DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE SPACE COMMAND

17 Feb 15

MEMORANDUM FOR AFSPC NAF AND CENTER COMMANDERS
HQ AFSPC DIRECTORS
AFRL/CC
SAF/AQR

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. In accordance with AFSPC Strategic Guidance and the Space and Cyberspace Core Function Support Plans, I directed an update to the AFSPC long-term S&T challenges. Four S&T challenges were 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.

AFSPC Long-Term S&T Challenges

a. Revolutionize capabilities to enhance Battle Management Command, Control and Communication (BMC3) of space and cyberspace operations and integrate with other multi-domain military operations.
b. Advance disruptive innovations, placing capabilities into space and cyberspace domains rapidly and at dramatically lower cost with significant performance increases.
c. Develop advanced space and cyberspace technologies that provide real-time domain awareness, 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.
d. Establish mutually-supportive, resilient space and cyberspace technologies that provide predictive threat analysis of the domains, quickly identify emerging threats and differentiate them from natural phenomena, and respond appropriately and effectively to allow operations through and recovery from these threats.

3. 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

Attachment:
Long-Term S&T Challenge Descriptions

ATTACHMENT

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

Long-Term S&T Challenge Descriptions:

To meet our needs 10-30 years in the future, emerging, breakthrough, disruptive and game-changing technologies which provide revolutionary improvements are required to stay ahead of adversary developments. As these technologies mature, they may be integrated into multi-domain, multi-mission portfolios ensuring we maintain assured persistent access to the space and cyberspace domains. As the commercial presence in the space and cyber domains expands, the commercial infrastructure should be leveraged while maintaining cyber security on spacecraft and ground systems. Achieving success for each challenge requires innovative approaches and processes that identify and assess emerging S&T. The goal is to minimize risk, reduce cost and accelerate introduction of capabilities. The following paragraphs include examples of potential advancements and research areas that address the AFSPC S&T long-term challenges. These examples are neither exclusive nor exhaustive, but are meant to illustrate typical focus areas.

1. Revolutionize capabilities to enhance battle management command, control and communication (BMC3) of space and cyberspace operations and integrate with other multi-domain military operations.

   Evolutionary development and enhancement of capabilities is no longer sufficient to provide the warfighter with new capabilities in the areas of domain awareness and C2. Currently, the Air Force is faced with the loss of electromagnetic spectrum bandwidth previously used for C2. To offset this and to meet the long-term technological needs of the Air Force, the following capabilities and research are areas of high interest:

   a. New bands of the spectrum using new equipment and entirely new communications capabilities.
   b. Enhanced communications technology integrating space, cyberspace, and DoD mission systems.
   c. New technologies addressing near-instantaneous and secure communications.
   d. The theory and modeling of covert and side channels.
   e. Information management systems that are user friendly and provide data analytics including data storage that is quickly and easily discoverable.
   f. Increased automation and resiliency of space and cyberspace BMC3, to include automated informing and tasking, which frees operators to accomplish warfighter missions and provides survivable data pathways.
   g. Systems that rapidly communicate requests for support, with automation capability to prioritize requests and enable machine-to-machine dissemination of approved products.
   h. Systems that demonstrate revolutionary and dynamic visualization capabilities.
   i. Cognitive communications for agile, reconfigurable, and composable communications and sensors to enhance resilience and agility.
   j. An ability to transmit information unimpeded and undetected across the electromagnetic spectrum.

k. Development of future technologies which might combine Game Theory, disruptive spectrum sensing techniques, and emerging Cyber-Physical Systems technologies to facilitate resilient BMC3.

2. Advance disruptive innovation, placing capabilities into space and cyberspace domains rapidly and at dramatically lower cost with significant performance increases.

   The cost of placing capabilities into space remains high. Truly effective space operations will require the ability to place capabilities in space in the same manner that aircraft conduct bombing, close air support or transport missions. Chemical rockets are expensive. We must strive to reduce launch and operations costs while continuing to achieve mission success, develop new capabilities that lower cost or replace them with more cost-efficient ones. The following may be means to achieve this goal:

   a. Development of breakthrough capabilities and concepts (e.g., rail guns, mass drives, space-based 3D printers) to dramatically reshape, rescope and rethink launch and deployment such that it is more responsive to mission needs.
   b. Development and deployment of smaller, networked and functionally resilient satellite and/or satellite constellations for communications, navigation and timing and missile warning.
   c. Develop payload design capabilities that allow rapid integration into commercial satellites meeting hosted payload timelines and possible variable and innovative orbits.
   d. Cyberspace technologies and methodologies to rapidly develop, deploy, modify, and reconfigure offensive and defensive cyber capabilities. Defensive cyber capabilities include: enhanced network automation/resiliency and protection efficiency, advanced cyber platforms, access and payload technologies, stealth, persistence, communications technologies, reverse engineering and malware reuse/reapplication, selective attribution and malware source detection, and metamorphic and polymorphic technologies are also examples.
   e. Technology and strategy which enable a trusted, secure mixing of government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) components throughout AF weapon systems.
   f. Automated, intelligent cyberspace systems for analysis, operation, defense, attack, verification and validation of software systems to shorten testing and verification/validation.
   g. Development and deployment of new sensor technologies and instrumentation to decrease the footprint of our launch ranges, enhance capability, and ensure public safety.
   h. Mathematical foundations of system software, hardware, human users and attackers, and network architectures addressing cybersecurity, key metrics, abstractions and analytical tools.

3. Develop advanced space and cyberspace technologies that provide real-time domain awareness, 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.

In combat, the warfighter and supporting systems could be overwhelmed by the amount of information being delivered. Intelligent systems that rely on the knowledge gained over centuries of combat need to be developed and deployed for the warfighter. These systems should provide proposed courses of action for space and cyberspace operations to support combat in the five domains. Potential AFSPC increased capabilities and areas of interest are:

a. Data fusion and visualization tools which will accomplish mission situational awareness across: space and cyberspace; Intelligence, Surveillance, & Reconnaissance (ISR); and air and ground platforms. These would include sensors to track and maintain custody of objects in Low Earth Orbit (LEO), Medium Earth Orbit (MEO), Geosynchronous Orbit (GEO), and other orbits, including Highly Elliptical Orbits (HEO)/Molniya and to better predict natural phenomena (e.g., solar flares) and ways to mitigate/isolate those impacts to space and cyberspace systems.
b. Decision Support tools are for intent and behavior determination. This includes engineering and delivering cognitive capabilities such as agile, reconfigurable and composable communications and sensors.
c. Methods to augment operator cognitive capabilities and capitalize on the ever increasing ability of machines to process large volumes of data.
d. Approaches to better utilize the convergence of information – ingest, fuse, correlate, trust and employ large amounts of data (including non-governmental data) – in areas of situational awareness, cyber, commercial and DoD-generated data being collected. This also includes increased direct-to-warfighter data dissemination.
e. Technology to enable centralized/remote management out to the end-user device reducing the manpower required for administrative communications and free up cyber personnel to work on mission systems.
f. Prediction and anticipation of the nature of space and cyberspace systems attacks.

4. Establish mutually-supportive, resilient space and cyberspace technologies that provide predictive threat analysis of the domains, quickly identify emerging threats and differentiate them from natural phenomena, and respond appropriately and effectively to allow operations through and recovery from these threats.

Space and cyberspace operations are the backbone of all military operations. As such, these systems must include resiliency and graceful failure mechanisms (including failure and attack remediation technologies). As we mature to space-enabled cyberspace operations and cyber-enabled space operations, we must keep pace with the technological advances of other Major Commands, Combatant Commands, Services and Agencies, as well as coalition partners, industry and academia, ensuring all our systems are interconnected in providing domain awareness. They must be protected with new technologies and support the development and deployment of capabilities such as:

a. Resiliency and ability to recover from natural or manmade events (both kinetic and non-kinetic which also might include improved radiation hardening of all space systems).

b. Mutually supporting, enhancing, complementary, and compatible systems acquired by other Major Commands supporting Combatant Commands, Services and Agencies, as well as coalition partners, industry and academia.
c. Technologies which identify and bridge the seams dividing space and cyberspace.
d. New capabilities in space and cyberspace ensuring neither domain is subjected to a debilitating surprise attack. Sensing and discriminating between normal system failures and malicious failures.
e. An ability to counter other space and cyberspace capabilities, potentially in a surgical, non-attributable manner, to maintain freedom of action for our operations.
f. Flexible and scalable encryption (including reconfigurable sensors and fractionated platforms) allowing the operator to fight through adversarial conditions.
g. Using quantum technologies in the areas of computing and cryptography enhancing data management capabilities and anticipate threats and reconfigurations.
h. Technologies which detect and autonomously mitigate on-orbit debris threats.
i. Advanced cybersecurity methods, models, and algorithms.
j. Theories and methods to operate securely on distributed and cloud systems, as well as, systems that may not be secure.
k. New approaches for mitigative actions to predict, pre-empt, avoid, defend, fight through and/or recover and reconstitute from a cyber-attack. These technologies could include the following:
    1. Automatic generation of BMC3 options with Monte Carlo-like analysis results.
    2. Moving target techniques (MTTs) such as internet protocol (IP) hopping and dynamic reconfiguration.
    3. Enabling surgical effects against adversarial bots or co-opted infrastructure within the blue terrain while minimizing side effects against friendly missions.
    4. Facilitating non-traditional behavioral analysis to discover and track privileged and sophisticated insider threats.
    5. Enable detection of hidden code within legitimate files.
    6. Keyless digital signatures for logistically feasible data integrity checking/auditing.
    7. Data protection and recovery technologies which provide increased mission resiliency.
    8. Innovative and expansive cloud use (including the Internet of Things (IoT)), implementation, protection and exploitation technologies.
l. Timely, accurate and discriminatory attribution mechanisms essential to the space and cyberspace domains/missions.
m. Methods to discover and prevent malicious code imbedded in software or hardware – supply side and operating system.