The United States Air Force Blueprint for Cyberspace

November 2, 2009

Foreword

Cyberspace is a critical global domain, in which the USAF will conduct integrated operations in support of Joint Force Commanders' needs. The United States is not alone in recognizing the asymmetrical advantages of this domain. Potential adversaries worldwide are rapidly improving or pursuing their own cyber capabilities. Attempts to disrupt or penetrate our networks are relentless. The blueprint that follows provides a framework to meet these challenges by evolving our culture and improving our capabilities.

Air Force Space Command as the lead USAF Major Command (MAJCOM) for cyberspace will execute this blueprint as a unified effort--working closely within the Air Force, and with sister services, combatant commands, Joint Staff and other partners to fully provide the necessary capabilities for the future.

C. ROBERT KEHLER
General, USAF
Commander, AFSPC
2 November 2009

Table of Changes

Date	No.	Page	Description
17 Mar 2010	1	13	Reference to Minuteman crossed out in Objective 5

Table of Contents

The United States Air Force Blueprint for Cyberspace

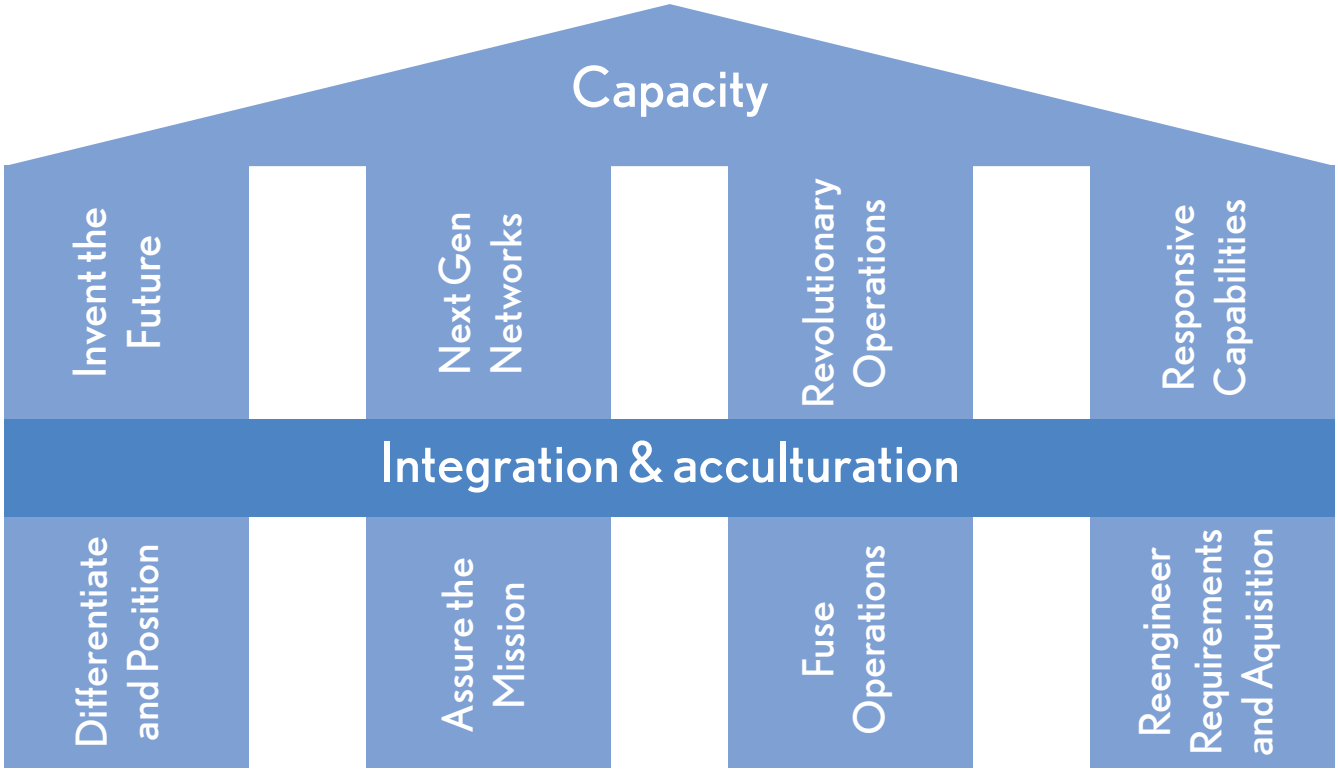
Purpose

The United States Air Force (USAF) Blueprint for Cyberspace provides commander's guidance and intent, identifies opportunities and delineates objectives and strategies that will shape USAF actions over the next five years. This document describes the first phase of a two-phase approach. It defines specific actions to align cyber activities and functions, to evolve and integrate the unique capabilities the USAF brings to the joint fight, and to build cyberspace operational capacity, including:

- Positioning the USAF with enhanced and differentiated capabilities complementing those of our sister services
- Assuring the mission by securing the USAF portion of DOD-Global Information Grid (GIG)
- Fusing cyber and intelligence functions to create seamless operations
- Establishing cyber requirements and re-engineering acquisition processes
- Institutionalizing a cyber culture and mindset

The second phase addresses longer-range objectives, including:

- Creating unique capabilities through innovation and integration
- Building the next-generation network/cyber infrastructure
- Refining operations to create synergies and seamless capabilities
- Fielding and further developing operationally responsive capabilities
- Achieving cyber integration and acculturation



Tenets of the USAF Blueprint for Cyberspace

Phase II of the USAF Blueprint for Cyberspace will be shaped by the results of several efforts currently underway:

- A summary of the information gathered on the future of cyberspace, and how to get ahead of the curve and create a sustainable advantage
- The analysis and recommendations for developing a coordinated USAF-wide effort for cyber innovation
- The plan for the next-generation secure architecture including an analysis of network information flow, technology and mission needs
- The analysis and recommendations for developing an integrated cyber operations center
- The establishment and refinement of modeling and simulations to support real-time operations and rapid acquisitions
- The analysis of the options for threat fusion and the synergies with United States Cyber Command (USCYBERCOM), DOD, the Intelligence Community, law enforcement, other government agencies and industry
- Investigation of joint community, other service, government and international entity cyber initiatives for future collaboration opportunities

Phase II specifics will also be driven by lessons learned and several other factors: progress on Phase I; the Phase II Program Action Directive (PAD) and Programming Plan (PPlan); and further direction from USAF, other national leadership, and USCYBERCOM on supporting combatant commands and other national requirements.

The objectives of this blueprint align from the Presidential Guidance down through the USAF priorities and AFSPC 2010 goals, and will be integrated into the USAF Space and Cyberspace Service Core Function Plan. The results of this blueprint will contribute significantly to the AF vision to "Fly, Fight and Win ... in Air, Space and Cyberspace." Additionally, this blueprint incorporates the initial goals and guidance from the Secretary of Defense and joint community ensuring USAF cyber efforts complement those of other cyber participants, provide maximum benefits to the joint fight and contribute significantly to the national cyber effort.

Current Situation

Cyberspace touches practically everything and everyone every day. The security and prosperity of our nation is dependent on freedom of access to and freedom of action in cyberspace. While there are many benefits that come with this access, there are numerous inherent vulnerabilities. Threats via cyberspace pose one of the most serious national security challenges of the 21st Century. The threat is asymmetrical with a minimal cost of entry; events of the last several years show that one person, with one computer, can affect an entire nation. Growing arrays of adversaries are targeting the US military and our critical national infrastructure, commerce and citizens. The combined and coordinated efforts of government, industry and academia will be required to effectively counter many of these attacks and assure mission success in the future.

Presidential Guidance

In May 2009, the White House released the "Cyberspace Policy Review - Assuring a Trusted and Resilient Information and Communications Infrastructure" that contributes to this blueprint. While the White House review sought primarily

"to assess US policies and structures for cyber security," it examined "the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military and intelligence missions as they relate to the security and stability of the global information and communications infrastructure." The review recognized "America's failure to protect cyberspace [as] one of the most urgent national security problems facing the new administration" and that "protecting cyberspace will require changes in policies, technologies, education and perhaps laws."

On the technology front, the review concluded "existing solutions can only do so much given the underlying design of the Internet architecture," and cited an advisory group for the Defense Advanced Research Projects Agency (DARPA) as saying, "the defense of current Internet Protocol-based networks as a losing proposition and called for an independent examination of alternate architectures." The President called for the federal government to work with industry on the development of "next-generation secure computers and networking for national security applications."

Joint Guidance

The Department of Defense (DOD) defines cyberspace as "a global domain within the information environment..." Cyber operations are defined as "the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace; such operations include computer network operations and activities to operate and defend the GIG."

The President's Unified Command Plan assigns United States Strategic Command (USSTRATCOM) the mission to conduct cyberspace operations. To fulfill the President's vision, the Secretary of Defense (SECDEF) tasked USSTRATCOM to establish the sub-unified US Cyber Command (USCYBERCOM). Subsequently, the USSTRATCOM Commander directed the development of an overarching vision and unified framework to synchronize and integrate global cyberspace operations. This direction compliments the Joint Chiefs' of Staff GIG 2.0 concept calling for the integration of service specific cyber infrastructures into a common enterprise; organized, trained and equipped to support the Joint Force Commanders. Thus, the intent for USCYBERCOM is to direct operations and defense of specified DOD information networks and conduct full spectrum military cyberspace operations in order to enable actions in all domains. In response, each of the military services is aligning its organizations and capabilities to support the SECDEF's direction.

USAF Intent

The significance of USAF operations in cyberspace is readily apparent. Not only is cyberspace vital to today's fight, it is key to the continued US military advantage over our enemies, now and in the future. Consequently, the USAF is steadfastly intent on providing a full range of cyber capabilities to Joint Force Commanders, whenever and wherever needed. Today, USAF cyber capabilities range from the virtual to the very real, including critical combat communications provided to the warfighter within hours upon the arrival of the USAF.

The USAF will move forward aggressively to:

- Consolidate and protect the USAF portion of the DOD network
- Build capacity by increasing the skill of our people, generating innovative operational capabilities, leveraging new partners and integrating those capabilities with those in the air and space.

- Expedite requirements and acquisition processes to deliver proactive and responsive cyber capabilities
- Develop doctrine, policies, security and guidance to effectively employ and innovate in cyberspace
- Prioritize and advocate for needed resources for cyberspace
- Significantly increase intelligence and analytical capabilities
- Shift paradigms from network-focus to mission-focus
- Develop cyber expertise to meet mission needs
- Improve commanders' decision making abilities by increasing situational awareness
- Affect changes in behavior, practices and culture by improving training, standards, communication and accountability
- Modernize and sustain the technology and equipment used for combat communications
- Eliminate seams in command and control (C2), security and doctrine to improve cross-domain effectiveness
- Combine and converge traditional operations with cyberspace operations to deter attacks and affect outcomes
- Partner with the DOD and other services to integrate, synchronize and consolidate the network infrastructures used by the joint forces

Commander's Guidance

The USAF will contribute to the joint fight by organizing, training and equipping expeditionary-capable cyber forces which will be presented to USSTRATCOM, USCYBERCOM, and other Combatant Commanders (COCOMS) as needed to conduct full spectrum operations. Consistent with joint terminology, operating concepts and views on the joint operating environment, the USAF views cyberspace as a contested operational domain that pervades and enables capabilities and effects in all other operational domains. Cyberspace is persistent, real-time and inherently global. USAF operations in the air, space and cyberspace domains are interdependent and focused on the needs of the Joint Force Commanders. The USAF will protect cyber capabilities and integrate them with other domains to enable joint warfighting effects greater than the sum of their parts.

The protection of the USAF portion of the DOD network architecture will focus on mission assurance. Until now, US adversaries have faced little to no risk or consequence in attacking or exploiting our systems, and the response has been to build stronger "walls." The time has come to think of cyberspace in a new light; not only must we defend against any attack, we must be able to "fight through" any attack, accomplish our missions and retain the ability to respond–thus giving us mission assurance in the face of future attacks or other disruptions. Under the direction of the Commander, US-CYBERCOM, we will prepare and conduct a dynamic defense with a range of responsive capabilities enabling flexible strategic and operational response options for the combatant commanders. The USAF will assess network vulnerabilities and threats by mapping mission dependence on cyberspace, mission essential functions and supporting infrastructure. Additionally, the USAF will leverage its space and air assets to create redundancies for mission assurance and critical infrastructure needs while ensuring cross-domain tactics, techniques and procedures (TTPs) are effective and consistent. Training and standardization and evaluation programs will reflect the operational mission focus and the combat mission readiness status of USAF cyber forces.

The USAF will continue to improve security of existing cyber infrastructure while pursuing a next generation network architecture that is integrated, mobile, visual, virtual, secure, responsive and intuitive. Currently, the joint community and COCOMS are supported by a multitude of decentralized network infrastructures operated by the services, contractors and industry, most running different configurations of the same programs, which is costly, complex and difficult to defend. It is both necessary and inevitable to integrate and synchronize these networks while transitioning to a single seamless network. The USAF will seek a single, integrated network encompassing air, terrestrial, and space layers that is managed and commanded/controlled as a single entity and that is fully compatible with a seamless DOD network. Cyber operators must be able to employ this common architecture and associated technologies for the full range of cyberspace operations, and to do so seamlessly with those of our mission partners. This next-generation architecture will enable exponential increases in capabilities for every mission and increase synchronization and real-time global situational awareness. It is estimated that in the next decade an Airman will carry in his hand 10 times the computing power of his current desktop, laptop and phone combined. It is the goal of the USAF to ensure each Airman has access to leading-edge technology and connectivity through an assured next-generation network.

The USAF Concept of Operations

In October 2008, the Secretary of the Air Force designated Air Force Space Command (AFSPC) as the USAF lead MAJCOM for organizing, training and equipping cyber capabilities. This alignment allows the USAF to focus its efforts and capitalize on inherent synergies found in space and cyberspace architectures and processes.

Additionally, the USAF established a new cyberspace operational Component Numbered Air Force (C-NAF) under AFSPC. In August 2009, the USAF activated the 24 AF as its operational cyberspace entity with the responsibilities to integrate, employ and consolidate cyber capabilities in support of Joint Force Commanders and USAF component commander needs.

24 AF is the USAF's cyber warfighting organization and has the requisite capabilities and authority to establish, operate, maintain and defend USAF networks, conduct other operations as required and present cyber forces and capabilities to USCYBERCOM and the other combatant commanders as required. The 24 AF Commander serves as the USAF component commander to USCYBERCOM and provides the operational focus, flexible command and control (C2) capability and single streamlined force to support Joint Force Commanders. To accomplish cyberspace missions and tasks, 24 AF is assigned three wings and is directly supported by the Air Force Intelligence, Surveillance and Reconnaissance Agency (AFISRA).

24 AF Commander is also the Air Force Network Operations (AFNETOPS) Commander and, under the direction of the USCYBERCOM Commander, will execute C2 over the AF portion of the GIG. As a focal point for all AFNETOPS, 24 AF has established the 624 Operations Center to ensure that global network components essential for mission success are defended, survivable and available to support air, space and cyberspace operations, and that cyberspace operations are integrated and synchronized with USCYBERCOM.

The USAF will seek an expanded concept of operations that integrates air, space and cyberspace capabilities, streamlines command and control, advances doctrine and creates a security framework to facilitate integration and to allow cross-ideation for air, space and cyberspace.

New Style of Partnerships

Because of the shared risk and to reduce vulnerabilities, the USAF must establish new relationships and actively strengthen and expand its partnerships with interagency, joint, industry, academia and international entities. Cyberspace transcends military domains and national boundaries and has changed the way we interact globally. The USAF operates a small percentage of the global cyberspace infrastructure. Industry currently provides over 90% of the cyberspace infrastructure, which potentially correlates to DOD mission success. This necessitates that the USAF must continue to foster existing relationships to enable and support the execution of the mission while fulfilling national objectives.

The USAF must create new patterns of interaction with the cyber research and innovation communities and anticipate and articulate new needs for the science and technology community. Rapid technology advancements inherent in this domain require the USAF to continually strive to pioneer the future by developing new partnerships with academia and industry. The USAF needs to rapidly exploit technical advances by establishing a continuous process for working with the science, industry and academic communities that form the leading-edge information technology sector to shape our activities in the cyberspace domain.

Capability Integration

The USAF will develop unique cyber capabilities that originate in its distinct missions and take full advantage of the integration of air, space and cyber capabilities. Each service brings its own cyber strengths and capabilities to the joint team and the nation. Since air, space and cyberspace are inextricably linked both operationally and technically, the potential exists to integrate capabilities across these domains to exponentially increase each other's power. This integration promises to give joint force commanders unrivaled global access, persistence, awareness and connectivity capabilities and to rapidly restore critical infrastructure via a cross-domain network-of-networks approach. The USAF will seek to develop cyber capabilities that complement those of other services and will explore the combination of cyber with other non-kinetic capabilities to achieve synergies.

The speed and nature of operations in cyberspace domain dictates a fusion of mission competencies and skills. The traditional cyber tasks must be integrated to present a full spectrum of seamless and synchronized capabilities and operations. Airmen will stop thinking of themselves as operators, communicators, intelligence experts, etc. but rather as an integrated team of multi-disciplined well-trained cyber professionals with the technical and tactical skills needed to execute any and all missions. The USAF will revolutionize its operations by establishing an integrated cyber operations center that is fully integrated with those of our joint partners to serve as the intersection for a full range of cyber capabilities. Expeditionary cyber forces comprised of team members with the appropriate training and experience will provide leading edge, tailored capabilities to meet USAF component and Joint Force Commanders' needs worldwide, from Irregular Warfare to high-end conflict.

Like offense and defense in the other operational domains, operations and intelligence in cyberspace must not be separated. The USAF will optimize the fusion of intelligence and operations by significantly expanding and exploiting the full range of our intelligence resources and analytical capabilities. It is the USAF's goal to move from situational awareness to situational comprehension and ultimately situational projection with data that is easily shared across organizational boundaries. Since there are many common operating pictures (COPs) being assembled across the services and agencies, it is desirable to improve and consolidate COPs while making relevant USAF tools and data

available to the joint COPs. The USAF will work to integrate space and cyberspace indicators and warnings to develop an advanced early warning architecture across the AF-GIG. Seamless operations and the strength of USAF partnerships will act as force multipliers to build capacity.

Operational Responsiveness

The rapidly changing cyberspace environment demands that we create a new acquisition strategy that is predictive, adaptive and timely and keeps us on the cutting edge of new technology. COCOM needs will emerge quickly and our goal is to deliver operational capabilities at the speed of need; therefore, the USAF will improve the process of indentifing cyber requirements and delivering responsive cyber capabilities. The re-engineering of requirements and acquisition to better support COCOM needs necessitates a tiered approach to meet operational needs in this dynamic environment. Our cyber adversaries attack 24 hours a day, seven days a week, 365 days a year and act and react in real time. This reality requires real-time modifications to existing capabilities and also a rapid hours-to-weeks acquisition process to meet these constantly evolving threats. The USAF will develop requirement thresholds to determine whether the need is real-time, rapid or foundational. An agile and adaptive requirements process will ensure that the USAF is optimizing limited resources while responding to future operational demands.

Cyberspace Culture

The USAF will strive to change its cultural mindset in the day-to-day execution of cyber operations. The importance of cultivating a new mindset cannot be overstated. It demands a fundamental shift in leadership that encourages creative, yet critical thinking and rewards innovative activities and solutions. Cyberspace does not function independently of other capabilities provided by the USAF or other DOD agencies. For example, the question of capability integration is broader than just the USAF and requires an understanding of how USAF cyber capabilities may leverage or be leveraged by the capabilities of the other military services and mission partners. In addition, the integration and acculturation of cyberspace must permeate doctrine development, accession and advanced training, professional military education, exercises, war games, recruitment and day-to-day operations.

A cultural change is also critical in the USAF operation and defense of the AF-GIG. Every USAF airman, government civilian, and contract partner must become a cyber defender. The United States is vulnerable to cyber attacks by relentless adversaries attempting to infiltrate our networks- at work and at home- millions of times a day, 24/7 planting malicious code, worms, botnets and hooks in common websites, software and hardware, such as thumb-drives, printers, etc. Once implanted, this code begins to distort, destroy and manipulate information, or "phone" it home. Certain code allows US adversaries to obtain higher levels of credentials to access highly sensitive information. Adversaries attack computers at work and at home knowing Airmen communicate with the AF network via email or transfer information from one system to another.

Airmen have a critical role in defending the USAF networks. They can significantly decrease the adversary's access to the USAF networks by:

- Not opening attachments or click on links unless the email is digitally signed, or directly verifying the source directly
- Not connecting any hardware or download any software, applications, music or information onto our networks without approval
- Encrypting sensitive but unclassified and/or mission critical information
- Installing the free Department of Defense anti-virus software on home computers

As always, USAF Airmen are the core of our mission success; and the civilians and contract partners of the USAF also play a unique and critical role. Technical competence alone is not sufficient to meet the challenges of the 21st century. Airmen must be technically astute, tactically competent, armed with warrior ethos and equally prepared to deploy forward or operate in place to accomplish the mission. The USAF will increase cyber expertise by implementing a focused recruitment strategy, a specific and carefully managed cyber career pathway and career-long professional development. The USAF will increase opportunities for education and provide specialized organic cyber operational training to include a centrally managed force of trained personnel with forensic and other specialized skills. The USAF will develop procedures to identify and track cyber professionals within the USAF personnel system and leverage the contributions of the Air National Guard and Air Force Reserve Command to develop and present unique capabilities.

Conclusion

This shall serve as the USAF Blueprint for Cyberspace and the foundation from which we will assure mission success by conducting operations effectively. The USAF will implement this blueprint as a unified effort within the Air Force, the sister services, the combatant commands, the Joint Staff and other partners to fully provide the capabilities for the future. This is the essence and intent of the USAF mission. In the words of Chief of Staff General Norton Schwartz and Secretary of the Air Force Michael Donley: "We have made a commitment to the warfighter and we will deliver."

Objectives and Strategies

USAF Priority: Partner with the joint and coalition team to win today's fight

Objective 1:
Position and differentiate USAF cyberspace capabilities.

Strategies:

- Integrate and innovate unique capabilities that come from USAF and joint missions and the intersection of air, space and cyberspace
- Communicate unique capabilities, milestones and achievements

Objective 2:
Present synchronized, full spectrum capabilities to the joint fight.

Strategies:

- Baseline existing cyberspace operational capabilities and weapon systems
- Fuse current and planned cyber personnel into COCOM force presentation
- Develop an overarching program to assess mission effectiveness in a cyberspace contested environment with results influencing operational needs and TTPs
- Integrate AF space and cyberspace capabilities into COCOM planning efforts
- Identify priority joint requirements and focus on collaboration to meet the need
- Create a unified C2 approach for agile, proactive management of space and cyberspace
- Create an environment similar to an integrated operations center to allow teams with different skill sets to work together and brainstorm to solve problems
- Develop expeditionary cyber teams
- Partner with the other services to realize the joint information environment vision of GIG 2.0
- Develop robust ISR capabilities across the range of military operations

Objective 3:
Move from Situational Awareness to Situational Comprehension and Situation Projection.

Strategies:

- Achieve sustained Situational Awareness (SA) through a Common Operational Picture (COP) and fuse with the joint and COCOM COPs
- Capture trends, vulnerabilities, and best practices for integrating AF cyberspace operations with our partners
- Develop a continuous process to establish effective communication and coordination to update and refine the architecture and user inputs into a collective cyberspace SA capability

- Identify private sector, government, academia, military, and the Intelligence Community systems that comprise or contribute to a cyberspace COP
- Fuse cyber intelligence to deliver proactive, responsive operational cyber capabilities
- Create or integrate into a "Threat Fusion Center" = Increase situational awareness by leveraging AF SPC's sensor-centric indicators and warnings
- Develop, refine and apply data mining and visualization technologies
- Tap into cross-disciplinary expertise perspectives to ensure comprehension is accurate and complete
- Invest in appropriate modeling and simulation technologies
- Conduct wargaming, trend extrapolation and other forecasting techniques to aid in situation projection

Objective 4:
Fully integrate cyberspace capabilities in all mission areas across all domains and into the joint fight.

Strategies:

- Update guidance, policy, doctrine, instructions, plans, orders and programs to incorporate cyber relationships, operations and capabilities
- Develop a program to incorporate cyber requirements into all future weapon systems
- Modify security policies to maximize integration of cyber capabilities into special access programs
- Develop a shared cyberspace analysis architecture

Objective 5:
Increase capacity and capabilities during routine and crisis operations through TFI.

Strategies:

- Evaluate current mission requirements relative to Air Reserve Component (ARC) core competencies for routine and crisis operations
- Evaluate emerging mission requirements relative to ARC core competencies for routine and crisis operations
- ~~Develop Cyber Minuteman Concept~~ - Create contingency capability using Air National Guard forces to ensure the USAF can provide continuity for vital functions if the nation loses some critical infrastructure like power and communications

USAF Priority: Develop and care for Airmen and their families

Objective 6:
Employ highly trained cyber experts to ensure mission essential functions for today and tomorrow.

Strategies:

- Add basic cyber defense and awareness training for all airmen and officers at accession

- Institutionalize Cyber Professional Force Development process
- Create a cyber personnel inventory with the skills required to meet current and future mission requirements
- Develop and implement cyber training and career-long educational construct
- Establish Cyber Professional Development Program
- Develop cyber exercises and war games
- Develop and execute USAF cyber competition and awards
- Develop a force for cyber intelligence analytical support
- Update guidance, policy, doctrine, instructions, plans, orders and programs to incorporate current and emerging cyber capabilities

USAF Priority: Modernize our air and space inventories, organizations and training

Objective 7:

Ensure mission success by maximizing cyber continuity, availability and resilience.

Strategies:

- Install and implement network security programs
- Baseline network operations and network infrastructure
- Standardize using a mission focus
- Devise solution to map USAF network to USAF missions with end-to-end forensics approach
- Automate tracking mechanism for network configuration changes
- Standardize TTPs/CONOPS
- Develop metrics for readiness, availability, resilience and capacity
- Employ network "Gold Teams" to ensure AF networks are protected and resilient under attack
- Coordinate training and exercises

Objective 8:

Improve and integrate network and mission architectures to allow synchronization of full spectrum operations.

Strategies:

- Improve and integrate architectures to enable full spectrum operations
- Develop future architecture
- Implement current Combat Information Transport System (CITS) block upgrades and architectures at an increased pace
- Integrate mission development, acquire monitoring and reporting mission system software
- Integrate with A3/A2 to develop a system that can provide situation projection, rather than just SA
- Publish requirement for mandatory Key Performance Parameters for Net Defense in Capability Development Documents (CDDs) for USAF-developed capabilities

- Redefine role of MAJCOM/A6s in response to paradigm shift, increasing information content and information management.
- Leverage Combat Communications to accelerate the upgrades to the USAF architecture

Objective 9:
Enhance partnerships with interagency, joint, industry, academia and international entities to increase effectiveness and DOD-wide efficiencies.

Strategies:

- Reinvigorate interagency outreach program
- Reinvigorate joint outreach program
- Consolidate disparate USAF space and cyberspace engagement efforts with industry, academia and coalition partners
- Create new patterns of interaction with the cyber research and innovation communities

Objective 10:
Field asymmetric capabilities and concepts for air, space and cyberspace.

Strategies:

- Develop a single innovation center for advanced training, exercises, TTPs and capabilities development for space and cyberspace
- Demonstrate combined Space/Cyberspace Expeditionary Group Concept
- Create "Quick Kill Teams" for 3 regional problems identified and use cyber sub-profile under Space Intelligence Defense Portfolio
- Leverage our know-how and know-where in positioning and timing to address the challenge of attribution in cyberspace
- Bring the tradition of secure cyberspace operations identical to air and space

USAF Priority: Recapture acquisition excellence

Objective 11:
Cyber capabilities delivered at the speed of need to outpace the threat posed by our adversaries.

Strategies:

- Create centralized cyber requirements process
- Develop initial concept for rapid cyber acquisition
- Develop initial concept for real-time cyber capabilities delivery