AIR FORCE CYBER COMMAND
STRATEGIC VISION

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
FEB 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Air Force Cyber Command Strategic Vision	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force. Air Force Cyber Command,Barksdale AFB,LA**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

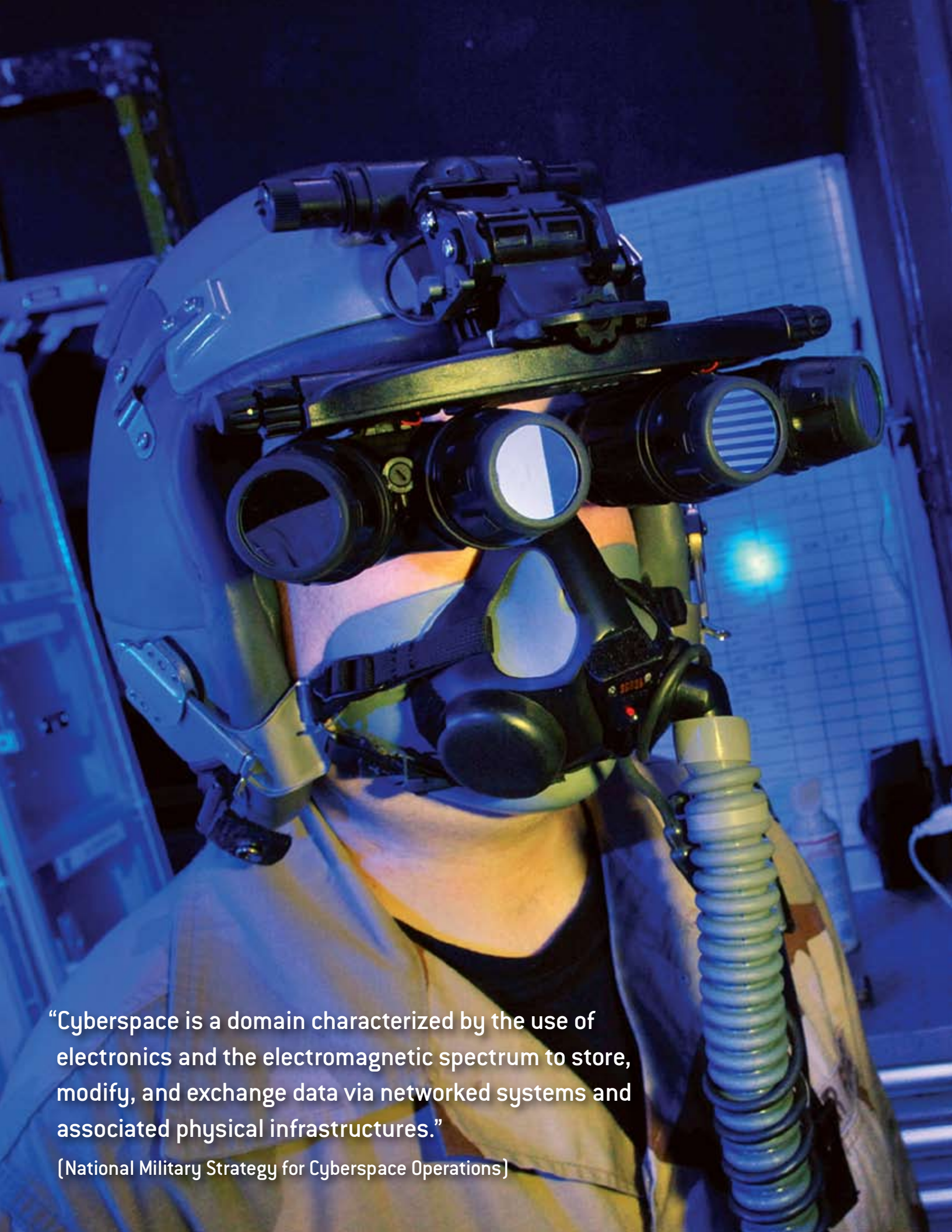
12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**24**	



"Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."

(National Military Strategy for Cyberspace Operations)

AIR FORCE CYBER COMMAND
STRATEGIC VISION

FOREWORD

Warfighters rely upon cyberspace to command and control forces in the 21st century. Revolutionary technology has presented cyber capabilities, which can provide decisive effects traditionally achieved only through kinetic means. Recognizing the domain's importance, Secretary of the Air Force Michael Wynne announced Air Force Cyberspace Command (Provisional) in September 2007 to bring together the myriad existing cyber capabilities under a single commander. This new command will provide combat-ready forces equipped to conduct sustained operations in and through the electromagnetic spectrum, fully integrated with global air and space operations.

As the nation's premier global, multi-dimensional maneuver force, the United States Air Force is charged with safeguarding America by dominating air, space, and cyberspace. We provide global vigilance, global reach, and global power in and through these domains with the agility, reach, speed, stealth, payload, precision, and persistence to deliver global effects at the speed of sound and the speed of light.

- Global Vigilance is the persistent, worldwide capability to keep an unblinking eye on any entity—to provide warning on capabilities and intentions, as well as identify needs and opportunities.
- Global Reach is the ability to move, supply, or position assets—with unrivaled velocity and precision—anywhere on the planet.
- Global Power is the ability to hold at risk or strike any target, anywhere in the world, and project decisive, precise effects.

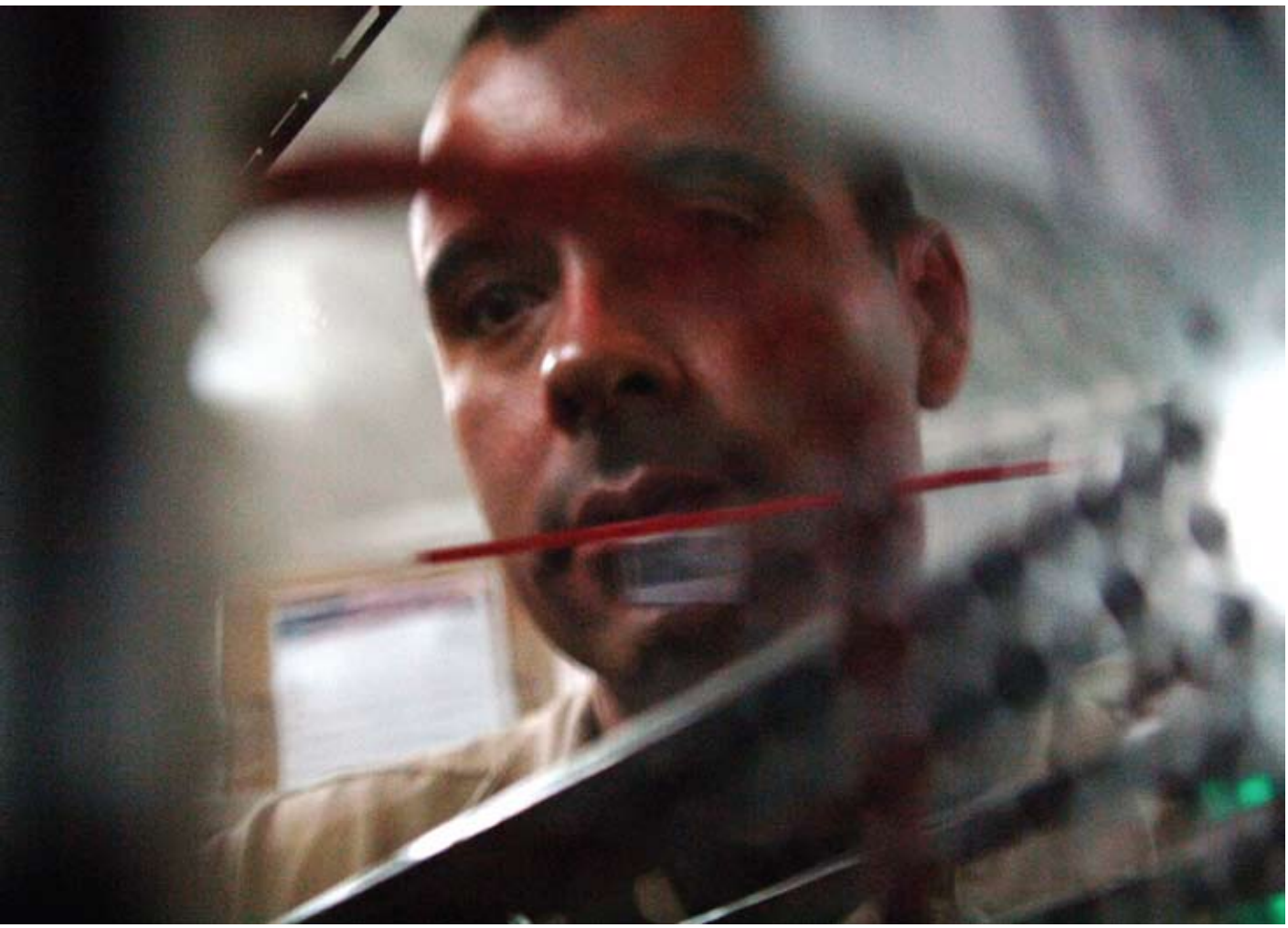
The Air Force permits joint freedom of maneuver in all warfighting domains: land, sea, air, space, and cyberspace. With this freedom, the Joint Force commander can achieve desired outcomes across the spectrum of military operations: from providing humanitarian relief to deterring war, to achieving desired policy aims, and ensuring joint maneuver in the other domains. The Air Force's ability to create—and capitalize on—a wide array of effects in peace, crisis, and war provides vast sovereign options for our military and political leadership.

The Air Force's non-negotiable commitment to America's Joint Team is to provide forces proficient across the full spectrum of military operations to protect the United States, its interests, values, and allies; deter conflict and prevent surprise; and, should deterrence fail, prevail against any adversary.

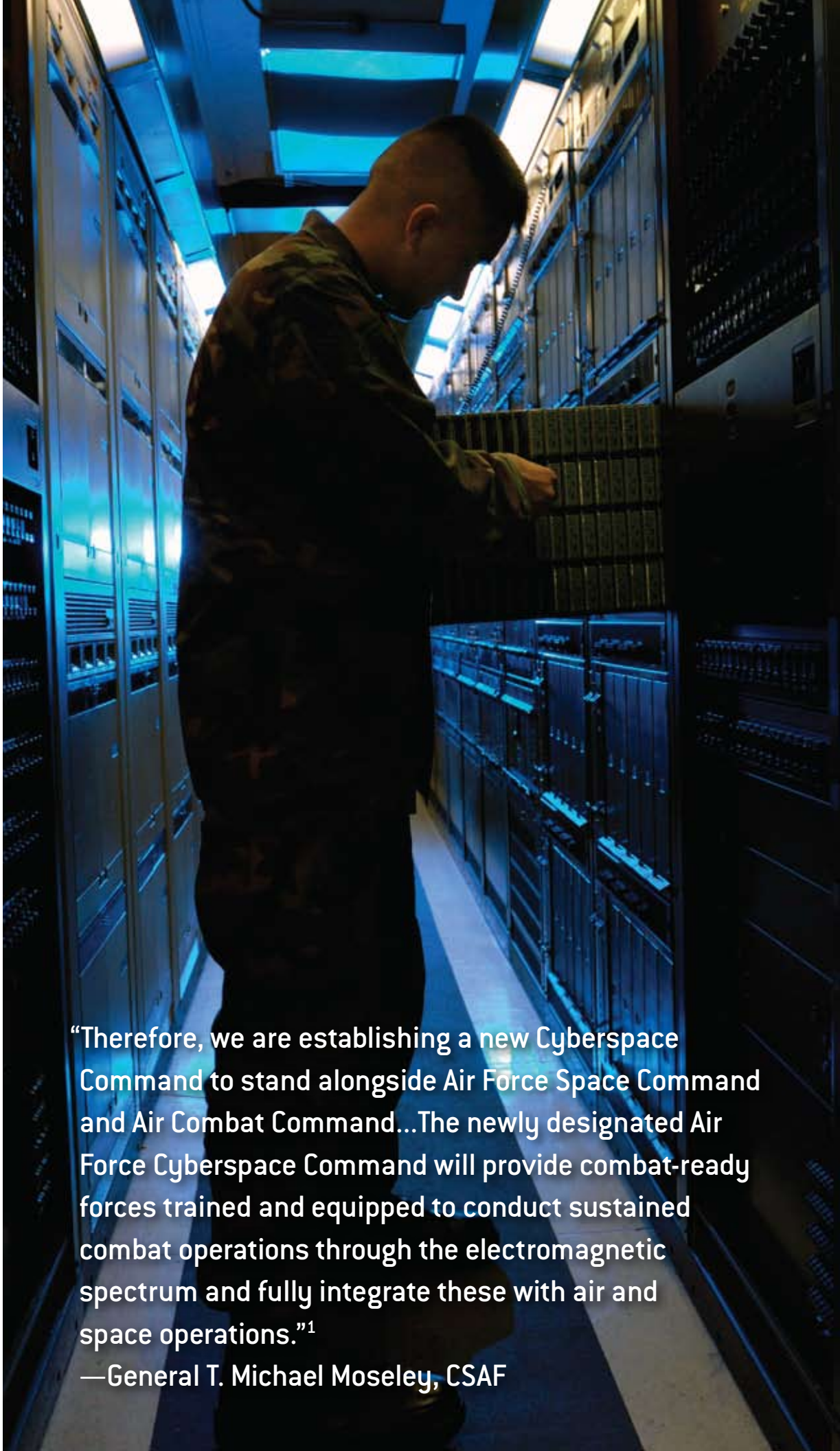
Mastery of cyberspace is essential to America's national security. Controlling cyberspace is the prerequisite to effective operations across all strategic and operational domains—securing freedom from attack and freedom to attack. We will develop and implement plans for maturing and expanding cyberspace operations as an Air Force core competency. We will provide decision-makers flexible options to deter, deny, disrupt, deceive, dissuade, and defeat adversaries through a variety of destructive and non-destructive, and lethal and non-lethal means. Finally, we will do this in friendly cooperation with our professional partners and teammates in other MAJCOMs, Services, COCOMs, and U.S. government agencies.

This *Air Force Cyber Command Strategic Vision* is a foundation for the tremendous work that lies ahead as the organization achieves initial operational capability in 2008 and postures for full operational capability in 2009. It explains the mission of Air Force Cyberspace Command in the context of the strategic realities faced by the United States and how our capabilities will enhance the Air Force's global vigilance, global reach, and global power, while expanding the options available to the Joint Force. Air Force Cyberspace Command will be a dynamic warfighting organization integrating capabilities, systems, and warriors to establish cross-domain dominance. The Strategic Vision describes how we will develop 21st century cyberspace warriors and how they will control cyberspace to deliver sovereign options for the defense of the United States.

WILLIAM T. LORD
Major General, USAF
Commander, Air Force Cyber Command (Provisional)



CONTROL
CREATE
DELIVER



"Therefore, we are establishing a new Cyberspace Command to stand alongside Air Force Space Command and Air Combat Command...The newly designated Air Force Cyberspace Command will provide combat-ready forces trained and equipped to conduct sustained combat operations through the electromagnetic spectrum and fully integrate these with air and space operations."[1]

—General T. Michael Moseley, CSAF

PART ONE: VISION STATEMENT

Air Force Cyberspace Command's mission is to provide combat-ready forces trained and equipped to conduct sustained combat operations in and through the electromagnetic spectrum, fully integrated with air and space operations. The Air Force was operating in cyberspace before the advent of the computer. This vision statement captures our non-negotiable commitment to produce sovereign options for the United States by developing, maintaining, and enhancing cyberspace capabilities to conduct sustained and integrated combat operations in and through the electromagnetic spectrum.

Secure Our Nation by Employing World-Class Cyberspace Capabilities to Control Cyberspace, Create Integrated Global Effects, and Deliver Sovereign Options

Secure Our Nation

Our overarching goal is the security of the United States and attainment of our national objectives. Cyberspace is critical to our nation's power and influence. Cyberspace is the foundation for a growing portion of our commerce, critical infrastructure, and national security. Securing our nation's critical infrastructure will increasingly depend upon effective cyberspace operations and exploitation of cyber technology. Before the inception of radar, Airmen fought and won battles in the electromagnetic spectrum. We will build upon this legacy by enhancing the scope and breadth of our cyberspace capabilities.

Employing World-Class Cyberspace Capabilities

We will develop, sustain, and enhance our capabilities both to defend national interests from attack and to create effects in cyberspace to achieve our national objectives. We will integrate our capabilities, systems, and warriors to increase the impact of our military power. This will ensure our ability to operate in and control cyberspace, convey operational advantages to our forces in all domains, and prevent surprising events within cyberspace that are contrary to our national interests.

[1] General T. Michael Moseley, USAF, Chief of Staff, in prepared remarks to House Armed Services Committee, 28 February 2007. See http://armedservices.house.gov/pdfs/FCAF022807/WynneMoseley_Testimony022807.pdf, Section 1.2.

Control Cyberspace

Cyberspace integrates operations across all other domains, facilitating interdependent offensive and defensive operations to achieve dominance at the place and time of our choosing. Controling cyberspace will allow us to create the full spectrum of desired effects across future integrated battlefields. The Air Force has routinely employed electromagnetic capabilities to engage the enemy, establishing and sustaining the air and space superiority that has proved decisive in winning the nation's battles and wars. We will leverage this expertise and further develop capabilities enhancing our freedom of action while limiting the flexibility of our adversaries.

Create Integrated Global Effects

The Air Force uses agility, speed, and precision to deliver kinetic and non-kinetic, lethal and non-lethal, global and theater effects. Cyberspace is the medium for electronic warfare, command, control, communications, surveillance, and reconnaissance. It allows us to create and execute capabilities across all domains, providing reach and speed, distance, stealth, massed effects, and precision, irrespective of natural and man-made boundaries. By controlling cyberspace, we will dissuade and deter conflict. If our adversaries underestimate our resolve, we will engage them in the electronic battlespace and defeat them. We will be the best at what we do, and we will accomplish our mission as part of the Joint Force.

Deliver Sovereign Options

Fulfilling our national security objectives increasingly depends upon our ability to control and operate in the wide expanse of the electromagnetic spectrum. The United States must have the freedom to operate in this domain—we must use cyberspace to secure freedom from attack and freedom to attack.

In 2005, the United States Air Force adopted a new mission to integrate our air, space, and cyberspace capabilities. At that time, the Air Force began reorganizing these capabilities to forge a major command dedicated to organizing, training, and equipping forces for warfighting operations in the electronic battlespace. Today, cyberspace operations are a defining component of the Air Force mission—as important as air and space operations.

THE CYBER DOMAIN


NO SMOKING

PART TWO: THE STRATEGIC ENVIRONMENT AND CYBERSPACE

THE STRATEGIC ENVIRONMENT

The United States faces a strategic environment that is unpredictable and increasingly dangerous. It is characterized by the confluence of globalization, economic disparities, and competition for scarce resources; by the diffusion of technology and expansion of electronic capabilities that create significant vulnerability; and by systemic dislocations impacting state and non-state actors and international institutions. Our competitors recognize the United States is a globally networked society increasingly dependent on the cyberspace domain. Essential process controls in manufacturing, public utilities distribution, banking, communications, and national security have shifted to integrated networked systems. This trend is expanding, and our economy and national security are increasingly exposed to the associated risks. Resources for conducting harmful attacks are widely available and inexpensive, creating a low cost of entry for any adversary. The attacks on the United States on September 11, 2001 have forced us to reexamine our vulnerabilities.

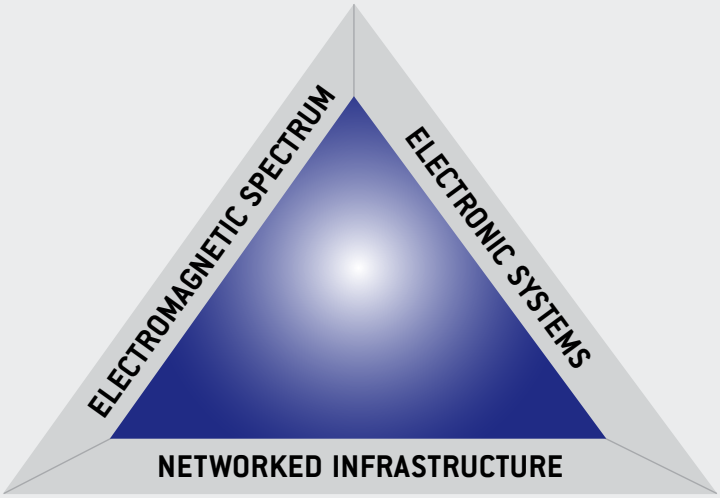
CYBERSPACE

Cyberspace encompasses the electromagnetic spectrum with its distinctive physical properties and those of the manmade electronic systems created to operate across the domain. Exploiting improved technologies makes it possible to enhance global vigilance, global reach, and global power by delivering increasingly larger information payloads, higher levels of energy, and increasingly sophisticated effects. Cyberspace allows us to overcome the limitations of distance and time and the barriers of land and sea. Figure 1 (on page 8) depicts the key components of cyberspace power—the science of the electromagnetic spectrum, the technology of electronics, and integrated manmade infrastructure.

Cyberspace links operations in all other domains, facilitating interdependent offensive and defensive operations to achieve situational dominance at a time and place of our choosing. Effects in cyberspace can occur nearly simultaneously in many places, can be controlled precisely, be massive or precise, enduring or transitory, kinetic or non-kinetic, lethal or non-lethal. Operations in cyberspace conform to the Air Force's traditional strengths: controlling tempo and initiative using global reach and agility; generating significant effects with minimal collateral damage using precision engagement; and minimizing exposure of forces.

Achieving and maintaining control of cyberspace is critical to effective operations, enhancing our current advantages in precision engagement, situational awareness, and operational reach. Figure 2 depicts how American combatant commanders utilize inte-

THE CYBERSPACE DOMAIN



CYBERSPACE *"A domain...of ELECTRONICS...the ELECTROMAGNETIC SPECTRUM...NETWORKED systems and associated physical INFRASTRUCTURES."* **National Military Strategy for Cyberspace Operations**

FIGURE 1

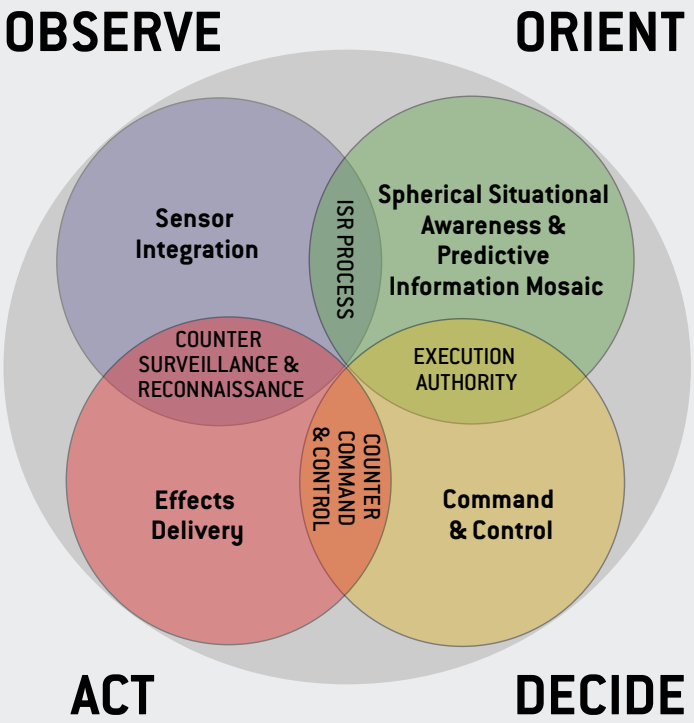


FIGURE 2

grated surveillance and reconnaissance, situational awareness and battle management to deliver effects and counter adversary action across all domains.

Cyberspace control will be the foundation for effective operations across strategic, operational, and tactical levels, allowing the United States to create a full spectrum of effects across future battlefields. These effects will disrupt, degrade, or deny our adversary's ability to attack.

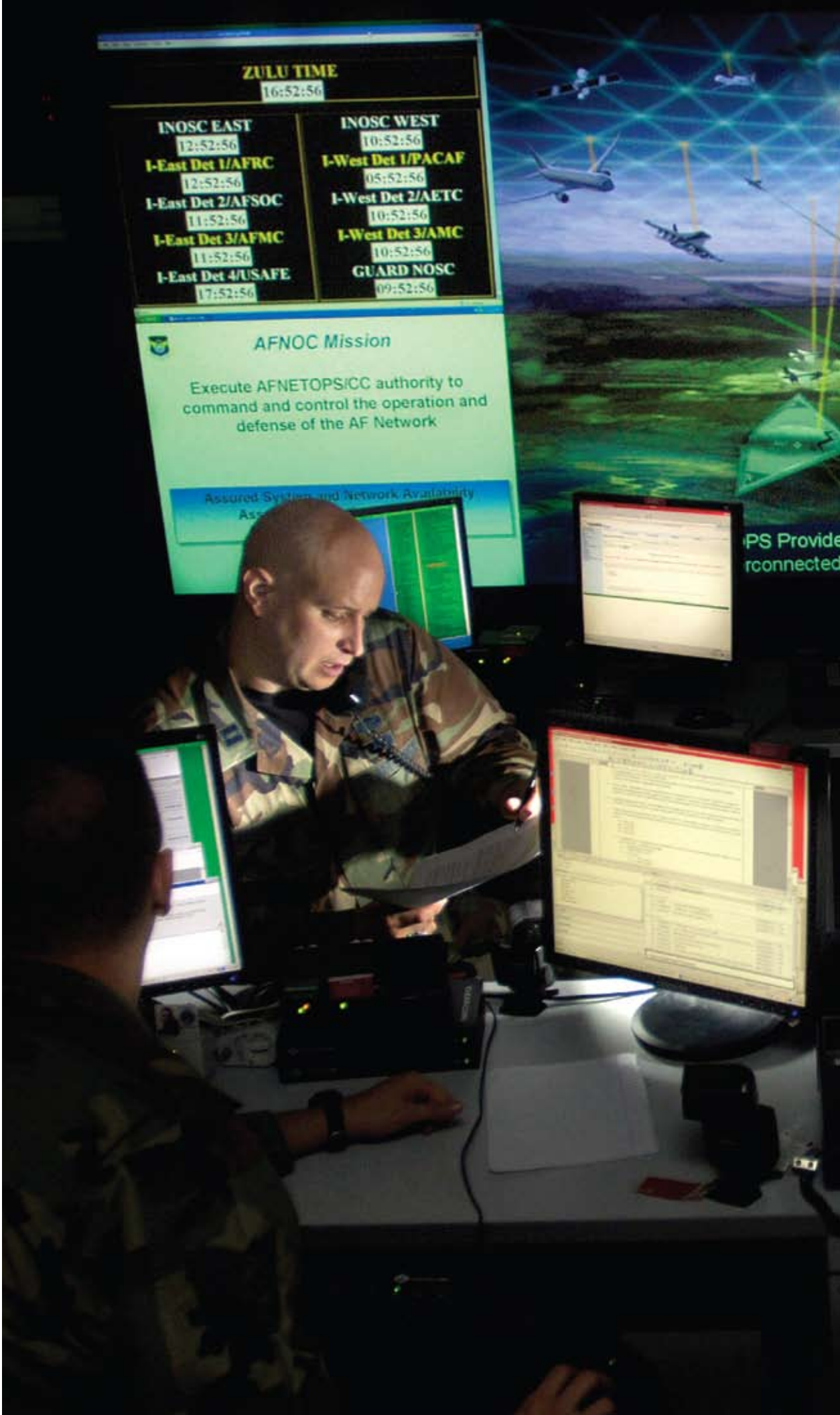
CYBERSPACE SUPERIORITY

Global Vigilance, Reach, and Power Across the Electromagnetic Spectrum

Global vigilance requires the ability to sense and signal across the electromagnetic spectrum. Global reach requires the ability to connect and transmit, using a wide array of communications networks to move data across the earth nearly instantaneously. Global power is the ability to hold at risk or strike any target with electromagnetic energy and ultimately deliver kinetic and non-kinetic effects across all domains. These cyberspace capabilities will allow us to secure our infrastructure, conduct military operations whenever necessary, and degrade or eliminate the military capabilities of our adversaries.

Controlling this domain ensures friendly use of the electromagnetic spectrum while selectively denying this capability to our adversaries. As part of the Joint Force, Air Force Cyberspace Command will deliver the capability to engage rapidly and degrade or destroy an adversary's terrestrial, air, and space infrastructure, and his electronic attack systems. Successfully controlling cyberspace creates the potential to achieve victory before a kinetic shot is fired. Our cyberspace capabilities will dissuade and deter potential aggressors, but if deterrence fails, our mastery of it will help to ensure that we prevail.

DOMINATE CYBERSPACE


ZULU TIME
16:52:56
INOSC EAST
12:52:56
I-East Det 1/AFRC
12:52:56
I-East Det 2/AFSOC
11:52:56
I-East Det 3/AFMC
11:52:56
I-East Det 4/USAFE
17:52:56
INOSC WEST
10:52:56
I-West Det 1/PACAF
05:52:56
I-West Det 2/AETC
10:52:56
I-West Det 3/AMC
10:52:56
GUARD NOSC
09:52:56
AFNOC Mission
Execute AFNETOPS/CC authority to command and control the operation and defense of the AF Network

PART THREE: ACCOMPLISHING THE MISSION

Cyberspace operations must provide our commanders with enhanced means to execute decision-making, accelerate operations, provide battle changing opportunities, and deny those capabilities to our adversaries. Our adversaries clearly understand this reality. They have declared the intent to target and degrade our air and space superiority by defeating us in the electronic battlespace. We must ensure the Air Force has the capability to achieve and sustain control of cyber space whenever and wherever the nation requires the use of military force. Air Force Cyberspace Command is tasked with achieving this objective.

CREATING CAPABILITIES TO DOMINATE CYBERSPACE

The capabilities and forces required to achieve effects in cyberspace can fall into several broad categories: *Using the Domain* (Cyberspace Attack and Force Enhancement); *Controlling the Domain* (Cyberspace Defensive Operations and Cyberspace Offensive Counteractions); and *Establishing the Domain* (Global Expeditionary Cyberspace Operations, Command and Control Network and Security Operations, and Cyberspace Civil Support Operations). Determining the capabilities required to achieve a particular effect in support of an overall operation depends on the desired operational outcome and the characteristics of the portion of cyberspace being contested.

Using the Domain

Air Force Cyberspace Command will leverage friendly operations across the electromagnetic spectrum and counter any adversary operating in the domain. We will maintain a multi-dimensional perspective, recognizing that cyberspace capabilities will synchronize and integrate combat operations across air, space, land, and sea. Offensive operations in cyberspace involve both force employment and force enhancements. Defensive warfighting in cyberspace will counter an adversary by attacking his networked systems while simultaneously defeating enemy attempts to threaten our own systems. Through this broad mission area, we will gain military advantage to ensure operational freedom of action through cyberspace attack, the delivery of cross-domain effects through cyberspace force enhancement, and the conduct of cyberspace support operations.

Cyberspace Attack Operations: Cyberspace effects gained from emerging technology, such as directed energy, include: sensor disruption, data manipulation, decision support degradation, command and control disruption, and weapon system degradation. Cyberspace attacks can be conducted on an adversary's terrestrial, airborne, and space-based communication infrastructure as well as his forces, equipment and logistics. Air Force Cyberspace Command will enhance traditional air superiority by generating effects in and through a larger portion of the domain. Air Force Cyberspace Command will engage across the electromagnetic spectrum and employ electromagnetic capabilities against assets in the other domains.

Force Enhancement Operations: Air Force Cyberspace Command will oversee sensors and data integration to connect global, theater, and special operations centers to provide warfighters global situational awareness. A globally linked command and control architecture will provide reachback between regional commanders and other operations centers. Command and control systems must account for cyberspace forces and have the ability to plan for their employment and task them accordingly.

Controlling the Domain

Operating effectively in cyberspace requires a command and control system to synchronize cross-domain attack operations and deconflict friendly use of cyberspace. While enhanced technology has allowed greater use of the electromagnetic spectrum, it has also caused a dramatic increase of electronic fratricide.

Cyberspace Defensive Counter-Operations: Air Force Cyberspace Command will defend friendly forces and vital interests from hostile attacks. Cyberspace defense consists of active and passive cyberspace operations including employment of defensive measures designed to destroy attacking adversary forces or reduce their effectiveness. Cyberspace defense includes measures to preserve, protect, recover, and reconstitute friendly cyberspace capabilities before, during, and after a hostile attack. Cyberspace defense encompasses cyberspace attack deterrence, cyberspace attack mitigation and survivability, attack attribution, vulnerability detection and response, data and electronic system protection, and electromagnetic and infrastructure protection.

Cyberspace Offensive Counter-Operations: Cyberspace favors offensive operations. These operations will deny, degrade, disrupt, destroy, or deceive an adversary. Cyberspace offensive operations ensure friendly freedom of action in cyberspace while denying that same freedom to our adversaries. We will enhance our capabilities to conduct electronic systems attack, electromagnetic systems interdiction and attack, network attack, and infrastructure attack operations. Targets include the adversary's terrestrial, airborne, and space networks, electronic attack and network attack systems, and the adversary itself. As an adversary becomes more dependent on cyberspace, cyberspace offensive operations have the potential to produce greater effects.

Establishing the Domain

Effective operations within cyberspace require global expeditionary cyberspace operations and network operations security that ensure cross-domain freedom of action for United States and allied forces and deny that same freedom to our adversaries.

Global Expeditionary Cyberspace Operations: To develop and execute a fully integrated airpower strategy in support of strategic, operational, and tactical objectives, we must man air operations centers with cyberspace operators trained at the operational level of war. To support theater objectives, we will develop cyberspace force packages as part of our expeditionary air and space forces to provide the continued and effective means to deliver effects to meet the Joint Force commander's objectives. Air Force Cyberspace Command will deploy and present forces to the supported Joint Force commander, under his operational or tactical control, as appropriate. We will build and maintain flexible cyberspace capabilities to support strategic-level objectives. This will require unprecedented levels of global coordination—cross-command, interservice, and interagency coordination.

Command and Control of Network and Security Operations: We will work with the Joint Force to establish complete situational awareness of both friendly and adversary operations in cyberspace. In part, this will be accomplished by finding, fixing, and targeting, and neutralizing threats. We will also embark on building relations with other involved U.S. government agencies and friendly nations to ensure the availability of a safe and viable electromagnetic infrastructure.

Cyberspace Civil Support Operations: Air Force Cyberspace Command will support the defense and protection of critical infrastructure. We will also support the defense industrial base in protecting sensitive information. The secure functioning of cyberspace is essential to our economy and our national security. We will act with federal, state, and local governments, as well as private sector parties to identify our dependencies and reduce our vulnerabilities to these threats before they can be exploited. We will ensure such disruptions of cyberspace are minimal and result in the least possible damage.

DEVELOPING THE 21ST CENTURY WARRIOR

Perhaps the most critical mission of Air Force Cyberspace Command is the development of full-spectrum professionals to employ core cyberspace capabilities across the entire range of military operations. While this force will initially draw from the strengths of existing operational and support career fields, we will identify and define specific cyberspace-focused career paths. We must develop a Cyberspace career path that is as full and viable as career paths for existing specialties. Airmen will enter the Air Force knowing they will become cyberspace operators.

Defining cyberspace competencies and capabilities is the first and most important step in building the Cyberspace warrior. This analysis will be based on needs and specific mission. This process will lay the

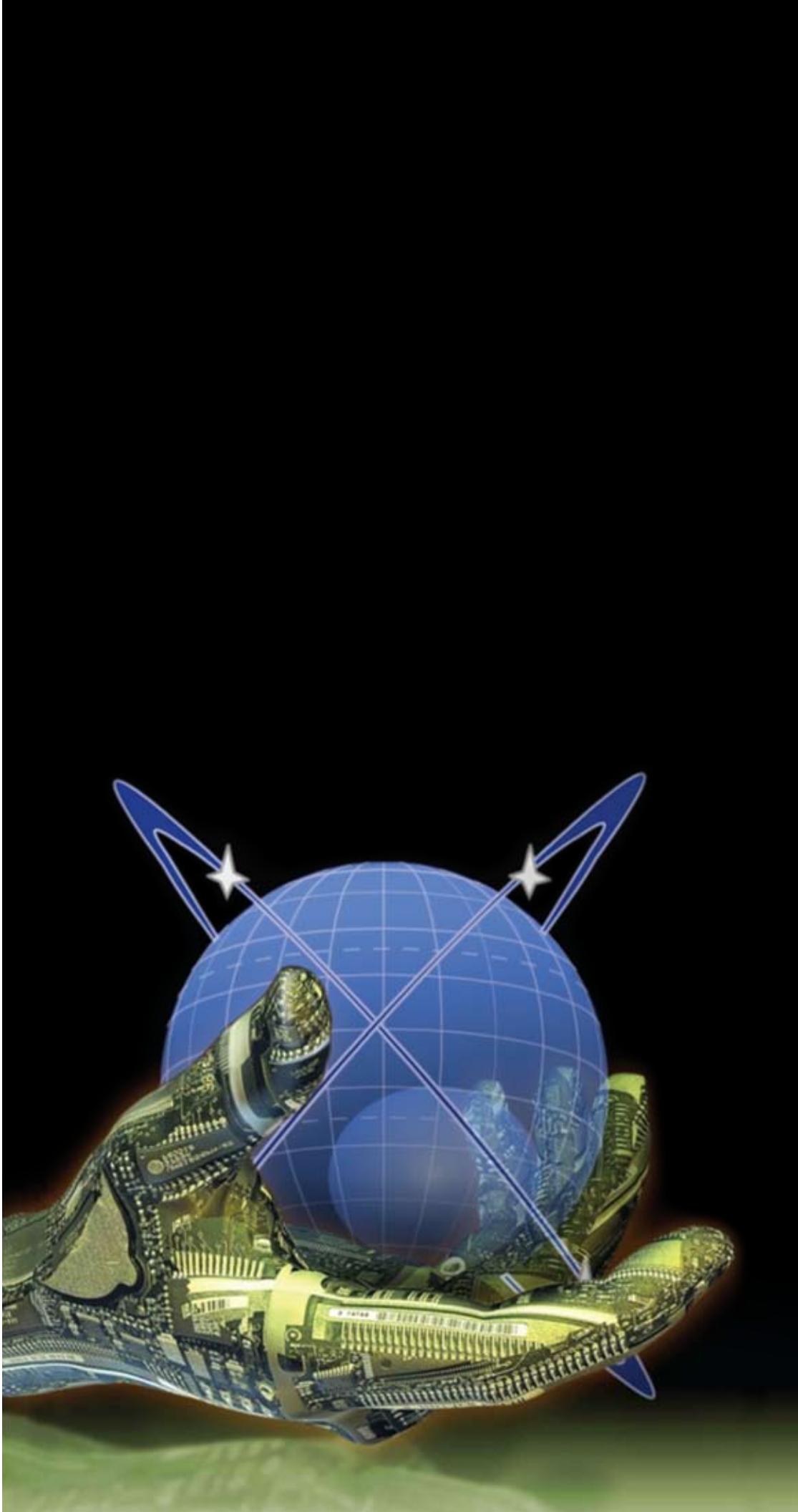
groundwork for a cyberspace-focused career field prepared to meet current and future manpower requirements.

Shaping the emerging cyberspace career force will match defined skills, competencies, and grades with capabilities-based cyberspace requirements to support the combatant commands. The initial approach for manning Air Force Cyberspace Command will consist of identifying personnel possessing cyberspace skills in electronic warfare, network warfare, and network operations for reclassification to new specialties and reassignment to new or realigned organizations. We will then establish a set of separate and tailored career fields to ensure cyberspace operations theory and skills can develop freely. The cyberspace career force will be shaped and sized to meet skill requirements consistently over the course of a full career.

Developing the cyberspace career force will require the right combination of pre- and post-accession learning experiences capable of planning and executing cyberspace operations at all levels of war. We will develop career field specific education and training programs including the development of a cyberspace weapons school with aggressor squadrons. The resulting professionally trained and credentialed cyberspace career force will further develop the theory of cyberspace power and engage with industry and academia to further enhance combat capability.

Sustaining the cyberspace career force will be essential to the long-term success of Air Force Cyberspace Command. To be truly effective in institutionalizing cyberspace power, the Air Force will have to adapt its culture to accept these new warriors. Cyberspace concepts must become part of the Air Force vernacular, and cyberspace warfare training must occur at each level of developmental education.

Delivering cyberspace career force capabilities will require changes to the personnel system to identify qualified Airmen with critical skills for presentation to combatant commands when required. The cyberspace career field will be managed as a total force, with skill sets being tracked across all Air Force components.



CONCLUSION

The *Air Force Cyber Command Strategic Vision* links the mission of Air Force Cyberspace Command to the 21st century strategic realities faced by the United States. We will provide combat-ready forces trained and equipped to conduct sustained offensive and defensive operations throughout the electromagnetic spectrum fully integrated with air and space operations. We will leverage Air Force cyberspace capabilities to counter our adversaries, to support operations in all domains, to create global and theater effects in support of the Joint warfighting team, and to deliver sovereign options to our national leadership.

We will achieve this vision through a holistic, agile, and evolutionary approach to science and technology, research and development, systems acquisition, operations, force structure, education, training, and doctrine in order to create and expand a set of cyber space capabilities that enhance our nation's sovereign options. The mission of Air Force Cyberspace Command is one means by which the Air Force will continue to endure as the world's premier 21st century air, space, and, now, cyberspace power.

.

Air Force Cyberspace Command...

Securing Our Nation by Employing 21st Century Cyber Capabilities
to Control Cyberspace, Create Integrated Global Effects,
and Deliver Sovereign Options

AIR FORCE CYBER COMMAND
STRATEGIC VISION