Sharing the Cyber Journey

Suzanne M. Vautrinot, Major General, USAF

0620 ZULU (1120 PDT): Based on remotely piloted aircraft (RPA) surveillance, special operations forces prepare to enter a village that contains a high-value target (HVT).

0630 ZULU: The mission commander in the joint operations center monitors the HVT and surrounding village activity via real-time video feed from the Predator aircraft.

0632 ZULU: The mission commander loses visual surveillance of the current operation.

- Did a civilian system administrator in California pull a circuit offline to perform routine maintenance?
- Did a highway construction crew in Florida cut a fiber-optic cable during excavation?
- Did an adversary nation inject malicious software, preventing operation of the common operating system display?
- Did lightning take out a transformer in Nevada and cut off power to the data transmission system?

0635 ZULU: Forces reach preposition points and stand by for mission authorization.

06?? ZULU: The mission commander aborts the mission due to lack of situational awareness.

As the forces hunker down, the entire command and a global support structure hit afterburner in an attempt to determine (1) what happened to cause the loss of visual contact, (2) can it be recovered, and (3) will it be in time to achieve the intended mission?—a situation with seemingly infinite causality, demanding action in finite moments.

Maj Gen Suzanne M. "Zan" Vautrinot is commander, Twenty-fourth Air Force, and commander, Air Force Network Operations, Lackland AFB, Texas. She is also the commander, AFCYBER, and is responsible for providing combatant commanders with trained and ready cyber forces to plan and conduct cyberspace operations. General Vautrinot is a 1982 US Air Force Academy graduate who has served in various cyber operations, plans and policy, strategic security, space operations, and staff assignments.

The author gratefully acknowledges the contributions of Capt Jeffrey A. Martinez and Capt Matthew R. Kayser in preparing this article.

While the operations center staff check their equipment, computer maintainers in dozens of locations check for indicators of hardware or software system failure; civil engineers evaluate power, chillers, and HVAC systems operation; network operators across the globe search for dropped fiber connections; satellite operators work to verify communication and data feeds; spectrum analysts look for jamming indications; intelligence analysts dive into indications of potential adversary action; weather experts evaluate scintillation—all while mission commanders check their watches.

One operation, one mission, yet it requires a myriad of extraordinary experts—each unique and each integral to an RPA operation that depends on well over a hundred individual commercial and military network connections, dozens of integrated hardware systems, miles of fiber-optic cable, significant satellite bandwidth, and millions of lines of software code. Welcome to the cyber domain: an environment of intellect, integration, and, for good as well as ill, complex interdependency.

The scenario described above could affect equally any military weapon system or mission. In the vast majority of cases, these network dependencies are not well documented, the real-time status of network systems is not automated or transmitted, the supporting infrastructure is diverse and aging, the investigation remains essentially manual, and the fingers generally point to the "distant end," located in the vicinity of Valhalla. One might conclude poor performance, inadequate resourcing, or perhaps poor design, but the dynamics simply reflect the way cyber has rapidly emerged—in our equipment and in our collective psyche.

Historically, technology was leveraged to improve performance of each weapon system relative to the environment in which it must operate. That environment was governed by Mother Nature, and our ability to fly through, dive beneath, breathe without, orbit above, or move undetected was achieved by creating systems that overcame environmental limitations. Each new technology was ingeniously integrated into our ground, sea, air, and space systems to gain capability. By leveraging communications, computers, networks, and information technology, we improved the capabilities of each existing system while also making them dependent on a new environment—a man-made cyber environment. The acute dependency was unintentional, and like our legacy networks, it grew with the best of intentions and a dearth of strategic design.

A strategic discussion on cyber has become more than a DoD activity; it is now a national imperative. As Malcolm Gladwell might say, we are at a tipping point. Relative to cyber technologies, do we continue to bolt on or should we bake in? Regarding cyberspace as a man-made environment, do we simply respond to changes or work with our civil sector counterparts to alter the environment to our collective advantage? As we leverage the technologies associated with cyberspace, we have an opportunity to constantly create and re-create our environment—to design the future.

Leveraging the Past, Innovating the Future

Every generation stands on the many shoulders of greatness that preceded it. For military leaders and as part of our Air Force heritage, flying faster, turning tighter, launching further, viewing in more detail, and arriving with greater precision all align with a tradition of innovating beyond the heritage left by revered forefathers. The world we face today is significantly different from that of our predecessors. From a military perspective, the most formidable changes do not just involve enhancing the physical attributes of our weapon systems or incrementally adjusting the traditional methods of employing those weapon systems. The distinction is that now we can leverage the virtual, and the implications are boundless.

We did not arrive at this point overnight. For decades, leaders in engineering, cryptology, computer science, information technology, and many other contributing disciplines expanded and then integrated these technologies. Yet, although the technical disciplines were varied, the application of cyber now follows a path similar to air, sea, and space in their early stages. Akin to the Wright Flyer's relationship to the F-35, mainframes, and eventually personal computers, were the harbingers of our cyber capabilities. Continued platform development led to aircraft being used as a ground force and intelligence enabler during Army Air Corps operations. Similarly, integrated networks enabled the rapid dissemination of information for defense and intelligence operations. Code-breaking and cryptology applied to secure communications foreshadowed today's cyber information assurance and exploitation capabilities.

Airpower eventually emerged as both a supporting element and a formidable alternative to traditional land and sea forces. The application of cyber capability to enable ground, sea, air, and space operations continues to accelerate, but as with airpower, we should similarly expect cyber to emerge as a strategic alternative.

To advance cyber toward this strategic alternative, Twenty-fourth Air Force (24 AF) was established as a war-fighting numbered air force focused on full-spectrum cyberspace operations. It operates under three distinct roles: Air Forces Cyber (AFCYBER), the USAF cyber component force provider to combatant commanders (COCOM) through US Cyber Command; AF Network Operations (AFNetOps), the operator and defender of the Air Force portion of the DoD network; and 24 AF, the organize, train, and equip lead for USAF cyber personnel. Since both the AFNetOps and 24 AF functions oversee USAF-specific mission areas, they report to Air Force Space Command (AFSPC); in the AFCYBER role, they report directly to US Cyber Command and provide capabilities at the operational level to the joint war fighter.

Currently, we have a reactive defense posture that is outdated and manpower intensive. Our heterogeneous architecture, composed of legacy infrastructures, is difficult to maintain and provides limited situational awareness across the networks. With a steady topline cyber funding amount, as depicted in figure 1, every dollar spent toward protecting our networks needs to move us toward a more homogeneous and centralized

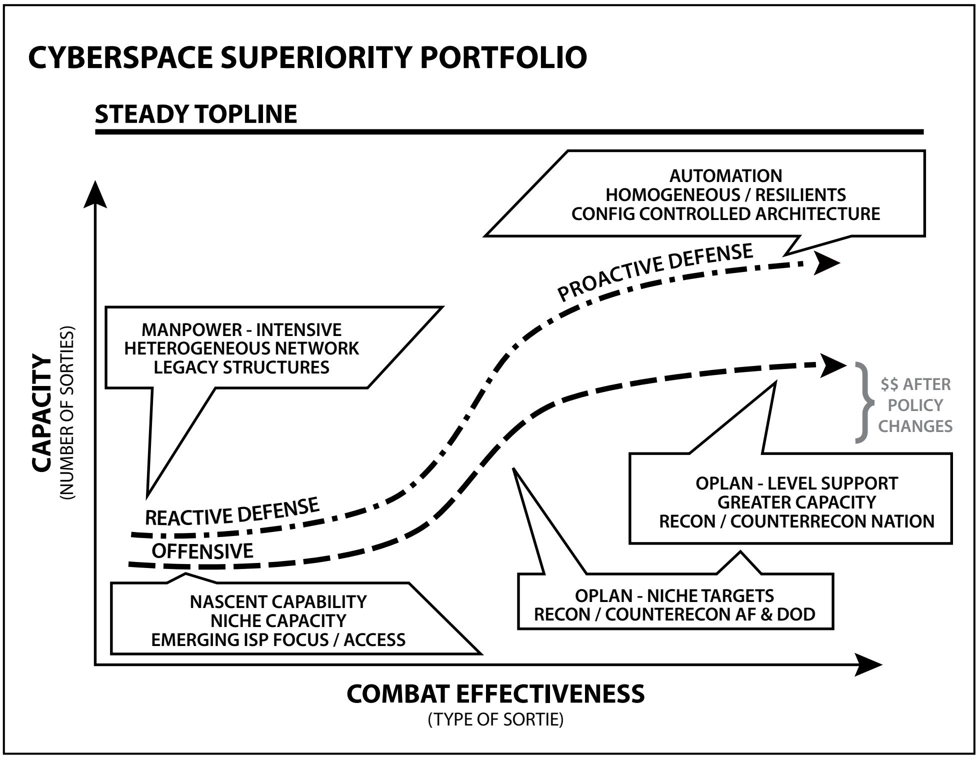

Figure 1. Cyberspace investment challenge

architecture that can reap the benefits of automation. Future investments must reflect advancement toward automation and resilient architectures so the efficiencies gained in manpower can increase the capacity of a skilled technical workforce.

We are at a nexus regarding future cyberspace operations providing for the national defense. For the Air Force to fulfill its commitment to providing global reach, global power, and global vigilance, it must do what Airmen have always done—innovate. To accomplish these goals, we have developed three integrated strategies: deliver a robust, defensible, trusted network; operationally leverage cyberspace capabilities; and build and deliver combat power. The remainder of this article is organized around an Air Force leadership dialog and Airmen's fulfillment of these strategies.

Deliver a Robust, Defensible, Trusted Network

The RPA exemplar applies equally to every military service member's ground, sea, air, or space operations; to their civilian counterparts' corporate business; and to local, state, or federal government activities. Each requires assurance that the networks, the multifaceted environment on which they are now so dependent, can be trusted to enable mission success.

Cyberspace is not simply the Internet; rather, it is a network of interdependent information technologies including the Internet, telecommunications networks, computer systems, and embedded processors. Its use has become ubiquitous within every public, industrial, academic, and military organization. Individually and collectively, we have increased productivity, interaction, performance, and efficiency by use of and by reliance on cyberspace. We "face-time" with friends and family, we pay bills via bank websites, parents monitor home security while away, and troops use social media to stay connected to home. Most importantly for this conversation, the nation and the Air Force have increased weapon system performance, extended operational capabilities, and enhanced command and control by leveraging cyberspace. Yet, as with all things yin, there is a yang. The dark side leverages this common ground to steal, compromise, degrade, or destroy information; disrupt networks or communications; or deny service. In military terms, cyberspace is a contested environment. Hactivists, cyber criminals, terrorists, and adversarial nations are active in cyberspace networks across the globe; our military networks are no exception. DoD networks are probed millions of times per day. In a typical week, the Air Force blocks roughly two billion potential threats and denies two million phishing or spam e-mails. Armed with an understanding of the growing threat to and our dependency on the network, Air Force leaders directed a service-wide migration to a more defensible network—creating the AFNet migration and facilitating a "defense-in-depth" alignment. Helping create this defensible construct, AFSPC, through its subordinate units at 24 AF and the Air Force Network Integration Center, is reorganizing and reequipping to address the limitations resident in current Air Force heterogeneous network architecture and the underlying technologies. What is meant by "heterogeneous" network? We have many variances in hardware, configuration, and software licensing. As the network expands, updating and maintaining various systems becomes problematic. Inevitably, devices are not properly or consistently configured, and vulnerabilities arise. Moreover, the ability to discern the "root cause" of network issues requires significant time and resources to first understand the configuration, then find and address the underlying problems.

The process of moving from this dispersed, installation-managed network architecture to a single, homogeneous, and centrally managed Air Force network, called the AFNet, is the number one cyberspace initiative in the Air Force. Originally, the AFNet migration consisted only of consolidation of individual base active directory "trees" into a single Air Force active directory tree. Now the term has evolved into a broader concept involving all the necessary steps to move to a single Air Force network. Industry counterparts like AT&T preceded us in this endeavor, applying significant up-front capital and draconian change management. Their conclusion, and ours, is that without the initial homogeny, we cannot implement the necessary sensors and automation to strengthen and defend network operations at the scale required for a global industry or military operations.

The first step was to realign AF network interfaces through a small number of gateways, thereby increasing visibility of network traffic as it moved into and among various organizations. This allows Air Force operators to observe patterns of (network) behavior and respond to anomalous activity. That response can include notification of other service and DoD-level operations centers (notably the joint operations center for US Cyber Command), implementing passive defenses within the AFNet, conducting forensics, reverse-engineering software, and supporting law enforcement and/or intelligence professionals in tracing the sources and potential implication of intrusions. The vast majority of this work remains appropriately invisible to network users; nevertheless, it is foundational to a defensible network.

The second step of migration involves consolidation of each individual base's active directory structure into a single Air Force active directory tree. Simply put, active directory enables a centralized approach for network management and security. It provides services that authenticate and authorize users, assigns and enforces cyber policies, and simplifies updating computers. This will enable a simpler, more automated approach to managing the Air Force's e-mail and SharePoint applications. In addition, it will allow shutdown of the legacy systems at each base. Airmen at all levels and every base continue to rise to the challenge, and to date, roughly a quarter of all locations have migrated, with a targeted completion in FY-13. Migrating the entire Air Force population of roughly 850,000 personnel at over 400 locations will result in a much more defensible construct that aligns the Air Force leadership vision with the guidance and intent of US Cyber Command: to provide a more secure and, ultimately, operational platform.

There are many advantages to this AFNet migration, the most important being the opportunity to now increase sensing, automation, and situational awareness. In the Central Command Combined Air Operations Center, walls are filled with screens depicting operational status and battlefield video feeds for real-time analysis and decision making. The corresponding cyber information to depict network operational status and enable real-time analysis does not currently exist, nor was it possible prior to the rearchitecting of the AFNet. Operators in the 624th Operations Center, 24 AF's command and control unit, manually perform the task of data synthesis after distant-end units enter status information into the system. There is no common operating picture of activity across our networks, making it more difficult to assess and respond to the threat environment. Yet, there are innovators: cyber professionals from many career fields who daily apply capabilities and leverage new tactics, techniques, and procedures to successfully provide mission assurance, threat detection and response, and network operations and defense. The capabilities for sensing the status and automating operational activities will continue to expand, and so must the capacity elements necessary to reach and execute full-spectrum cyber operations globally. Migration to a single architecture provides the opportunity for Air Force–wide network situational awareness—an awareness that enables robust, defensible, and trusted air, space, and cyber operations.

When designers of major weapon systems build cyber technologies into their programs, they fail to integrate them with the Air Force network. Frequently, these systems introduce cyber vulnerabilities into the network that cannot be patched or updated using established capabilities and processes. Networks cannot just be the domain of cyber folks; they must be central in the development and operation of every weapon system for design and connection interfaces. This requires application and enforcement of network standards for any weapon system that uses the Air Force network.

In that pursuit we are striving to increase awareness of rapid technological advances and best practices through partnerships with academia, industry, sister services, and government agencies. General Alexander outlined in his recent remarks to the Senate Armed Services Committee that, in his view, there are three key players that make up a cross-government team to mature and implement an effective cyber strategy for the nation: the Department of Homeland Security, the Federal Bureau of Investigation, and the DoD/intelligence community/National Security Agency/ USCYBERCOM. Through USCYBERCOM, we have teamed with cyberspace law enforcement counterparts: leaders like Steve Shirley at the DoD Cyber Crime Center, and the OSI to share information on current threats and tactics as well as leverage their unique forensics expertise. Via 24 AF and the Air Force Computer Emergency Response Team (CERT), the USAF participates in the Defense Industrial Base Initiative, an agreement with over 30 industry partners, including many of the larger corporations in this country, to collaborate with the Departments of Defense and Homeland Security to share sensitive threat information and thereby improve the collective cyberspace defense. Moving forward, we will continue to leverage the great capacity and unique capabilities of not only 24 AF and Air Force Space Command but also the expertise of Airmen in our intelligence, law enforcement, and engineering development communities.

The Air Force utilized partnerships with Department of Energy and university national laboratories, like Lawrence Livermore National Laboratory, to deliver a network defense system in the early 1990s. We continue to develop and expand those core relationships today. We are working with Lawrence Livermore to field a network situational awareness capability that is being used by other government organizations. These channels for cooperation increase the flow of information and create a higher level of awareness across all levels of academia, industry, and government.

Improving our defensive network posture is not just about changing equipment and infrastructure; it is also about adopting a proactive defense mind-set. Instead of waiting until an adversary penetrates our networks to assess our vulnerabilities, we have created a specialized team that searches our networks and seeks out those vulnerabilities before they are exploited. This mobile precision capability demonstrates the viability to identify, pursue, and mitigate threats impacting critical links and nodes and provides an additional tool in protecting mission networks. However, we cannot seek or defend everything, so identifying and defending those interfaces that are essential to mission success are crucial. A key facet of this mission is identifying and focusing on a COCOM's prioritized "defended asset list," those critical areas that must be able to operate through an attack. In creating this team, we partnered with the US Transportation Command, as tanker information, logistics tracking, and airlift movements are some of our adversaries' highest-valued targets. As yet a nascent capability, this team may represent one of the most viable missions for expansion.

Proactive defense also reduces the need for human in-the-loop processes; it is far superior to the current reactive process. When we detect an intrusion attempt, the Air Force CERT identifies the characteristics of that attack and updates active sensors, located at multiple defensive levels within the network, with the "learned" information so they can deter existing threats and repel the next attack using the same method. We share information with our academia, industry, and government partners so similar methods of attack can be thwarted across the domain. Our goal is to move away from this reactive process and develop a heuristic capability. Rather than operators having to inform the sensors about each new attack attribute, the sensors themselves will recognize and repel similar attack patterns. Automating this process would further allow us to devote capacity to expanding defensive or mission assurance operations.

Previously, we did things for the sake of the network itself, as if it were the end objective. This resulted in defending every part of the network essentially the same. Our defensive architecture was deployed to defend critical mission systems, core services, and business systems equally. Our primary defensive organization, the Air Force CERT, could not easily distinguish critical mission systems from routine business systems at a base. Today, this is changing. Emphasis is on supporting operational missions dependent on cyberspace. The focus is on the mission, not the network. This fundamental shift in perspective has driven both how AFSPC crafted the AF Cyber Core Function Master Plan and how AFCYBER refocused its operational activities.

Operationally Leverage Cyberspace Capabilities

Cyberspace operations encompass more than the management and configuration of hardware and software. The Air Force can leverage cyberspace to create integrated effects to respond to crises and conduct uninterrupted operations. As mentioned earlier, instead of responding to the cyberspace environment, we can leverage it to our advantage and our enemies' disadvantage. This provides myriad opportunities to develop and provide new capabilities to the war fighter while offering our adversaries new avenues of attack if we do not fully understand the environment we have created. The repercussions of this new environment must be considered when developing tools and extending the domain to austere locations.

We have come a long way in changing our priority from network assurance to mission assurance. Airmen have begun to distance themselves from a "service provider" maintenance mentality and transition to a "complete the mission" focus. A great example of efforts in this area is support to RPA missions and the objective of operating through a cyberspace attack or outage and accomplishing the mission. Providing mission assurance required extensive front-end mapping to understand the various links from the United States to the overseas flight. The system was designed with over 100 touch points, many of which are not military-controlled, across several different networks, making it critical to establish relationships with commercial organizations. The forward commander of joint air assets prioritizes the most critical RPA missions, and then our operations center identifies and takes proactive steps to ensure the availability of key nodes and failure points along the network infrastructure. While we cannot assure every RPA, we can focus our resources on the highest-priority missions to deliver the greatest downrange advantage. This provides a stark contrast to previous net-focused priorities that resulted in equal defense across the network.

In addition to mission assurance, we are engaged in global operations as the Air Force cyber force provider to US Cyber Command. Over the past two years, our operational units have conducted 17,000 computer network operations in support of combatant command and national agency taskings. Our Airmen executed pursuit of an HVT through computer network exploitation that enabled special operations forces to eliminate the target. We have directly supported objectives to disrupt terrorist command and propaganda efforts. Cyber represents an alternative; it can provide kinetic effects while using nonkinetic capabilities.

COCOMs are beginning to recognize these alternative capabilities and incorporate cyber early in the campaign planning process. Lt Gen Michael Basla, while Air Force Space Command vice-commander, said senior commanders had asked him for the "menu of nonkinetic cyberspace capabilities so they can integrate those into their planning processes." Cyber capabilities are driving a change in the way we plan, and they require flexibility and a focused, detailed understanding of the cyber environment. We are leveraging the Air Force intelligence community to achieve full-spectrum mission objectives.

To support theater planning for operations in and from cyberspace, target development plays a key role in application of capabilities, especially with respect to industrial control systems (ICS). Rail yards, ports, and power plants are generally built in the same manner worldwide, whether in Tennessee or Ukraine. The initial 80 percent of system understanding can be performed with industry research; the last 20 percent of interface with a particular system requires substantive effort to establish the connections necessary for effective capability employment. Similar to our defensive discussion in figure 1, we currently provide a niche capacity and nascent capability to the war fighter. With constant cyber funding and resources gained from proactive defense, OPLAN-level niche targets, such as ICS infrastructure, offer opportunities to expand combat effectiveness in a resource-constrained environment.

There is a lot of angst on the issue of authorities, and most of it stems from a lack of understanding of how to leverage the necessary authorities to accomplish the mission. Flexibility within the law allows leveraging all the authorities necessary to accomplish the mission without necessarily having a position that bestows the authority on 24 AF. War fighters routinely operate within their inherent Title 10 roles while leveraging the NSA's SIGINT authorities (Title 50) to support planning and targeting requirements at the tactical, operational, and strategic levels. War-fighter requirements are submitted to the NSA via the national SIGINT requirements process (NSRP) and are vetted and serviced based on national and theater priorities. This system works well and has been tested in the crucible of war many times. Likewise, 24 AF has units assigned, which are Title 10 units but have a US Signals Intelligence Directive (USSID) that defines the limits and processes they use to collect signals intelligence under the oversight of the Air Force Intelligence, Surveillance, and Reconnaissance Agency and the authority of the NSA. These units routinely move between conducting missions under both their Title 10 and Title 50 hats.

Title 32 authorities define how National Guard units support their respective state. Oft time Air National Guard forces can rapidly transition from Title 32 to support Title 10, all the while exercising caution to ensure Guard members are not put in positions exceeding their authority. For example, when an Air National Guard F-16 is on alert supporting NORTHCOM's air sovereignty mission, it can be training under Title 32, but when it is scrambled, it immediately transitions to a Title 10 role. Conversely, when a natural disaster strikes a state, active duty forces are limited in what they can do under Title 10, but National Guard forces from that state, under the direction of their governor, have more flexibility. This is important when we look at operations in the cyber domain, especially associated with the nation's cyber infrastructure. Industrial control systems are becoming ubiquitous and operate everything from power, water, and fuel systems to building alarms and environmental systems. Title 10 forces assigned to 24 AF have the authority to assess and defend the ICS on a military base. However, they have no authority to deal with systems off base that are essential to military operations. This is a Department of Homeland Security (DHS) responsibility. Though, under certain circumstances, National Guard units, when invited by the civilian entity or acting under the authority of their governor under a declared state of emergency, can be called up to defend of these systems. Interagency policy must continue to evolve and enable these units to synchronize efforts between National Guard and active duty forces to ensure the mission is not interrupted by attacks on the ICS infrastructure off base. Sharing of intelligence and vulnerabilities must also be improved. Today, the national ICS CERT at Idaho National Laboratory performs this function under the authority of the DHS. Synchronizing the ICS CERT efforts with military ICS defensive measures must continue to improve if we are to provide a comprehensive defense of our critical national infrastructure.

Twenty-fourth Air Force can also leverage law enforcement authorities (Title 18) when necessary through our embedded Office of Special Investigations (OSI) support. The OSI works with other law enforcement agencies to investigate cyber crime impacting Air Force networks.

Protecting our information lines of communication and understanding the adversary's key information lines of communication are within the 24 AF's set of responsibilities. We must consider information our key center of gravity and understand what particular information is mission critical to our success. This is not as easy as it may first seem. Are precision navigation and timing our most valuable information, or are timely communications with our airborne assets, including control links to our remotely piloted aircraft? We could expand this list considerably, but the point is made. The difficulty comes when we map the information flows to the supporting infrastructure. Without this level of detail, we cannot adequately defend mission-critical information.

We must also analyze the information centers of gravity of our adversary. This obviously includes those information lines of communication essential to its military operations, but it also includes other information lines of communication that impact the adversary's populace, allies, and supporting entities (including nonstate actors). Similarly, it is critical to understand the information lines of communication that support the adversary's infrastructure, including machine-to-machine communications. By understanding these essential information pathways and systems, we can produce strategic effects without ever staging our forces near an adversary's weapon systems.

Build and Deliver Combat Power

A proper foundation is critical to building a strong structure. It starts with early exposure to science, technology, engineering, and mathematics (STEM). The Air Force supplements the foundation with formal training to create the skilled technical workforce required to manage and protect its cyber resources and facilitate mission users.

A successful STEM program requires collaboration and partnerships with local and national academic and civic leaders. At the high school level, CyberPatriot is the premier national cyber defense competition. It inspires students toward careers in cyber security and other STEM disciplines. At the college level, students compete at the National Collegiate Cyber Defense Competition, and future cyber defenders test their acumen in the National Security Agency's Cyber Defense Exercise. For Reserve

Officer Training Corps cadets, the Advanced Course in Engineering summer program consists of an instructional component and cyber war games, hands-on internships, and cyber officer development that focuses on the study of cyber and its unique leadership challenges. The Air Force Academy's first cyber competition team won the 2012 Cyber Defense Exercise while competing against other service academy cadets, DoD postgraduate students, and the Royal Military College of Canada. In the same week, the team traveled to San Antonio, Texas, and placed second in the National Collegiate Cyber Defense Competition out of 136 teams. In such a dynamic environment, relying only on a STEM background is insufficient for continued success. That is why the AF has established deliberate processes for training and certification of its cyberspace professionals. Undergraduate cyber training (UCT) is a rigorous six-month program to provide foundational training for new cyber officers and enlisted personnel. Intermediate network warfare training builds on UCT and delivers qualified operators prepared to serve in a wide range of positions. Mission qualification training provides unit and position-essential instruction. Similar to the Space 200 and 300 programs, cyber professionals attend Cyber 200 or 300 taught by the Air Force Institute of Technology. These courses provide the career force with continuing education. Last month, we borrowed a page out of our air and space domains by graduating the first weapons instructor course class at the Air Force Warfare Center at Nellis AFB, Nevada. This course teaches professionals to integrate capabilities across air, space, and cyberspace to deliver precise effects. In an effort to increase joint capacity, our sister services are invited to participate in future classes.

DoD training and certification standardization, to include the Guard and Reserve, is key to the nation's success in cyberspace. To emphasize the need for the same training and certifications, the organized Reserve Corps was formally established in 1948 by the Truman administration, but it was not until 1973 when Secretary of Defense James Schlesinger declared the Total Force policy. The Air Force Reserve was held to the same readiness standards and inspections; mobilization planning, operational evaluation, and participation in exercises enhanced Air Reserve Component (ARC) capabilities. In cyber, we can incorporate that same readiness standard, but we must leverage the ARC differently than we have traditionally. We require associations, with flexible drilling, that allow Guard and Reserve members to perform active missions, not merely training scenarios. In the dynamic cyberspace environment, continued engagement is the best way for the ARC to both support our substantial steady-state mission requirements and be optimally trained and prepared to mobilize, if needed, for a more robust cyber defense of our nation. That continued engagement by our citizen Airmen also enables us to leverage private-sector skills while at the same time providing knowledge gained from bona fide mission experience that should be beneficial to civilian cyber roles in local communities and improve the defenses of industry and government, bringing mainstays of cyber to Main Street. This fuels collaboration between the DoD and the private sector and raises the overall level of national cyber security.

Within the strategy document titled *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, Secretary of Defense Leon Panetta makes clear that cyberspace forces are a key component to the nation's ability to project combat power. Specifically, "Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and space." To provide resilient, cost-effective cyberspace capabilities for the joint war fighter, an innovative, rapid, tool development process must be accompanied by an acquisition program that reflects an immediate-, medium-, and long-term systems approach.

A factor that hinders the development of cyber capability is the outmoded practices, policies, and rules that guide cyber acquisition from the top down. The current acquisition system was constructed and optimized to support the acquisition of large-scale weapon and training systems. It is based on the five-year Program Objective Memorandum (POM) cycle, which starts two years out from the beginning of the planned acquisition. This drives us to develop large acquisition programs that can survive the vetting process within the Air Force and the Office of the Secretary of Defense. These programs are built from requirements that are defined years in advance and remain relatively static throughout the POM process. The end result is acquisition of outdated equipment and inflexibility that prevents adapting leading-edge technology while it is still leading edge. One example is the modernization of the Air Force boundary. Prior to 2010, the Air Force boundary was defined by more than 140 Internet points of presence, one at each base. But since 2003, we have been consolidating these Internet gateways into 16 regional gateways that now define the boundary to the Air Force network. While the benefit of consolidating the boundaries is indisputable, the "controls" on program execution illustrates the challenge with applying traditional acquisition methodology to cyber modernization and domain design. Planning for the program began in 2003, and the final gateway was fielded in 2010. By the time the last gateway was fielded, the equipment was obsolete. Although certainly willing to innovate, the process prevented alternatives which kept pace with an intensely dynamic man-made, necessitating modernization of the gateways as soon as they were fielded.

Complicating things further, acquisition programs often field capabilities without a clear understanding of their operational impact on the defensibility, operability, and sustainment of the domain (on behalf of all who use it). Standard acquisition practices often resulted in the fielding of multiple brands and/or standards of network components such as routers and firewalls, adding to the operational burden for the units maintaining and operating the equipment. For example, the Air Force network infrastructure from DISA to the base boundaries includes 1,800 same-brand network routers and switches. Personnel trained on that standard brand are very skilled at operating and configuring those routers. However, a subset of bases deviated with four different brands or variants of routers and switches…without interface testing or a standard for configuration. A small communications team on a base can be trained to efficiently operate nonstandard gear, but as operations are consolidated at network operations units that have enterprise-wide responsibilities, it places undue strain on significantly reduced resources. In theory, these dissimilar infrastructure devices should all communicate with little difficulty, and configuration should be similar. But it does not work that way. While this adds diversity to the network, the ultimate result is a highly heterogeneous network architecture that significantly complicates updating and maintaining these devices. Central management becomes difficult if not impossible, and inevitably, some of the devices do not get properly configured and thereby create vulnerabilities. In addition, training and manpower requirements to maintain such a heterogeneous network cause an unacceptable burden on the already limited cyber manpower resources. This creates a huge workload for Air Force network operations units and adversely impacts the reliability of service to some bases. This problem will be exacerbated as the Air Force continues to offload work from the shrinking base communications units to the network operations units.

One additional innovation involves Air Force Material Command (AFMC) working with AFSPC to establish a Cyber Solutions Center in San Antonio. This center of cyber innovation primarily supports rapid acquisition providing cutting-edge capabilities for the joint war fighter. It has acquisition professionals from AFMC, science and technology expertise from Air Force Research Laboratory, and is integrated with the cyber development expertise resident in the 24 AF. This team of acquisition, technical, and operational experts is integrated with the daily operations of 24 AF and becomes a powerful engine for innovation that greatly increases the Air Force's ability to create and integrate new and innovative technology. This type of collaboration, along with DoD standardization, increases the capacity of a skilled technical workforce to leverage full-spectrum capabilities to meet the Air Force vision of global reach, global power, and global vigilance.

One opportunity 24 AF is working, in close coordination with AFSPC leadership, is revamping the current program for increasing bandwidth and connectivity at the bases. The legacy program is primarily focused on older, wired technology and fails to leverage the capabilities available with today's wireless technology. By leveraging new technology, we will provide ubiquitous connectivity to base users, reduce infrastructure, increase reliability and resilience, and enable control of government-owned devices to enhance productivity.

Conclusion

Twenty-fourth Air Force is extremely proud of the part its Airmen play in defending the nation in cyberspace at the "speed of cyber," that is, Mach 880,000. The Air Force core contribution to specific joint operations and to the nation's defense is its ability to command, control, and precisely apply forces to provide inherent reach, power, and vigilance—globally. We have effectively leveraged the cyber domain to enhance these core capabilities and to expand operational effectiveness in every engagement. However, this drives a dependency on the networks that directly exchange critical information, often with little human involvement. This trend is only going to increase, as is the trend for adversaries to undermine or contest our ability to leverage the domain. We cannot revert to the days when we, and our platforms, operated without reliable, near-instantaneous access to information—time marches on, and innovators surge forward.