes.

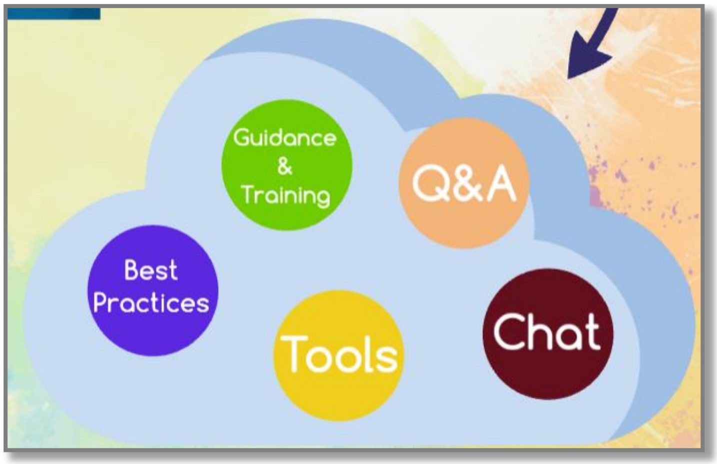


Figure 2: An online collaborative tool to share experiences, TTPS, training, data sets and tools can greatly improve MDT performance by harnessing the collective power of the masses to naturally gravitate toward more effective solutions.

Upon arriving at Schriever AFB on Tuesday, SSgt Super logs into the network and reviews the day's tasking's. This week she is finishing an FMA effort for one of the space operations missions at Schriever. Since this is the second mission she has completed FMA on ("FMA'd" is the verb coined during the sprint) Sara implemented some procedural improvements and has developed an FMA template for her mission type. To help the other MDTs in her unit and provide continuity for her MDT she logs into the AF MDT Common Body of Knowledge (CBK).

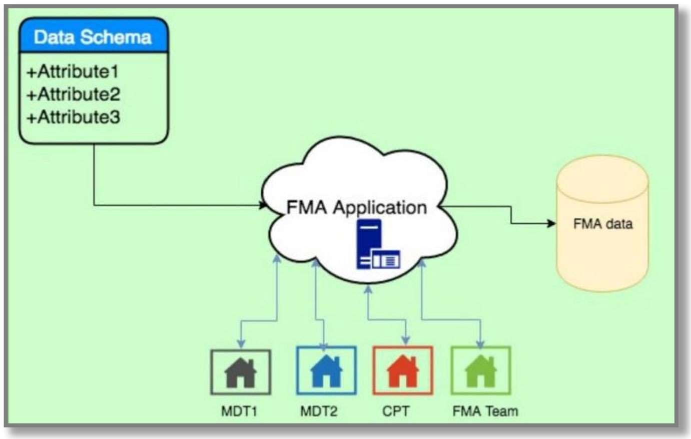


Figure 3: Standardized data formats and language facilitate easier sharing and analysis. These also enable machine-human teaming toward algorithmic analyses and timely, robust response actions and counter-moves to changing cyber threats.

This collaborative social environment serves as a social repository for MDT information sharing, TTPs, and baseline templates. Upon logging in Sara uploads her FMA template in the AF standardized format with a summary and any special instructions. She then submits comments to the MDT "best practices" forum that detail her lessons learned and the process improvements that proved successful at the 50 NOG. Once complete, like Facebook, these items are automatically shared to the all members of her unit, a practice quite natural to our millennial and Generation-Z Airmen.

As a top contributor to the CBK, SSgt Super receives a message from the system asking for help on behalf of Amn Byran Kandoo at Whiteman AFB. When Sara logs in she sees that her process improvement recommendations regarding FMA and industrial systems have been up-voted by other MDT members across the AF and are now near the top of the MDT best practices list. Amn Kandoo is part of a recently created MDT and is asking for help scanning industrial control systems with Nessus. Seeing that Byran is logged in, Sara connects with him directly via the CBK and provides firsthand knowledge about how her team solved the problem and what tools worked best. She even points him toward an FMA template she used once in the past to jumpstart her first FMA effort.

Amn Kandoo, armed with the tips provided in the CBK and by SSgt Super, quickly establishes basic cyber key terrain, threats, and controls using the FMA template he received from CBK. Amn Kandoo applies the template and begins minor modifications to tailor the FMA for his installation. The template, while incomplete, provides immediate insights to the Program Management Office (PMO) supporting a nuclear mission on the installation. Mr Sammie, an SES overseeing the PMO, uses data tags provided in the FMA data standards to quickly identify cyber linkages to vital mission threads. Once his team engages with the MDT and the appropriate intel resources to prioritize risks, Mr Sammie ensures needed

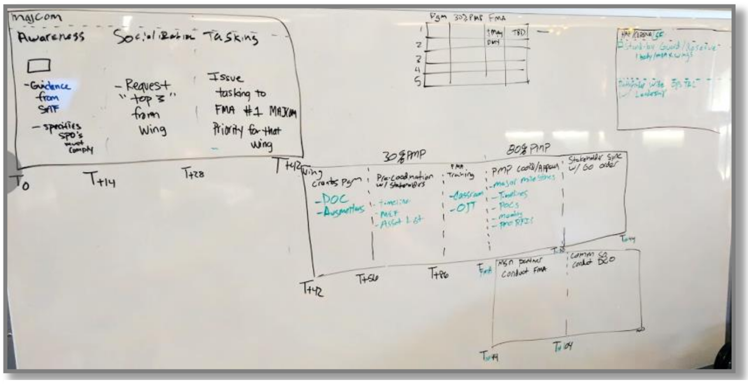


Figure 4: Designers prototype the framework of a wing-level FMA process that includes XP oversight and cross functional coordination. After testing this and many other idea on multiple personas the team agrees that wing-level ownership removes most roadblocks.

cybersecurity controls are addressed in the next PMO deployment and aligns with the MDTs across the AF on the best active risk mitigation measures for the newly identified vulnerabilities.

Collaboration using the CBK allows the experiences of SSgt Super to inform and guide Amn Kandoo. The result is a quicker MDT FMA effort that affects needed changes in mission systems to assure Air Force operational capabilities. Collaboration is vital to fostering best of breed FMA and MDT innovations, but the FMA process cannot succeed without proper leadership involvement. This brings us to our next theme, "top cover," a colloquialism meaning the highest ranking individuals (the CEOs of the Air Force) empower a process to be conducted for the benefit of the mission and with the resources needed.

Top Cover through Formalized FMA Program

As the CSI squadrons have been driven to standup MDTs and execute FMA they are having serious issues driven by a lack of top cover. In the current CSI model the FMA process is owned by the MDT in the cyber squadrons. Unfortunately the missions that need analysis are owned by other units across the wing and installation. Without appropriate top cover and installation buy-in the MDTs cannot succeed.

When Amn Kandoo was beginning his FMA process he needed to get access to specialists in the nuclear deterrence mission set. Amn Kandoo coordinated with his MDT OIC, Lt Maxx Newblood, to set up a series of observations and meetings with nuclear operators. As a key member of the installation's FMA program, Lt Newblood met with the host wing's FMA lead in the XP office, Maj Janet Planit. Maj Planit, a patch wearer, coordinates with key representatives across the installation's operational threads, introducing Lt Newblood, providing an overview of FMA and why it is being done, and clearing the way for the MDT to tightly observe and document the cyber linkages to the global strike mission.

With encouragement from Wing/XP, Amn Kandoo leads a small team of cyber operators conducting FMA. Unfortunately, while conducting their analysis Amn Kandoo comes across some specialized systems with which they are unfamiliar. After referring to the CBK, Amn Kandoo informs Lt Newblood and Maj Planit that they have a potential delay in FMA due to the specialized legacy systems that existing MDT TTPs and training do not address. Maj Planit elevates the issue to request support from the AF's new mobile FMA tiger team. This team, comprised of the very best MDT operators and PMO technical experts, conducts research and arrives on scene a few weeks later to help Lt Newblood and Amn Kandoo assess the legacy systems, ensure the local MDT is trained on those systems, and establishes new TTPs and training guides in the CBK for such systems. In addition to strengthening the AF's ability to defend its key terrain, Maj Planit has become more knowledgeable as a planner and operator, having increased her multi-domain lethality as she moves up in rank and toward Joint leadership roles.

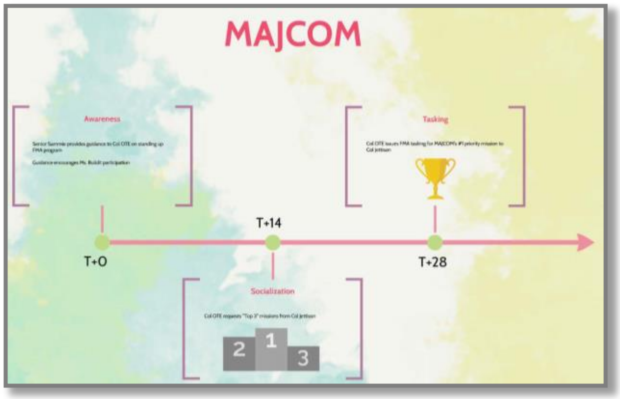

MAJCOM
Awareness
Senior Sammie provides guidance to Col OTE on standing up FMA program
Guidance encourages Ms. Buildit participation
Tasking
Col OTE issues FMA tasking for MAJCOM's #1 priority mission to Col Jettison
T+0
T+14
T+28
Socialization
Col OTE requests "Top 3" missions from Col Jettison
2
1
3

Figure 5: FMA is formally tasked to wings based on MAJCOM priorities. Cyber key terrain and defense actions must become commander business in the digital age AF.

Creating Future Leaders

Talent Management

SSgt Super is making some tough choices today. She could take a new job with a local contracting company or she could reenlist. After discussing her choices with her leadership, she understands she is only one of a few elite FMA experts with the special experience identifier. Even though the contracting company is offering her almost twice as much, her command can offer her a base of preference option as a reenlistment reward to retain her talents. As a result, she decides to reenlist and work for the 52nd CS MDT in Germany.

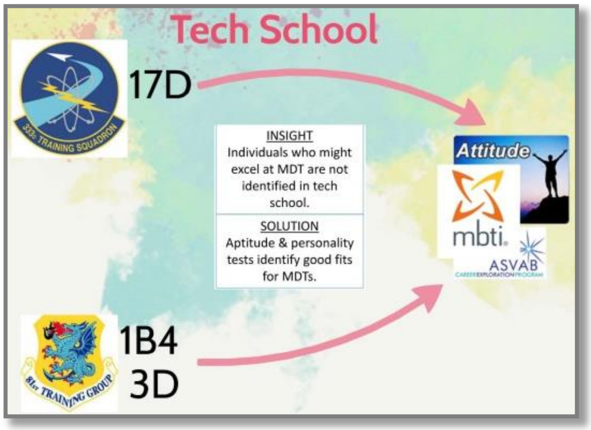

Tech School
17D
333rd TRAINING SQUADRON
INSIGHT
Individuals who might excel at MDT are not identified in tech school.
SOLUTION
Aptitude & personality tests identify good fits for MDTs.
Attitude
mbti
ASVAB
CAREER EXPLORATION PROGRAM
81st TRAINING GROUP
1B4
3D

Figure 6: MDT talent management starts with recognition of skills in tech school.

As SSgt Super PCS's, her back-fill turns out to be Amn Kandoo. As AFPC searched for a replacement amongst the moveable enlisted force, Amn Kandoo was near the top of the list. His SEI indicated significant FMA talent and a line for SrA.

Training

As presented in the earlier sections, FMA training will be enhanced via the Mobile Tiger Teams to provide OJT and life-support/expertise to existing and new MDTs that are encountering difficulties. While this is an important aspect of improved FMA training, it is not the only change needed. Initial Skills Training (IST) needs an update to ensure that airmen are being taught how to conduct FMA, why they conduct FMA and how FMA integrates with the deliberate planning process. This includes understanding and internalizing joint planning language to better integrate with other operators. FMA training needs to include not only academic exercises in the application of the method, but realistic scenarios where Airmen conduct FMA and integrate the outputs into MDT defensive actions and wing operational planning cycles. Realistic training scenarios, serious gaming in exercises, and sharing of TTPs via the CBK and practice on virtual ranges (LVCG, live-virtual-constructive-gaming) will move the AF toward training like we must expect to fight in the cyber-contested battlefield of today.

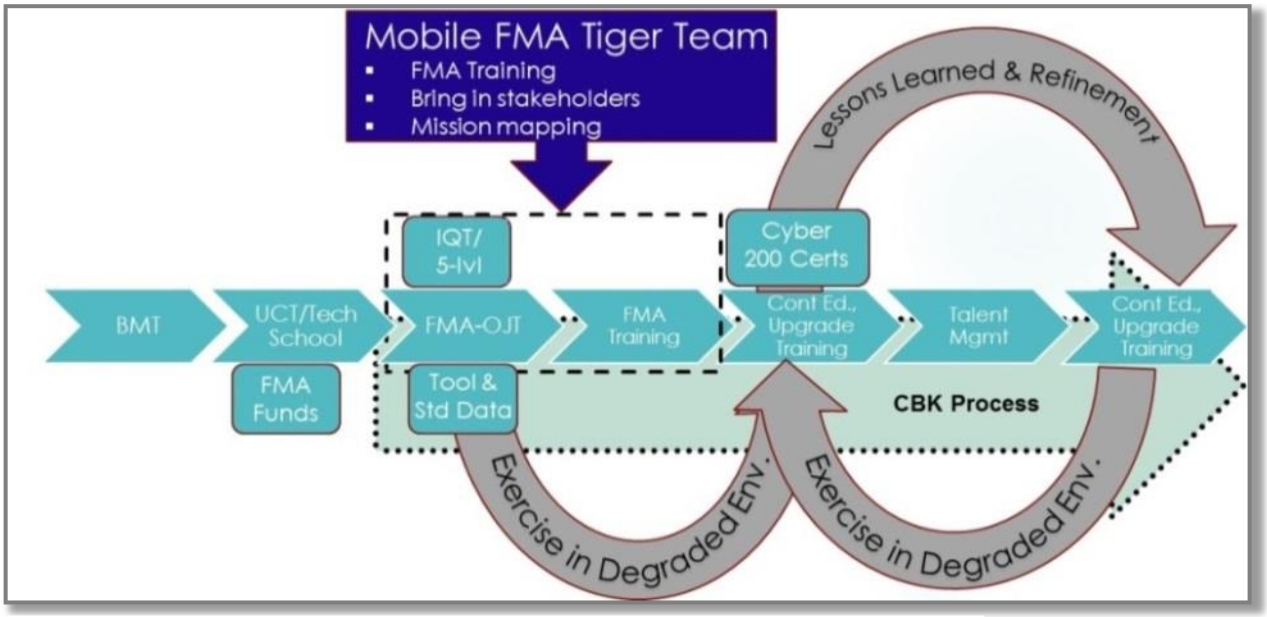


Figure 7: As communications squadrons transition to cyber squadrons, FMA must be incorporated into the training pipeline and integrated with operational planning topics.

Summary of Key Risks and Benefits

The cyber squadron initiative moves units from traditional roles as communications service and information technology (IT) deliverers to mission defenders. Functional Mission Analysis (FMA) is a proven path to transition from delivery of IT support services into the mission planning and operations cycle. Since MDTs today are dual tasked (IT support and FMA), realigning them to the wing has the beneficial outcome of providing top cover and mission ownership, but does not eliminate the risk accepted to the IT service delivery mission. Wings and supported units may experience degraded IT support until commercial and mobile capabilities are mature, so the AF's full commitment to cyber defense is required; otherwise, the communication squadrons will never transform into cyber squadrons capable of defending Air Force missions.

> The cyber squadron initiative moves units from traditional communications service and information technology deliverers to Air Force mission defenders.

The design sprint addressed two primary threads – solving current issues and creating future leaders. Foremost, the lack of top cover and lack of wing support leads to an inability to perform the FMA mission. Wing ownership adds IT risk by re-tasking billets toward FMA, but this helps reduce and identify critical mission risks by expanding the persistent defense of key cyber terrain. Allowing better collaboration, training and management of MDT forces will expedite the FMA process and result in a more cyber secure and mission ready Air Force.

Tactically, a standardized and integrated collaboration tool is paramount to enabling pathfinder success. Along with this, implementing a formalized tasking structure top-to-bottom from SAF/HAF through MAJCOMs, PMOs, and wings will speed CSI adoption and integration.

Recommendations and Next Steps

Short term, low risk/cost, high payoff changes ready for implementation now are:

- At least once a month during the pathfinder conference call, include a time for bottom-up information and successes to connect various pathfinders with each other to allow cross-talk and challenge/solution discovery.
- Plan an in-person pathfinder conference for operational and tactical collaboration

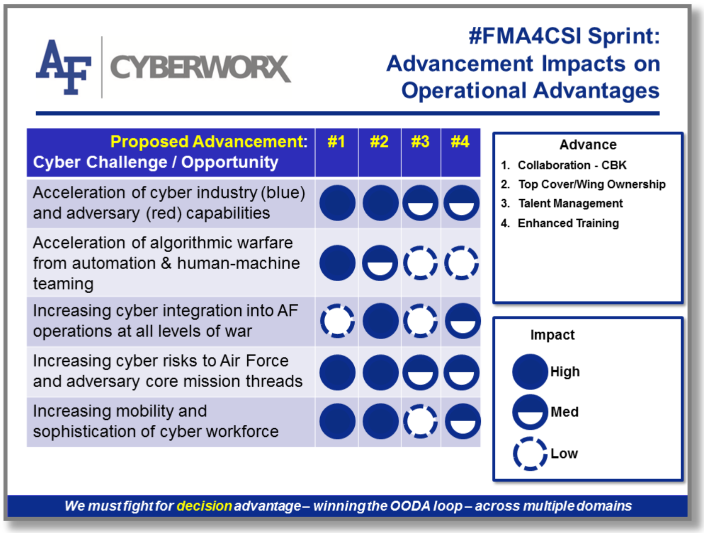
- Incentivize the use of existing collaboration technologies to improve cross flow of ideas, TTPs, and knowledge between MDTs and key stakeholders.
- Mandate MDT cyber personnel use accepted Joint terminology.
- Direct wings to take ownership of FMA and organize and conduct stakeholder round-tables to kick off wing FMA planning with cyber MDTs, a key part of the defensive posture.

Long term recommendations:

- Investigate state of the art social collaboration technologies to harness the power of Airmen. Demand signals already exist indicating a huge appetite for better collaboration mechanisms (e.g. Facebook use to share tech solutions).
- Alter IST to include FMA with a joint operations planning focus. Stress joint language, not cyber language.
- Investigate tailored talent management paths that grow specialized skill sets required for MDT operations.
- Stand up an Air Force FMA traveling tiger team to act as an expert consultant to new MDTs or new mission threads. This team will help execute initial FMA efforts, train MDT operators in the field, and produce, test and validate new and emerging TTPs.

Three Slide Summary: Ops Advantages via The Fast Track

The CyberWorx "three slide summary" section is designed to help in consideration of the recommendations in this report. The slide below weighs the operational improvements proposed in the report against the current cyber challenges and opportunities we face as an Air Force, listed on the left-hand side of the slide.



AF | CYBERWORX

#FMA4CSI Sprint:
Advancement Impacts on Operational Advantages

Proposed Advancement: Cyber Challenge / Opportunity	#1	#2	#3	#4
Acceleration of cyber industry (blue) and adversary (red) capabilities	●	●	◓	◓
Acceleration of algorithmic warfare from automation & human-machine teaming	●	◓	◌	◌
Increasing cyber integration into AF operations at all levels of war	◌	●	◌	◓
Increasing cyber risks to Air Force and adversary core mission threads	●	●	◓	◓
Increasing mobility and sophistication of cyber workforce	●	●	◌	◓

Advance

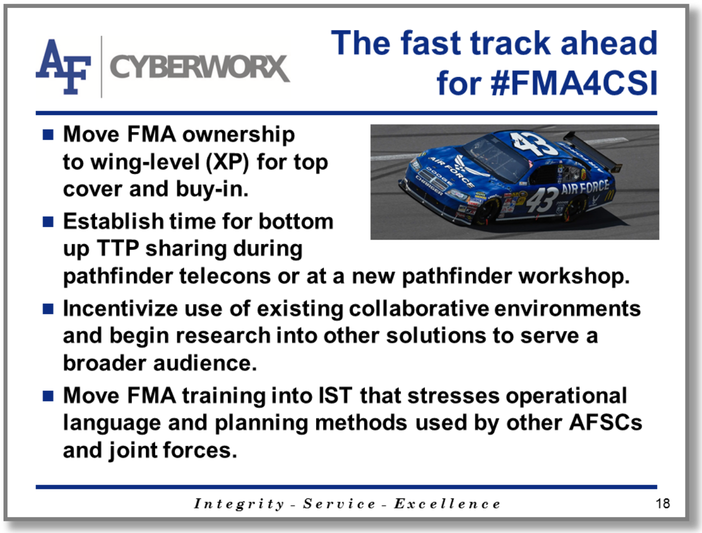
1. Collaboration - CBK
2. Top Cover/Wing Ownership
3. Talent Management
4. Enhanced Training

Impact

● High
◓ Med
◌ Low

We must fight for decision advantage – winning the OODA loop – across multiple domains

In deciding what to do, the decision to do nothing is a decision and brings its own risks. Thus, the "fast track" slide below spells out a recommended set of actions to take at minimum to put the Air Force on a path of discovery in overcoming the challenges that drove this design project.



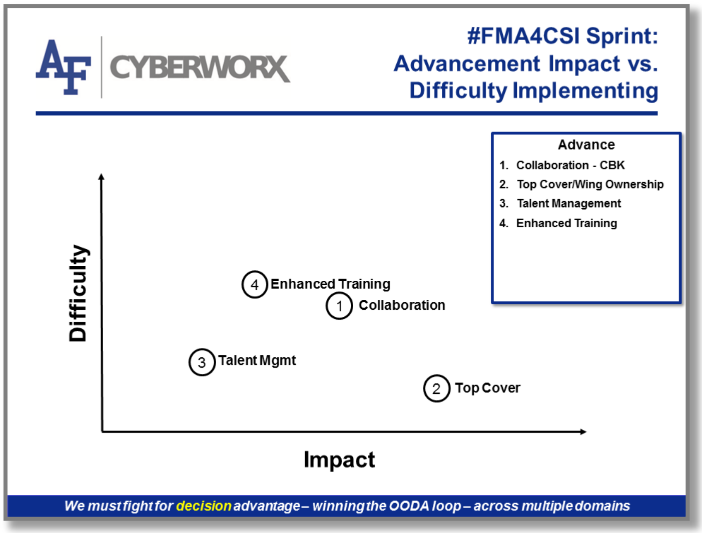
AF | CYBERWORX

The fast track ahead for #FMA4CSI

- Move FMA ownership to wing-level (XP) for top cover and buy-in.
- Establish time for bottom up TTP sharing during pathfinder telecons or at a new pathfinder workshop.
- Incentivize use of existing collaborative environments and begin research into other solutions to serve a broader audience.
- Move FMA training into IST that stresses operational language and planning methods used by other AFSCs and joint forces.

Integrity - Service - Excellence 18

We recognize we live in a resource-constrained world—neither money trees nor time machines exist. Each advance proposed in this report is graphed below: The graph compares the advance's relative impact on the ability of the Air Force to maintain information and decision dominance (x-axis) against the difficulty (e.g., expenditure of time/treasure, cultural evolution, policy change) needed to implement that advance (y-axis). Cultural changes, like those proposed in this report, are not easy, but they are possible and needed for success in our digital, cyber-contested world.



AF | CYBERWORX

#FMA4CSI Sprint: Advancement Impact vs. Difficulty Implementing

Advance
1. Collaboration - CBK
2. Top Cover/Wing Ownership
3. Talent Management
4. Enhanced Training

We must fight for decision advantage – winning the OODA loop – across multiple domains

CYBERWORX ™