DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE SPACE COMMAND

AUG 05 2016

MEMORANDUM FOR SEE DISTRIBUTION

FROM: AFSPC/CC
150 Vandenberg Street, Suite 1105
Peterson AFB CO 80914-4020

SUBJECT: AFSPC Long-Term Science and Technology (S&T) Challenges

1. Space and Cyberspace capabilities are critical to national security and Joint Operations. AFSPC must guide S&T activities toward technologies that enable development and delivery of capabilities ensuring our freedom of action in the Space and Cyberspace domains.

2. This update to the AFSPC long-term S&T challenges extends beyond the activities of AFSPC Strategic Guidance and the Space and Cyberspace Core Function Support Plans, to align with the Space Enterprise Vision (SEV), the Air Force Strategic Master Plan and the DoD 3rd Offset Strategy. Eleven S&T challenges are identified as the most critical to achieving the goals identified in those documents. These challenges form the cornerstone of our long-term S&T activities.

3. Many of our long-term S&T challenges cross-cut both space and cyber domains and are agnostic to specific solutions. As such, we must create trusted and resilient combat effects over the next 30 or more years to stay ahead of adversary developments. To do so, we must continue to evolve emerging, breakthrough, disruptive and game-changing technologies that are extensible, manufacturable, autonomous, reconfigurable, agile and adaptable. As these technologies mature, they may be integrated into multi-domain, multi-mission portfolios.

4. Achieving success for each challenge requires innovative approaches and processes that identify and assess emerging S&T. The intent is to manage risks in S&T to reduce future risks borne by programs, leverage S&T to reduce costs of proven technology on programs, and accelerate the introduction of new capabilities. The following outlines the most critical long-term S&T challenges for space, cyber, and cross-cutting space/cyber over the next 10-35 years. Additionally, examples of each challenge area are provided in the three attachments. These examples are neither exclusive nor exhaustive, but are meant to illustrate typical focus areas.

5. AFSPC Long-Term S&T Challenges – Space

a. **Enhanced multi-domain and multi-phenomenology Space Situational Awareness, Battlespace Awareness and ISR** – Effective use of advancing sensor technologies to provide information of activities in the terrestrial, air, and space domains, including exploitation of multiple spectral regimes (infrared, ultraviolet, radio, optical, etc.), and the integration and human interface of the sensor-derived information.

b. **New technologies applicable to extending space based capabilities** – Space-based sustainment of existing operational satellites, resurrection of decommissioned satellites, on-board defense and resiliency factors, and self-healing satellites.

c. **Enhanced Space Access and Logistics** – Use of evolved techniques to deploy space-based capabilities, such as multiple-payload boosters, resilient deployment, on-orbit servicing and construction (3-d, robotic, mini-factory, space station, etc.).

d. **New concepts in space ground operations** – Enterprise Ground Services, small-light-mobile emplaceable terminals, networking of high data rates, added resiliency, and defense of ground systems.

e. **Dynamic new technologies applicable to all space systems** – Autonomous and automated space systems with on-board sensors and warning technologies to defend against threats, micro-satellites and their communications methods, and smart mission disaggregation and aggregation.

6. AFSPC Long-Term S&T Challenges – Cyber
   a. **Trusted Autonomous Systems, Networks, and Applications** – Advance technologies for autonomous, goal-seeking network capabilities that access and exploit any available communication medium to preserve connectivity.
   b. **Human-Machine Interface Design and Biometrics** – Advanced human-machine interface technologies for human performance augmentation and biometric based access to a multi-level security multi-domain Cyber Enterprise.
   c. **Advanced Data Protection Technologies** – Resilient, scalable, and flexible low power data protection technologies that enable operators to seamlessly operate across classification domains with advanced user access methods.

7. AFSPC Long-Term S&T Challenges – Cross-Cutting Space/Cyber
   a. **Artificial Intelligence (AI)/Cognitive Electronic Warfare (CEW)** – Technologies for systems to be controlled and defended by an inherent cognitive capability embedded in the system, reducing human involvement.
   b. **Artificial Intelligence (AI)** – Technologies to advance Artificial Intelligence (AI) enabled, human decision augmentation.
   c. **Advanced Data Analytics** – Technologies to synthesize and display voluminous multi-source data to predict, detect, inform, and augment the spectrum of space and cyber operations to allow comprehensive command and control and situational awareness.

8. HQ AFSPC/ST will lead the effort to incorporate this guidance into our Command's S&T activities. My POC is Dr. Merri Sanchez, HQ AFSPC/ST, DSN 692-2261.

JOHN E. HYTEN
General, USAF
Commander

3 Attachments:
1. AFSPC Overarching Space Long Term S&T Challenges
2. AFSPC Overarching Cyber Long Term S&T Challenges
3. AFSPC Overarching Cross-cutting Space/Cyber Long-Term S&T Challenges

DISTRIBUTION LIST

14 AF/CC
24 AF/CC
25 AF/CC
AFNIC/CC
AFLCMC/CC
AFSMO/CC
AFRL/CC
AFRL/RV
AFRL/RD
AFRL/RI
AFRL/RQ
AFRL/RY
AFRL/STO
AFRL/XP
SMC/CC
SMC/CA
SMC/AD
SMC/GP
SMC/MC
SMC/LE
SMC/RN
SMC/RSE
SMC/ST
SMC/SY
SMC/ORS
HQ AFSPC/SSDP
HQ AFSPC/A5/8/9
HQ AFSPC/A2/3/6
HQ AFSPC/A4
HQ AFSPC/FM
HQ AFSPC/FMZ
HQ AFSPC/ST
HQ AFSPC/PA
AFOSR
AFTENCAP
NRO/AS&T
DARPA/TTO
DARPA/MTO
DARPA/STO
DARPA/AEO
SAF/AQR
SAF/SP
AF/ST
DIUx
DASD/R&E

ATTACHMENT 1

AFSPC Overarching Space Long Term S&T Challenges

Space - Overarching S&T Challenge Areas:

1) **Enhanced multi-domain and multi-phenomenology Space Situational Awareness, Battlespace Awareness and ISR** – Effective use of advancing sensor technologies to provide information of activities in the terrestrial, air, and space domains, including exploitation of multiple spectral regimes (infrared, ultraviolet, radio, optical, etc.), and the integration and human interface of the sensor-derived information.
2) **New technologies applicable to extending space based capabilities** – Space-based sustainment of existing operational satellites, resurrection of decommissioned satellites, on-board defense and resiliency factors, and self-healing satellites.
3) **Enhanced Space Access** – Use of evolved techniques to deploy space-based capabilities, such as multiple-payload boosters, space-plane deployment, and on-orbit construction (3-d, robotic, mini-factory, space station).
4) **New concepts in space ground operations** – Enterprise Ground Services, small-light-mobile emplaceable terminals, networking of high data rates, added resiliency, and defense of ground systems.
5) **Dynamic new technologies applicable to all space systems** – Autonomous and automated space systems with on-board sensors and warning technologies to defend against threats, micro-satellites and their communications methods, and smart mission disaggregation and aggregation.

Space - Detailed S&T Challenge Areas:

1) **Enhanced multi-domain and multi-phenomenology Space Situational Awareness, Battlespace Awareness and ISR**
   a. Technologies that will provide commanders with pre-decisional understanding of the space situation, adversary actions, environmental variables, attribution (natural versus man-made), and present courses of action. Predictive technologies underpinned by trusted data sources and resilient communication systems.
   b. New technologies/techniques to improve visualization and understanding.
   c. Technologies could include improved sensors which will provide detection and characterization of all events of interest in a format which will be ingestible by the Command and Control (C2) systems.
   d. Revolutionize space and cyberspace Battle Management Command and Control (BMC2) and integrate these capabilities tightly with other multi-domain military operations.

2) **New technologies applicable to space based capabilities**
   a. Smaller, networked and functionally resilient satellites and/or satellite constellations for communications, position navigation and timing (PNT), space situational awareness (SSA), and launch detection/missile warning operations in contested/degraded environments.
   b. Cognitive systems for secure, agile and autonomously reconfigurable communications and sensors to enhance resilience, agility, and self-healing.
   c. Spacecraft resilience to and reconstitution from natural or manmade events.
   d. Electromagnetic spectrum or exo-electromagnetic spectrum technologies for transmitting communications and satellite commands unimpeded and undetected.

e. Alternatives for ground and communication systems that increase capacity and connectivity with new approaches in phenomenology, frequency, reuse, routing and node concepts (e.g., waveforms, proliferated relay architectures, packetizing at spacecraft/relay level, data management for variety of priority, data type, data sensitivity and latency requirements).

3) **Enhanced Space Access and Logistics**
   a. Advanced innovations for space transport and servicing. This should include new transport capabilities to and through space, and logistics support capabilities for space vehicles.
   b. Companion microsatellites attached on larger payloads, designed to separate and potentially connect with other microsats to enable increased mission synergy.
   c. Development of lunar-based or orbiting manufacturing station with 3-D printing, construction capability, fueling, and potential data relay or diagnostics capabilities.
   d. Robotic/remote controlled harvesters of defunct satellite components and basic materials to develop new or regenerated satellites.
   e. Trans-atmospheric delivery to near-space to permit boost of a hosted space access vehicle.
   f. Rail-launched delivery system using magnetic rail-gun technology to initiate scramjet or super impulse propulsion.
   g. Rapid Launch Capability to enable rapid reconstitution of space-based capabilities.

4) **New concepts in space ground operations**
   a. Technologies to simplify ground operation of space systems and increase protection and mobility.
   b. Enhanced predictive technologies, autonomy and manufacturability.
   c. Space systems with a high level of trust capable of rapid extensibility to accomplish unforeseen space missions.
   d. Dynamic encryption and signal beaming based on mission needs, threats, and automated processes.
   e. Service capability focused for responsive and agile options for execution of all missions through advanced ground processing and user systems.

5) **Dynamic new technologies applicable to all space systems**
   a. Improved ultra-high efficiency power system components, such as solar cells, thermal generators, alternative power generation and storage technology, batteries and adaptive point-of-load converters.
   b. Maximize satellite dry mass reduction through game-changing technologies.
   c. Develop technologies and architectures that facilitate integrating US systems with international and commercial partner systems and technologies including but not limited to future worldwide PNT capabilities (e.g., Multi-Global Navigation Satellite Systems).
   d. Provide autonomous spacecraft protection through on-board sensing and warning technologies while implementing revolutionary spacecraft technologies to ensure threat avoidance.
   e. Innovate mini, micro and nanosatellite technologies that will provide capabilities to reduce space transportation cost.
   f. Implement space logistics and manufacturing technologies to extend the service life of conventional satellites.
   g. On-orbit Range and Test infrastructure technologies to develop on-orbit missions from current to S&T capabilities (e.g., Nellis in space, satellite and man-made space flight).

ATTACHMENT 2

AFSPC Overarching Cyber Long Term S&T Challenges

Cyber - Overarching S&T Challenge Areas:

1) **Trusted Autonomous Systems, Networks, and Applications** – Advance technologies for autonomous, goal-seeking network capabilities that access and exploit any available communication medium to preserve connectivity.
2) **Human-Machine Interface Design and Biometrics** – Advanced human-machine interface technologies for human performance augmentation and biometric based access to a multi-level security multi-domain Cyber Enterprise to enable faster-paced cyber defenses and improved, more secure Type 3 access control.
3) **Advanced Data Protection Technologies** – Resilient, scalable, and flexible low power data protection technologies that enable operators to seamlessly operate across classification domains with advanced user access methods.

Cyber - Detailed S&T Challenge Areas:

1) **Trusted Autonomous Systems, Networks, and Applications**
   a. Technologies to enable autonomous, goal-seeking, self-organizing, self-generating, and amorphous (*ad hoc*) network capabilities to include inherent abilities that enable enhanced access, and exploitation of owner agnostic communication mediums across the electromagnetic spectrum.
   b. Technologies to enable unimpeded and undetected information transmission in innovative ways across electromagnetic and/or other spectrums.
   c. Technologies to automate payload development and synchronize capability planning into singular action plans across the war-fighting domains through vulnerability analysis, discovery, reverse engineering, and adaptation.
   d. Autonomous "deep learning" machines and systems (AI) which can synthesize huge amounts of data/Situational Awareness/Intelligence Surveillance Reconnaissance and provide mission relevant information across all warfighting domains (a mission relevant shared consciousness) to support flat self-synchronizing C2 processes/systems (able to visualize relevant domains).
   e. Fully automated network and nodal analysis using AI.
   f. Autonomous and intelligent agents scanning, analyzing, and providing relevant, actionable information.
   g. Advanced algorithms, quantum technologies, and computational methods to understand behavior, pattern, context recognition, and heuristics.
   h. Predictive and automated threat analysis to inform operators and feed other automated cyber defense systems.
   i. Cognitive Networks (Self-aware, self-healing networks)
      I. The network is its own record; you don't need a separate database/app to house network infrastructure information (maps, status of equipment, configuration); all hosts, servers, etc., know about their neighbors.
      II. Network self-heals or reconstitutes (reconfigures and fights thru an attack).
      III. Cognitive communications for agile, reconfigurable, and composable communications and sensors to enhance resilience and agility.
      IV. Network is aware of key terrain and prioritizes based on impacts across the 5 core Air Force mission areas.

V. Research and study methods to seamlessly adapt cyber operations capabilities to radio frequency through air, space, and terrestrial assets.

j. Theories and methods to operate securely on distributed, cloud systems, and weapon systems, as well as, systems that may not be secure.
k. Autonomous "deep learning" machines and systems (AI) which can synthesize huge amounts of data/SA enabling self-healing/controlling networks and mission/weapon system
l. Self-organizing networks.
m. Interwoven or integrated layer networks.
n. Create sophisticated, fully integrated, and seamless technologies, methods, and assets to provide cyber offensive and exploitation capabilities across air and space assets, electromagnetic spectrum, and networks against any adversary cyber-capable systems.
o. Develop technologies to permit collective action of multiple EW platforms to deliver and create cyber effects from an *ad hoc* network of EW systems using swarm tactics that is cognitive and driven by advances in AI. Use advanced fusion algorithms that permit these *ad hoc,* networked, electronic attack-capable systems to autonomously prioritize targets based on risk and effects.

2) **Human-Machine Interface Design and Biometrics**

a. Technologies to enable a biometric based access to a multi-level security multi-domain Cyber Enterprise.
b. Technologies to advance Human-Machine Interface for human performance augmentation via somatic and/or cerebral methods.
c. Advanced human-machine teaming, where a human is working with a cyberspace weapon system (shared consciousness - human provides goals).
d. Research methods to develop stealthy, agnostic, and autonomous platforms, accesses, and payloads adapting capabilities across all networks, closed systems, electromagnetic spectrum, and space, air and terrestrial systems.
e. Completely dynamic, always on, cyber modeling and simulation environment allowing all operators, across all mission areas to evaluate the full spectrum of effects and impacts as they would occur on actual blue, gray, and red spaces.
f. Biological Computing.
   I. Data storage on DNA.
   II. Data computing.
   III. Human augmentation.

3) **Advanced Data Protection Technologies**

a. Technologies to advance Quantum capabilities in the areas of computing and cryptography.
b. Flexible and scalable encryption (including reconfigurable sensors and fractionated platforms) for software, hardware, and networks allowing the operator to fight through adversarial conditions and seamlessly operate between multiple classification level networks.
c. Advanced credentialing methods for accessing accounts, networks, data, and systems to prevent adversary exploitation and compromise and allow for complete auditing, attribution.
d. Polymorphic defensive measures which automatically and seamlessly change network configurations and defensive surfaces to confuse and thwart adversary activity.
e. Low Power Encryption which can also be used to protect routing protocols to entirely mask transmission addresses.

ATTACHMENT 3

AFSPC Overarching Cross-Cutting Space/Cyber Long Term S&T Challenges

Cross-Cutting Space/Cyber - Overarching S&T Challenge Areas:

1) **Artificial Intelligence (AI)/Cognitive Electronic Warfare (CEW)** – Technologies for systems to be controlled and defended by an inherent cognitive capability embedded in the system, reducing human involvement.
2) **Artificial Intelligence (AI)** – Technologies to advance Artificial Intelligence (AI) enabled, human decision augmentation to enable decision superiority in the space and cyber domains.
3) **Advanced Data Analytics** – Technologies to synthesize and display voluminous multi-source data to predict, detect, inform, and augment the spectrum of space and cyber operations to allow comprehensive command and control and situational awareness.

Cross-Cutting Space/Cyber - Detailed S&T Challenge Areas:

1) **Artificial Intelligence (AI)/Cognitive Electronic Warfare (CEW)**
   a. AI/CEW involves the capability for systems to be controlled and defended by an inherent cognitive capability embedded in the system, reducing human involvement.
   b. Ensure control and desired recognition and reaction to threats.
   c. Establish effective human-interaction and prevention of a friendly system from "turning" as a result of an infiltration or logic anomaly.
   d. Transition to a fall-back capability immune from an adversarial AI/CEW capability.

2) **Artificial Intelligence(AI)**
   a. Develop advanced multi-domain technologies that provide real-time domain awareness and attribution, predictive battlespace awareness for man-made and natural phenomena, and rapid development and assessment of mitigative courses of action across all five operational domains – air, land, sea, space, and cyberspace.
   b. Create ethical based frameworks leveraging AI to mitigate insider threat, malicious activity, and support full spectrum cyber operations.
   c. Use AI augmentation for human decision makers by developing recommendations based on threats, indications and warnings, resources, and available tools.

3) **Advanced Data Analytics**
   a. Ability to detect and prevent insider threat through analytic means of intelligent human baselining and anomaly detection while integrating social factors.
   b. Automated cyber forensics and analytics with evidence discover, dynamic sensing and real-time classification and correlation of network captures and host-level events. Ability to synthesize multi-source, multi-time scale data and analytics. Needs to incorporate and inspect encrypted traffic.
   c. "Abstract away the uniqueness" by understanding the core capabilities/techniques and not being distracted by variants and signature adaptions.
   d. Technologies to improve data storage and access.
      I. Reduce cost and size for data storage.
      II. Reduce latency for data access.

e. Technologies to reduce power/resource consumption: Could root-in processing power with reduction in power consumption and increased heat resistance remove requirement for environmental controls?
f. Integrated, advanced, and voluminous multi-source data across all networked, closed, embedded, electromagnetic spectrum, and unique business and weapon systems to predict, inform, and augment the spectrum of space and cyber operations while providing singular visualization platforms for situational awareness and command and control of weapon systems operations, mission impacts, network activities, unit statuses, and more.
g. Technologies to enable geolocation of adversary and friendly network systems which can be integrated into the full spectrum of operations across all warfighting domains, providing complete infusion and situational awareness of physical locations of key targets and assets.