No. 15
August 2017

The Mitchell Forum

The Cyber Edge:
Posturing the US Air Force for the Information Age

By Lt Gen William J. Bender, USAF (Ret.)

About the Forum

The Mitchell Forum exists to give an open venue to authors with ideas and thoughts on national defense and aerospace power. The series features topics and issues of broad interest and significant impact on current and emerging policy debates. The views expressed in this series are those of the author, and not necessarily those of the Mitchell Institute.

Abstract

The United States has assembled the best Air Force for the industrial age, and it must now transform itself to retain supremacy in the digital age. To effect this transformation, Airmen must think and act differently about how they will face adversaries in 21st century warfare. First, there must be a laser focus on mission assurance across all domains, and ensuring our cyber-connected platforms can achieve success through contested domains. Everything the service accomplishes must benefit the mission. Second, the Air Force must have a trained and ready workforce to meet the core mission requirements today and into the future. The service must consider partnering with private entities that provide services that will free Airmen to engage in more mission-direct tasks. Third, Airmen must treat data as a strategic asset. Placing the right information with the right person at the right time affords us the opportunity to make smart battlefield decisions before our adversaries can act. Finally, the Air Force must manage IT at the enterprise level. At the scale of our networks, if we continue to build local solutions to enterprise problems, the service and the Department of Defense won't be able to sustain the costs. The Air Force must address each of these issues with a sense of urgency if the Air Force is going to adapt to and overcome future threats and adversaries in the 21st century.

Introduction

The US Air Force is unquestionably the world's greatest industrial age Air Force. However, the world is changing dramatically. Technological advances are driving change that is outpacing the ability of the military services to organize and adapt, and the pace of these advances is accelerating. As a result, the US is now challenged to retain the world's greatest Air Force in the information age. Our military leadership needs to make some foundational changes to the Air Force to ensure this happens; incremental change will not be enough. We must fundamentally transform the way the Air Force thinks about information technology (IT) and cyberspace.

The greatest asymmetric challenge the US now faces is the cybersecurity challenge, where our inability to guarantee mission assurance presents a great advantage to our adversaries. The ubiquity of IT in modern weapon systems and inherent reliance on cyberspace for every Air Force mission means there are vulnerabilities in every aspect of the USAF's mission. While a P-51 would have been impossible to stop through cyber attack, a vastly more capable F-35 is so dependent upon software and IT-enabled support equipment that it could prove less effective in certain scenarios than the Mustang. This is not just a hypothetical scenario, as researchers have demonstrated cyber vulnerabilities in modern fighter aircraft and self-driving cars.[1] The KC-46 Pegasus, for example, while a fabulous aircraft, cannot perform its mission if an adversary compromises its "firmware," or software that is permanently programmed in the read-only memory of household appliances, vehicles, and other consumer goods.

While a P-51 would have been impossible to stop through cyber attack, a vastly more capable F-35 is so dependent upon software and IT-enabled support equipment that it could prove less effective in certain scenarios than the Mustang.

To manage the risks associated with emerging "cyber-contested environments" the US will face in the future, we must radically transform a litany of decades-old policies, processes, and business practices to respond to this completely different world. Perhaps more importantly, we need to fully embrace cyberspace as an operational domain, and undertake the necessary cultural shift this will entail. I believe we should start by focusing on four main areas: increase focus on mission assurance, build a future cyberspace force, manage data as a strategic asset, and take measured steps to manage IT services and investments at an enterprise level.

Increase Focus on Mission Assurance

If this undertaking is to be treated seriously, mission assurance must start with leadership. Mission assurance is a commander's responsibility and with the right amount of focus, all Airmen will understand the reason behind enforcing cybersecurity procedures. This includes the critical importance of avoiding such seemingly minor actions such as connecting an unapproved device to a mission support system. Every Airman must come to understand the total dependency the Air Force has on cyberspace to perform our missions, and that our legacy systems were developed when cyberspace could not be contested. The times have changed and the Air Force must change too. Today's Airmen have to fight to secure, protect, and defend our legacy systems in an environment where deception, denial, and even destruction through cyberspace is not only possible, but likely. As demonstrated by Stuxnet, a weaponized computer worm first identified in 2010 and linked to attacks on Iranian nuclear infrastructure, cyberspace today is a contested domain.[2]

To best understand mission assurance and how to defend our "cyber-physical" systems, the Air Force has found it helpful to group systems into three broad categories—IT, operational technology (OT), and platforms. IT is the most commonly understood category and it consists of cyber-physical systems whose principal purpose is to receive, store, process, or transmit data. This includes desktop computers, notebook computers, smart phones, servers, routers, and other devices. Operational technology is less well understood in the military, and it is made up of cyber-physical systems whose purpose is to control or monitor something in the physical world. This technology includes devices and systems like thermostats, power plants, alarm systems, and aircraft flight control systems. The final category of platforms (fighters, bombers, remote piloted aircraft, and so on) is a collection, normally both IT and OT, within a clearly defined physical boundary,

generally as part of a vehicle. While this category includes IT and OT, the Air Force created three categories because it discovered that we defend IT, OT, and platforms very differently based on their characteristics, so this was the most useful categorization. Enemies can and will attack each of these systems via cyber vulnerabilities.

The key to effective mission assurance is not to focus on vulnerabilities of the various systems, but instead to assess risk to a given mission. Not all vulnerabilities are equal. For example, a vulnerability in a critical C2 node is much more significant than the same vulnerability in a library computer, but today we just count vulnerabilities across an organization with little analysis of what impact that particular vulnerability could have on the mission. We largely focus on vulnerabilities because we haven't applied the required resources to do the difficult work of analysis in order to understand the importance of our various systems to different missions. Instead of thinking in terms of resiliency and risk mitigation, the Air Force still has a compliance focus, where cyber readiness inspectors grade bases by counting vulnerabilities and patches instead of a base's ability to accomplish its missions in a cyber-contested environment.

Instead of thinking in terms of resiliency and risk mitigation, the Air Force still has a compliance focus, where cyber readiness inspectors grade bases by counting vulnerabilities and patches instead of a base's ability to accomplish its missions in a cyber-contested environment.

In an effort to shift the focus from counting vulnerabilities to mission assurance, there are three mutually supporting approaches that should be pursued: defense in depth, resiliency, and active defense. Defense in depth, especially on IT platforms, is well understood, though rarely well executed. If the Air Force doesn't filter out low-level threats via effective architecture and tools, our other defensive approaches will be overwhelmed. Resiliency attempts to eliminate single points of failure and provide multiple mission pathways. We must keep the focus on the mission and while mission resiliency is often produced via well-designed systems, there are other ways to build resiliency. Resiliency can exist outside of cyberspace—a compass and map in the hands of a well-trained Airman, for example, provides resiliency for a complex navigation system. The final approach for risk mitigation is active defense, a more challenging approach. Active defense in this context refers to continuous monitoring and response, in an automated fashion where possible, within Air Force systems. These activities are challenging in OT and still more difficult in weapons platforms due to their complex architecture. The Air Force has found that effective active defense on traditional IT systems surrounding platforms often provides significant benefit in cases with these weapon systems. It is also important to note that these three approaches must work together, as they all rely on each other given the deep interdependencies between Air Force systems.

For mission assurance to work, we also must teach all our Airmen—not just cyber professionals—to think differently about cyberspace. Accordingly, the service recently launched a yearlong cybersecurity socialization and acculturation campaign across the Air Force. It is not enough to tell Airmen not to plug thumb drives into the Air Force network; all Airmen must be well informed about the clever, persistent tactics adversaries use. Research shows attackers most often gain access due to mistakes made by well meaning but unaware cyber users. No Airman would deliberately cut a hole in the physical fence protecting an Air Force base because they know that would endanger the mission and their teammates. Service leaders need to make sure that our Airmen also understand that clicking on a link, or plugging into a device could be the equivalent of cutting a hole in a physical fence in cyberspace and can have just as significant of an effect on our missions and people. If the Air Force is to achieve long-term success, we must raise the level of cyber-awareness across the entire force, and also make some significant changes to how we train and focus our cyber professionals.

Build a Future Cyberspace Force

The Air Force must change the culture, missions, and organizational structure of its cyberspace forces to meet the service's core mission requirements in the future. The present-day expectations of installation commanders are

based on legacy activities traditionally provided by communications squadrons that do not represent the best way to use those Airmen. The Air Force must leverage industry by "commoditizing" communication services and support that can be delivered more effectively and efficiently as a service. This would allow the Air Force's organic workforce to focus on mission assurance, by repurposing and aligning base-level cyber operators to the task of defending weapon systems, as well as the stand-alone mission networks and critical infrastructure that successful missions depend on. The Cyber Squadron Initiative (CS-I) pathfinder effort is changing the culture, mission, operations, and organizational structure for cyberspace superiority by providing freedom of maneuver in, thru, and from cyberspace. Achieving this goal requires the Air Force to organize, train, and equip (OT&E) Airmen to achieve the three lines of cyberspace operations not just for the Cyber Mission Force presented to US Cyber Command, but for the purpose of assuring the five core Air Force missions.[3]

Organizing, training, and equipping a cyberspace force that solely provides communication and information capabilities by running cables, maintaining satellite services, and managing base networks is ineffective preparation for current and future conflict.

Organizing, training, and equipping a cyberspace force that solely provides communication and information capabilities by running cables, maintaining satellite services, and managing base networks is ineffective preparation for current and future conflict. Although every Air Force mission either directly or indirectly relies upon cyberspace, the Air Force can share service delivery responsibilities with industry experts. At the same time, we cannot completely outsource responsibilities for communications services and support to private industry, because the Air Force will, for the foreseeable future, require bare base capabilities to generate warfighting effects around the globe to meet USAF and Department of Defense (DOD) requirements. The challenge will be to find the right balance between Air Force requirements for cyberspace operations forces, and existing combat communications capabilities (and associated manpower) to meet the needs of combatant commands around the world.

Leveraging commercial solutions to deliver networks, software, and even engineering as a service will free many cyber Airmen to focus on weapon system defense and effects generation in, through, and from cyberspace. Recognizing these self-imposed service delivery dependencies is the first step to changing a culture where, today, cyber Airmen simply build and maintain the Air Force portion of cyberspace. Establishing the Air Force Installation and Mission Support Center and transitioning functional responsibilities such as information management and postal operations from the cyberspace functional community is the latest evidence of forward thinking with regards to our cyber forces. Enabling the Air Force to envision a future that assures freedom of maneuver in cyberspace is an absolute necessity in order to meet future US national security objectives through unilateral, or joint and combined airpower.

Revitalizing Air Force squadrons is one of three priorities espoused by current Air Force Chief of Staff Gen David Goldfein. CS-I is an effort that focuses the OT&E efforts of commanders at the lowest level to assure our ability to fly, fight, and win a future conflict. Wing commanders understand an evolution from cyber Airmen who deliver network services to Airmen who conduct cyberspace operations is required to achieve core missions defined within the Air Force Future Operating Concept (AFFOC). These same commanders are the strongest advocates for more trained and equipped CS-I pathfinder units, for changes to current policy and mission directives, and for advancements related to cloud and automation in order to relieve Airmen from their traditional information technology provisioning and support responsibilities. As of summer 2017, 45 pathfinder squadrons are galvanizing future organizational, training, and equipment requirements through the formation of Mission Defense Teams (MDTs) that are focused on future Air Force operations in a contested cyberspace environment.

Understanding threats from cyberspace requires commanders to know the key cyber terrain they operate in to accomplish their missions. Cyber Airmen assigned to CS-I pathfinder units conduct functional mission analysis in order to get situational awareness through intelligence, sensing, and "hunting" missions. These MDT

activities will allow commanders to make risk-informed decisions to operate weapon systems reliant upon cyberspace, but potentially at risk in this domain. Commanders can no longer use the excuse of not knowing about exploitable cyberspace vulnerabilities. Admitting that weapon system vulnerabilities exist is no different than acknowledging that adversaries use air defense systems and anti-access/area denial tools to prevent the US from gaining air superiority. The difficulty of achieving air superiority in certain high-threat regions of the world drives innovation in advanced radar detection capabilities, countermeasures, and new stealth technology to breach such anti-access systems. This same mentality must permeate the cyber side of the Air Force in order to advance needed cyberspace capabilities to achieve our core missions. Just as we advance our ability to operate in contested cyberspace environments, we must also advance our ability to generate effects from cyberspace.

Unlike airpower, which had to prove its independent worth in two world wars, nations around the globe already recognize the asymmetric advantages of cyberspace.

Offensive cyberspace capabilities could some day play a part in securing air superiority in a future conflict. In *A Call to the Future*, the Air Force acknowledges that future air superiority challenges "need not be solved by an air-breathing platform." [4] It should be noted that another part of CS-I is the cyberspace operations flight—where advancements in OT&E for offensive cyberspace operations (OCO) generation will occur. The integration of adversary cyberspace activity and threat vulnerabilities will synch up with the air tasking order (ATO) in wing operation support squadrons. This integration will ensure all Air Force forces plan, exercise, and execute effects through a proven ATO methodology. Validation of offensive cyberspace operations will come through activities such as the delivery of time sequenced non-kinetic and kinetic capabilities on a target and achievement of desired effects during Red Flag or similar exercises. We will certify teams as mission ready only after validation of team performance, just as for aviation mission crews. The Air Force must advance its efforts to build effective OCO teams that are fully mission capable before they're called upon by a combatant commander.

Unlike airpower, which had to prove its independent worth in two world wars, nations around the globe already recognize the asymmetric advantages of cyberspace. In just the past year since the start of CS-I pathfinder units, Air Force commanders around the globe have identified potential impacts to mission readiness via cyberspace activities. These commanders have taken steps to assure readiness by fully supporting CS-I. However, the Air Force as an institution must do its part by actively pursuing IT commoditization and the transfer of non-core CS-I functions to other organizations. The service must take these steps to free up the limited number of cyber Airmen, and allow them to focus on delivering freedom of maneuver in, thru, and from cyberspace.

Manage Data as a Strategic Asset

In today's high-paced and rapidly evolving information environment, having the right information at the right place and time is critical to derive strategic advantages in a competitive, interconnected world. In short, data is a strategic asset and we need to treat it as such. Properly managing data and information gives an organization insight into difficult problems through understanding our environment, our adversaries, and ourselves. This can lead to more accurate predictions, plans, and forecasts—which are then used to manage both expectations and potential consequences. The goal is to gain knowledge about the options and opportunities available to improve processes, productivity, and performance, and at the same time to increase both capability and capacity to influence adversaries through information, as an alternative to kinetic effects.

Today, the Air Force cannot claim to have the right information at the right place, as there is currently no data management strategy, no accountability for the data we do have, and no ability to link disparate data sources. Instead, data is spread across the Air Force in separate enclaves, making it difficult to manage and leverage. With the volume of the data increasing at a logarithmic rate, the service needs to take steps now to identify authoritative data sources that will help Airmen identify the data sources they need to ensure

compatibility between the data and data analytics platforms. Essentially, the Air Force needs a data capability focused on identifying and collecting visible data that is fit for purpose, and structure the data in a way that makes information accessible. The service also needs to manage that information as a strategic asset that can better inform operational decisions. By registering data and cataloging information to illustrate a contextual picture, the knowledge gained will help produce informed decisions and an improved understanding of the consequences of Air Force actions, impacts, and results.

Air Force leaders also need to champion the development of enabling technologies and services to provide readily available, relevant, valid, and timely data. These technologies need to fit within an initial automated framework to register authoritative data sources, establish an enterprise data dictionary, extract information, apply access controls, and provide analytical support. This framework should be accessible to Air Force, and ultimately joint force and coalition users, based on operational information requests submitted to an enterprise-level authority. The best way to accomplish these tasks is to designate an Air Force data capability overseen by a Chief Data Officer (CDO). The CDO would lead an organization capable of managing data for the Air Force at the enterprise level. The time has come for the Air Force to treat data as a strategic asset, and exploit the immense mission effectiveness and efficiency gains possible by doing so.

The time has come for the Air Force to treat data as a strategic asset, and exploit the immense mission effectiveness and efficiency gains possible by doing so.

Manage Enterprise IT at the Enterprise Level

A final focus area to consider, if the Air Force is to transform its cyberspace approach, concerns the need to manage IT at the enterprise level under centralized CIO-led governance. Private industry considers enterprise IT a business enabler, not a cost to be minimized. When enterprise IT is managed properly it can increase the speed of capability delivery, reduce total costs, improve C2, and enhance security of key mission capabilities. Huge efficiencies are also ready to be realized. As just one example, there are currently 100,000 federal data centers, running collectively at 10 percent utilization. It is worth noting that running data centers is the highest cost of modern Air Force operations, next to the cost of procuring jet fuel. An enterprise approach to data center optimization would be common sense.

The operating environment is also different in cyberspace, and the Air Force needs to think and act differently as a result. Single purpose "stove piped" programs, for example, that focus solely on cost, schedule, and performance can no longer disregard the contextual attributes of speed, agility, and cybersecurity. A vulnerable system can be the access point needed by an enemy to get to more critical and better-defended systems. Strong cybersecurity requires managing overall risk at the enterprise level.

Of course, the Air Force must do more than just manage IT at the enterprise level. We must also design, develop, and procure enterprise IT much faster and innovatively. Information technology is a different sort of technology, and we need to increasingly adopt a "buy versus build" mentality, to look for opportunities to procure commercial "off the shelf" technologies, as service offerings and software-designed solutions. Congress wants the Air Force to be innovative, agile, lean, efficient, and effective and has thus granted the service a wide number of authorities that could allow us to operate much more quickly. We have not always taken advantage of these opportunities, in large measure because these methods differ from previous practice. The Air Force needs to shift its mindset. We must focus on buying instead of building solutions, and utilize pathfinders and prototypes in taking a "think big, start small, and scale fast" approach similar to how commercial industry approaches problems.

The Air Force must also fully embrace cloud computing. Mission effective IT is possible if we move our operations, where and when it makes sense, into a cloud based format. By doing so, applications and data will be secure and accessible to multiple users, bringing a myriad of advantages such as state of the art infrastructure and applications without the capital expense of building out organic IT infrastructure. Paying for services rendered versus infrastructure is the modern IT industry model, and would result in significant savings of the large sums of IT dollars

the Air Force spends today sustaining legacy infrastructure. Every business has a core identity, and ours is developing, providing, and executing air, space, and cyber power, not building IT infrastructure. Refocusing would allow us to more quickly shift our military cyber force's work roles into maneuvering and defending our systems in cyberspace. Congress has seen fit to support moving IT infrastructure to the cloud in the past several defense authorization bills, and the Air Force should do so with a sense of urgency.

Conclusion: Assuring Cyber Dominance in an Information Age

The Air Force must change rapidly if it is going to remain the greatest Air Force in the world during the information age. Operations in, through, and from cyberspace represent the current focal point of asymmetric combat advantage, and we must be as dominant in the cyberspace domain as we have been in the air and space domains. To achieve that dominance will require making changes that will challenge the Air Force as an institution and its culture. These initial changes can be grouped within four focus areas.

First, the service needs to increase its focus on mission assurance and shift the way it measures performance—from compliance based measures that count vulnerabilities and patches to measuring how well we can assure our missions. Secondly, the Air Force has to build a future cyberspace force focused on cyberspace maneuver and put less emphasis on IT provisioning, which can be more effectively done by industry partners. Third, we also need to rationalize the way the Air Force manages data and enables airmen to access the data they need across the enterprise. The Air Force should also strive to use data from across the enterprise to improve our efficiency and effectiveness. Finally, we absolutely must manage enterprise IT at the enterprise level. Accomplishing this will yield lower costs, faster deployments, less complex acquisitions and administration, a more predictable future, and greater accountability.

The key attribute the Air Force is missing in the cyber arena is speed. The environment is dynamic, with rapidly advancing technology that has completely outpaced the policies, processes, and business practices we developed decades ago that served us well in a different time but now must be adapted. The Air Force must move to change and innovate if the service is going to survive and thrive in this new information-driven world. If not, the Air Force faces to the prospect of extinction, as the environment we sprang from fades further into the past. ✪

Endnotes

1 Author's note: See Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stephan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadoyoshi Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," (USENIX Security Conference, August 10-12, 2011) 3-5. Also see, Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in it" Wired, 21 July 21, 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (accessed August 4, 2017).

2 Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Broadway Books, 2015).

3 Author's note: Joint doctrine defines three cyberspace lines of operation: defensive cyberspace operations (DCO), offensive cyberspace operations (OCO), and Department of Defense information networks operations (DODIN). See Joint Chiefs of Staff, Joint Publication 3-12 Cyberspace Operations.

4 Headquarters US Air Force, *America's Air Force: A Call to the Future*, July 2014, pg. 17, http://www.af.mil/Portals/1/documents/SECAF/AF_30_Year_Strategy.pdf (accessed August 4, 2017).

About The Mitchell Institute

The Mitchell Institute educates the general public about aerospace power's contribution to America's global interests, informs policy and budget deliberations, and cultivates the next generation of thought leaders to exploit the advantages of operating in air, space, and cyberspace.

About the Forum

The Mitchell Forum series is produced and edited by Marc V. Schanz, Mitchell Institute's director of publications. Copies may be reproduced for personal use. Single copies may be downloaded from the Mitchell Institute's website. For more information, author guidelines, and submission inquiries, contact Mr. Schanz at mschanz@afa.org or at (703) 247-5837.

About the Author

Lt Gen William J. "Bill" Bender (USAF, Ret.) served as the Chief, Information Dominance and Chief Information Officer (CIO), Office of the Secretary of the Air Force, Pentagon, Washington, D.C. from September 2014 until his retirement from active duty on August 1, 2017.

Commissioned in 1983 after earning a Bachelors of Engineering degree from Manhattan College, Bender has held staff assignments at Air Mobility Command, US European Command, and Headquarters US Air Force. He has commanded an airlift squadron, an operations group, an air refueling wing, an airlift wing, and the US Air Force Expeditionary Center.

During his tenure as the Air Force's CIO, Bender led three directorates and 54,000 cyber operations and support personnel across the globe, overseeing a portfolio valued at $17 billion. Bender had overall responsibility for the Air Force's information technology portfolio as the senior authority for IT, investment strategy, networks and network-centric policies, communications, information resources management, information assurance, and related matters for the service. He also oversaw portfolio management, helped deliver enterprise architecture, and worked to integrate Air Force combat and mission support capabilities by pushing to network air, space, and terrestrial assets. Bender also oversaw efforts to shape doctrine, strategy, and policy for all Air Force cyberspace operations and support activities.

Bender is a command pilot with more than 4,000 hours in the T-37, T-38, C/KC-135, EC-18B, E/KE-3A/B, C-141B, C-17A, C-130E, C-130J, and KC-10.