Air Force Cyber Vision 2025

Dr. Mark T. Maybury
Chief Scientist
Cyber Vision 2025
Terms of Reference

- **Background:**
  - Need to forecast future threats, mitigate vulnerabilities, enhance the industrial base, and develop the operational capabilities and cyber workforce necessary to assure cyber advantage across all Air Force mission areas
  - An integrated, Air Force-wide, near-, medium- and far-term S&T vision to meet or exceed AF cyber goals and, where possible, create revolutionary cyber capabilities to support core Air Force missions

- **Key Stakeholders:** Air Staff, MAJCOMS, AFRL, 24th AF, ESC, ASC, SMC

- **Approach**
  - Identify state of the art and best practices in government and private sector
  - Analyze current and forecasted capabilities, threats, vulnerabilities, and consequences across core AF missions to identify critical S&T gaps
  - Articulate AF near (FY11-16), mid (FY16-20) and long (FY21-25) term S&T to fill gaps, indicating where AF should lead, follow, or watch
  - Address cyber S&T across all Air Force core missions and functions (air, space, C4ISR) comprehensively including policy as well as DOTMLPF considerations
  - Engage and partner (industry, academia, national labs, FFRDC, government)

- **Product:** Cyber S&T Vision to top 4 by 7/15/12 (Report 1/1/13)

DOTMLPF - Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, and Facilities
AF Cyber Accomplishments

- Organizing and Equipping
  - Stood up AFSPC/24th AF
  - Cyberspace Superiority CFMP (AFSPC)
  - AF Policy Directive (10-17) on Cyberspace Operations
  - Established AF-Cyber Integration Group (CIG) – HAF, CFLI
  - Cyberspace Operations and Support Community
  - Strategy for Cyberspace CORONA TOP 2011
  - DRAFT Cyberspace Roadmap (A3/CIO A6 and AFSPC/CFLI)

- Education and Training
  - Cyber Operator Career Field (17D)
  - UCT (Keesler AFB), Cyber 200, 300 (AFIT), Cyber WIC (Nellis)
  - AFIT Cyberspace Technical Center of Excellence (CyTCoE)

- Exercises: CyberFlag, Red Flag (live fire, air & space support of cyber, force on force defense of the CAOC-N)

- Employing AFCYBER warfighting forces in support of USSTRATCOM/USCYBERCOM

ECT = Undergraduate Cyber Training
CFMP = Core Function Master Plan
WIC = Cyber Weapons Instructor Course
Cyber Vision 2025

Study Methodology

STRATEGY

REQUIREMENTS AND PLANS

COCOM and MAJCOM Requirements

MISSION FOCUS

Threat

Cyber

Air Cyber

Space Cyber

C2 and ISR Cyber

Mission Support (Education & Training, Acquisition, T&E)

Cross Cutting Enabling S&T

RFIs, EXPERT SUMMITS

CFMPs
Current Environment

Cyberspace = interdependent network of information technology (IT) infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors, controllers, individuals, organizations and missions.

Cyber Threats = Nation states, non-state actors and domestic threats; launching/operating agents, bots, Trojans, worms, social engineering, insider attacks to deny, degrade, disrupt, destroy, or deceive

Cyber Missions = Cyber exploitation, defense, & operations; information assurance, command & control

Assured Air, Space, C4ISR and Cyber Operations

Integrated Air, Space, ISR and Cyber Operations

Situation Awareness, Common Operational Picture (COP)

• Networks
• Sensors
• Data Links
• Embedded Systems
• Command & Control
• Supply Chain
• Databases
• Operators

Cyber is Inextricably Entwined with the Air and Space Missions
Future Trends
1999-2025

- CMOS Integrated Circuit Feature Size
- Telecommunications bandwidth (log scale)
- Malware Signatures (Threats)
- US IC Off-shoring
- World-wide Internet Users (# and % population)
- Internet Hosts
- High Performance Computing Speed
- World-wide Software Revenue
- Mobile App Downloads
- Chinese Computing PhD Degrees
- US Computing PhD Degrees

2025
- Econ: China #2, India #3
- Population +2B
- 7T IP enabled devices
- 50 zetabytes ($10^{21}$) of data
- IT/nano/bio converge
- Quantum

CMOS – Complimentary Metal-Oxide Semiconductor; IC – Integrated Circuit
PhD Degrees in Computer Science/Computer Engineering/Computational Mathematics
External Experience

![List of companies and logos](image)

# RFI Responses (Total 102)

- Cyber: 34
- Msn Spt: 22
- C2ISR: 15
- Threat: 9
- S&T: 9
- Air: 8
- Space: 5

---

Distribution A. Approved for public release; distribution is unlimited.
Enduring Principles

- Least Privilege – provide only necessary authorities (e.g., white listing, discretionary access control, containment)
- Balance of Power – distribution of authority, peer review, two person rule
- Non-Interference – technical (multilevel) and operational (coord/synchronize)
- Minimization – limit attack surface, limit dependencies, reduce capability to essentials
- Simplification – allow only necessary complexity, employ standards (interfaces/controls)
- Survivability – fitness/readiness, awareness, anticipation, speed (responsiveness), agility (e.g., flexibility/ maneuver), and evolvability
- Resilience – robustness (e.g., redundancy), diversity, active defense, rapid reconstitution
- Optimization – offense/defense, human & machine intelligence, cost/benefit
- Leverage – maximize adversary cost/risk/uncertainty; maximize friendly benefit/assurance/efficiency
Environment & Findings

Realities

- Our operations (air, space, C2, ISR) depend on cyber
- Cyberspace is contested and/or denied
- Resources (financial, human, time) will be constrained
- Cyber operations can have digital, kinetic, & human effects

Findings

- Mission at risk: Interdependency growth driving cost and risk; Insider threat, supply chain threat, Advanced Persistent Threat (APT)
- Cyber S&T enables assurance, resilience, affordability, empowerment
- Need to integrate across authorities and domains
- Need to shape doctrine, policy, people, processes (RDT&E)
- Partnership and leverage essential

Source: SEI, LM  Distribution A. Approved for public release; distribution is unlimited  Source: SEI
AF Cyber S&T Vision

“Assured cyber advantage across air, space, cyber, C2ISR, and mission support”

- **Assured** – Ensured operations in congested, competitive, contested, and denied environments in spite of increased dependencies, vulnerabilities, and threats
- **Cyberspace** – its defense, exploitation, operation
- **Advantage** – we seek an agility, resilience, and effectiveness edge over our adversaries
- **Across** – we require advantage within and across
- **Air, space, cyber, C2ISR, mission support** – we require full spectrum cyber solutions
Recommendations

- **Assure and Empower the Mission** *(MAJCOMs)*
  - Assure national security missions to security standards exceeding biz systems
  - More effective use of Title 10/50/32
  - Multi-domain synch/integrated effects
  - Increase cost of adversary OCO

- **Improve Cyber Education, Accessions, ACE** *(AETC, A1, A6, AFSPC)*

- **Advance Processes** *(AFSPC, AQ, TE, MAJCOMS)*
  - Require/design in security; secure full life cycle
  - Rapid, open, iterative acq; engage user/test early
  - Integrate cyber across CFMPs
  - Advance partnerships, align funding

- **Enhance Systems and Capabilities** *(AFSPC, AQ, AFMC)*
  - Reduce complexity, verify systems
  - Hardened, trusted, self-healing networks and info
  - Agile, resilient, disaggregated mission architectures
  - Real-time cyber situational awareness/prediction, managed information objects, cyber FME

**Focused, Enabling S&T** *(AFRL)*
- Assure and empower missions
- Enhanced agility & resilience
- Optimize human/machine sysstems
- Establish foundations of trust

OCO = Offensive Cyberspace Operations; ACE = Air Force Cyber Elite; FME= Foreign Material Exploitation

Distribution A. Approved for public release; distribution is unlimited.
OSD Cyber S&T
Desired End State

Source: Cyber S&T Priority Steering Council Research Roadmap. Dr. Steven King Nov 8, 2011.
# Cyber S&T Desired Outcomes

**Across Air, Space, Cyber, C2 and ISR**

Technology Leader (L), Follower (F), Watcher (W)

<table>
<thead>
<tr>
<th>Area</th>
<th>Near (F12-FY15)</th>
<th>Mid (FY16-20)</th>
<th>Far (FY21-25)</th>
</tr>
</thead>
</table>
| **Assure and Empower the Mission** | • Semi-Automated Mission Mapping and Anomaly Resolution for Cyber SA (L)  
• Secure Communication (L)  
• Access and D5¹ Cyber Effects (L/F) | • Real-time AFNET SA & C2 (L)  
• Cyber Mission Verification and Assurance Across Sensors/Platforms  
• Survivable C3 (L)  
• Advanced Access, D5 Effects (L/F) | • Autonomous Cyber Mission Assurance/Management (L)  
• Predictable Cyber Effects on Mission Systems (L) |
| **Enhance Agility and Resilience** | • Fractionated², Morphable, Reconstituting Architectures (L)  
• Cyber Maneuver (L)  
• Intelligent Mix of GOTS/COTS (F) | • Online Vulnerability Identification and Adaptation (F)  
• Resilient Virtualization (F) | • Autonomous, Secure, Agile Composable CyberPhys Systs (L)  
• Cognitive Comm/Networks (agile, reconfigure, self heal) (L) |
| **Optimize Human-Machine Systems** | • Operator Selection (e.g., traits, methods) (L/F)  
• Operator Measurement (e.g., stress, cognition, perf., trust) (L)  
• Adversarial/Social Modeling (L) | • Automated Individual Performance Assessment and Training (L)  
• Initial Augmented Cognition (L)  
• Auto Cyber Battle Damage Assess (L) | • Intent/Behavior Detection and Forecasting (L)  
• Human-Machine Perf Optimize (L)  
• Neuroscience based brain computer interfaces (L/F) |
| **Foundations of Trust** | • Measurement, Vulnerability Model/Analysis, & Verification (L)  
• Real-Time Cyber Reverse Engineering (L/F)  
• Software Anti-Tamper (L)  
• Secure Virtualization (F) | • Information Integrity V&V (L)  
• Quantum Communication (L)  
• Root of Trust for Cyber C2 (L)  
• Embedded Anti-Tamper (F)  
• Semi Autonomous Supply Chain Assurance (F) | • Quantum Methods for V&V, Trust, and Vulnerability Assessment (F)  
• Provable Mission Assurance in Contested Domains (L) |

¹D5 = Degraded, Deceive, Destroy, Deny, Disrupt  
²Fractionated = physically and functionally distributed
## Cyber S&T Desired Outcomes and Example Programs Across Air, Space, Cyber, C2 and ISR

Technology Leader (L), Follower (F), Watcher (W)

<table>
<thead>
<tr>
<th>Area</th>
<th>Near (F12-FY15)</th>
<th>Mid (FY16-20)</th>
<th>Far (FY21-25)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assure and Empower the Mission</strong></td>
<td>• Semi-Automated Mission Mapping and Anomaly Resolution for Cyber SA (L)</td>
<td>• Real-time AFNET SA &amp; C2 (L)</td>
<td>• Autonomous Cyber Mission Assurance/ Management (L)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Managed Info Objects (MIO)</strong></td>
<td>• 100 Gbit dynamic mission SA</td>
<td>• Self-Protecting Information</td>
</tr>
<tr>
<td></td>
<td>• <strong>10 Gbit Mission Aware Routing</strong></td>
<td>• Cyber Mission Verification and Assurance Across Sensors/ Platforms</td>
<td>• Predictable Cyber Effects on Mission Systems (L)</td>
</tr>
<tr>
<td></td>
<td>• Secure Communication (L)</td>
<td>• Survivable C3 (L)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BLOS C2, Jetpacks JCTD</strong></td>
<td>• Assured Access Comm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Access and D5 Cyber Effects (L/F)</td>
<td>• Advanced Access, D5 Effects (L/F)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SCOTI</strong> Platform, JWIN</td>
<td>• Cross Air/Space/Cyber Sensor Integration and Plan Generation</td>
<td></td>
</tr>
<tr>
<td><strong>Enhance Agility and Resilience</strong></td>
<td>• Fractionated, Morphable, Reconstituting Architectures (L)</td>
<td>• Online Vulnerability Identification and Adaptation (F)</td>
<td>• Autonomous, Secure, Agile Composable CyberPhys Systs (L)</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Hopping, Morphable Architectures</strong></td>
<td>• Resilient Virtualization (F)</td>
<td>• Cognitive Comm/Networks (agile, reconfigure, self heal) (L)</td>
</tr>
<tr>
<td></td>
<td>• Cyber Maneuver (L)</td>
<td>• Architecture Diversity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Agile Tactical Communication</strong></td>
<td>• Heterogeneous Operationally Responsive Networks, Cyber Agility</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Intelligent Mix of GOTS/COTS (F)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Optimize Human-Machine Systems</strong></td>
<td>• Operator Selection (e.g., traits, methods) (L/F)</td>
<td>• Automated Individual Performance Assessment and Training (L)</td>
<td>• Intent/Behavior Detection and Forecasting (L)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Operator Selection (e.g., AFOQT)</strong></td>
<td>• Initial Augmented Cognition (L)</td>
<td>• Computational Social Science</td>
</tr>
<tr>
<td></td>
<td>• Operator Measurement (e.g., stress, cognition, perf., trust) (L)</td>
<td>• <strong>Operator SA, assessment, augment</strong></td>
<td>• Human-Machine Perf Optimize (L)</td>
</tr>
<tr>
<td></td>
<td>• Adversarial/Social Modeling (L)</td>
<td>• Auto Cyber Battle Damage Assess (L)</td>
<td>• Neuroscience based brain computer interfaces (L/F)</td>
</tr>
<tr>
<td></td>
<td>• 23 IOS Development</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Foundations of Trust</strong></td>
<td>• Measurement, Vulnerability Model/Analysis, &amp; Verification (L)</td>
<td>• Information Integrity V&amp;V</td>
<td>• Quantum Methods for V&amp;V, Trust, and Vulnerability Assessment (F)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Avionics Vulnerability Discovery</strong></td>
<td>• <strong>Crypto modernization, PKI, EKMS</strong></td>
<td>• Quantum Security Methods</td>
</tr>
<tr>
<td></td>
<td>• Real-Time Cyber Reverse Eng (L/F)</td>
<td>• Quantum Communication (L)</td>
<td>• Provable Mission Assurance in Contested Domains (L)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Software Anti-Tamper</strong></td>
<td>• Root of Trust for Cyber C2 (L)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Avionics Vulnerability Protections</strong></td>
<td>• Embedded Anti-Tamper (F)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Secure Virtualization (F)</td>
<td>• Semi Autonomous Supply Chain Assurance (F)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CMATH</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1$D5$ = Degrade, Deceive, Destroy, Deny, Disrupt

2SCOTI = Selective Cyber Operations Technology Integration

3JWIN = Joint Warfighting Integrated Network Operations
Air Force will leverage cyber capabilities and investments of our partners and focus S&T investment on Air Force mission

Distribution A. Approved for public release; distribution is unlimited.
Cyber Vision 2025

Key Messages

- Cyber Vision 2025 is the AF S&T vision for the *assured cyberspace advantage* enabled by key science and technology advances where the AF will lead, follow, or watch in the near, mid and long term.

- Key challenges include growing cyberspace threats, increased dependency and vulnerabilities, and resource constraints.

- Airmen are our most powerful cyberspace capability and their development is a priority.

- A principled approach and S&T advances provide opportunities to:
  - Reduce operating costs; enhance cyber acquisition
  - Empower cyberspace operators; partner for the joint fight
  - Advance agility/resilience, human/machine systems, and foundations of trust
  - Assure and empower all AF missions including C2 and ISR
  - Provide synchronized effects across air, space, and cyber

Call on Airmen to develop novel concepts of operations to take maximum advantage of forthcoming technologies.
Air Force Cyber Vision 2025

Air Force Cyberspace S&T Vision
Assured cyber advantage across air, space, cyber, C2, ISR, and mission support

Findings
- Missions at risk: Growing threats (insider, supply chain, advanced) and interdependencies
- Cyber S&T enables assurance, resilience, affordability, empowerment
- Need to integrate across authorities and domains (cross domain effects)
- Need to shape doctrine, policy, people, (RDT&E) processes
- Partnership and leverage essential

Recommendations
- Assure and Empower the Mission (MAJCOMs)
  - Title 10/50/32, Multi-domain synch effects
  - Improve Cyber Education, Accessions, Training (AETC, A1, A6, AFSPC)
- Advance Acquisition and Partnership (AFSPC, AQ, TE, MAJCOMS)
  - Require/design in security; secure life cycle
  - Rapid, open, iterative; engage user/test early
- Enhance Systems and Capabilities (AFSPC, AQ, AFMC)
  - Cyber Situational Awareness, Battle Damage Assessment, Foreign Military Exploitation
  - Simplicity, trust, verification, resilience
- Focused, Enabling S&T (AFRL)
  - Assure and empower missions
  - Enhanced agility & resilience
  - Optimize human/machine systems
  - Establish foundations of trust

http://tinyurl.com/cybervision
Cyber Vision Team

**Senior Governance Team (3*)**
- Dr. Mark Maybury (chair), Lt Gen Mike Basla (AFSPC/CV -> SAF/CIO A6), Gen Janet Wolfenbarger (AFMC/CC), Lt Gen William Lord (SAF/CIO A6), Lt Gen Larry James (AF/A2), Lt Gen Chris Miller (AF/A8)

**Key Senior Stakeholders**
- Lt Gen Charles Davis (ESC/CC, AFPEO C3I and Networks -> SAF/AQ), Lt Gen Ellen Pawlikowski (SMC), Lt Gen Judy Fedder (A4/7), Lt Gen Thomas Owen (ASC), Lt Gen “Hawk” Carlisle (A3/5), Maj Gen Neil McCasland (AFRL), Maj Gen Suzanne Vautrinot (24th AF), Maj Gen Mike Holmes (A3/5), Dr. Steve Walker (AQR), Dr. Jackie Henningsen (A9), Lt Gen(Sel) John Hyten (AQS -> AFSPC/CV), Maj Gen Robert Otto (AFISRA/CC), Maj Gen Earl Matthews (A3C/A6C), Maj Gen Ken Merchant (AAC), Maj Gen(Sel) Samuel Greaves (AFSPC/A8/9)

**Cyber S&T Mission Area Study Leads**
- **Air:** Dr. Kamal Jabbour (AFRL/RI), Dr. Don Erbschloe (AMC), Mr. Bill Marion (ACC)
- **Space:** Dr. Doug Beason (AFSPC), Col Brad Buxton (SMC) & Dr. Jim Riker (AFRL/RV)
- **Cyber:** Dr. Rich Linderman (AFRL/RI), Dr. Doug Beason (AFSPC) & Mr. Arthur Wachdorf (24AF)
- **C2ISR:** Dr. Steven K. Rogers (AFRL/RY/RI), Mr. Ron Mason (ESC), Mr. Stan Newberry (AFC2IC), Dr. Chris Yeaw (AFGSC), B Gen Scott Bethel (AFISRA/CV), B Gen (S) John Bansemer (AFISRA/CVA), DISL Keith Hoffman (NASIC), Dr. Rick Raines (CCR, AFCyTCoE)
- **Mission Support (Acquisition, Test & Eval, Edu & Trng, Workforce):** Dr. Steve Walker (AQR), Mr. Ron Mason (ESC), Mr. Mike Kretzer (688th), Dr. Nathaniel Davis (AFIT), Maj Gen Earl Matthews (A3C/A6C)
- **Enabling Technology:** Dr. Jennifer Ricklin (AFRL), Dr. Robert Bonneau (AFOSR)
- **Threat:** Mr. Gary O’Connell (NASIC), Col Matthew Hurley (AF/A2DD)
# Senior Independent Expert Review Group (SIERG)

<table>
<thead>
<tr>
<th>Air</th>
<th>Space</th>
<th>Cyber</th>
<th>C2ISR</th>
<th>Mission Support</th>
<th>S&amp;T, Threat, and Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prof Mark Lewis, U. Maryland</td>
<td><strong>Dr. Mike Yarymovych, Sarasota Space</strong></td>
<td>Prof Ed Feigenbaum, Stanford Gil Vega, DOE Prof. Gene Spafford, Purdue Dr. Herb Lin, Nat Academy Andrew Makridis, CIA Glenn Gafney, CIA</td>
<td>Prof. Alex Levis, GMU</td>
<td>John Gilligan Lt Col Marion Grant, USCYBERCOM/J9</td>
<td>Prof. Werner Dahm, ASU Evi Goldfield, NSF Charles Bouldin, NSF Lauren M. Van Wazer, OSTP Tomas Vagoun, NITRD</td>
</tr>
<tr>
<td>Natalie Crawford, RAND</td>
<td>Dr. Rami Razouk, Aerospace</td>
<td>Dr. Paul Nielsen, CMU/SEI Dr. Mark Zissman MIT LL Harriet Goldman, MITRE</td>
<td>John Woodward, MITRE Sue Lee Short, JHU-APL</td>
<td>Jim Gosler, Sandia Giorgio Bertoli, Army</td>
<td>Konrad Vesey, IARPA Stan Chincheck, NRL Dr. Wen C. Masters, ONR</td>
</tr>
<tr>
<td>Lt Gen George Muellner (Ret) USAF</td>
<td>Don Kerr Keith Hall, BAH</td>
<td>Gen Mike Hayden (Ret), USAF Lt Gen Ken Minihan (Ret) USAF RADM Will Metts, NSA/TAO Paul Laugesen, NSA/TAO Dr. Yul Williams, NSA/CSSTOC</td>
<td>VADM Mike McConnell, (Ret) USN</td>
<td>Lt Gen David Deptula, (Ret) USAF</td>
<td>Dr. Ernest McDuffie, CMU Mike Aimone, OSD (I&amp;E)</td>
</tr>
<tr>
<td>Robert Osborne, NNSA</td>
<td>Matt Linton, NASA ARC-IS</td>
<td>David Mountain, NSA Dr Starnes Walker, FItCyber, Navy Tim Grance, NIST</td>
<td>Lt Gen Ted Bowlds, (Ret) USAF Lt Gen Robert Elder, (Ret) USAF</td>
<td>Lt Gen (Ret) Trey Obering, USAF Dr. Tim Persons, GAO</td>
<td>Gen (Ret) Jim McCarthy, USAFA Dr. Peter Friedland Prof Pat Winston, MIT</td>
</tr>
<tr>
<td>Former USAF Chief Scientist</td>
<td>Former Director of NRO</td>
<td>Former Director NSA, DIA</td>
<td>Former DNI</td>
<td>Former AF CIO</td>
<td>AF SAB EXCOM</td>
</tr>
</tbody>
</table>

## Coalition

| Group Cpt Andrew Gudgeon, UK | Dr. Brian Hanlon, DSTO, Australia | Joseph Templin, Canada | 20 |
CV25 S&T Themes (1/2)

- **Mission assurance and empowerment**
  - Survivability and freedom of action in contested and denied environments
  - Enhanced cyber situational awareness for air, space, and cyber commanders enabled by automated network and mission mapping
  - Ability to detect and operate through cyber attacks enabled by threat warning, integrated intelligence (e.g., SIGINT, HUMINT, IMINT), and real-time forensics/attribution
  - Early vulnerability detection and enemy behavior forecasting enabled by advanced cyber ranges, including high fidelity, real-time modeling and simulation
  - Cross domain integrated effects and cross domain measures of effectiveness (MOEs), including cyber battle damage assessment

- **Agility and Resilience**
  - Active defense requires rapid maneuver enabled by dynamic, reconfigurable architectures (e.g., IP hoping, multilevel polymorphism)
  - Effective mix of redundancy, diversity, and fractionation for survivability
  - Reduction of attack surface, critical mission segregation, and attack containment
  - Autonomous compromise detection and repair (self healing) and real-time response to threats
  - Transition from signature based cyber sensors to behavior understanding to enhance high performance attack detection
CV25 S&T Themes (2/2)

- **Optimized human-machine systems**
  - Measurement of physiological, perceptual, and cognitive states to enable personnel selection, customized training, and (user, mission, and environment) tailored augmented cognition.
  - High performance visualization and analytic tools to enhance situational awareness, accelerate threat discovery, and empower task performance.
  - Autonomy appropriately distributed between operators and machines, enabled by increased transparency of autonomy and increased human “on the loop” or supervisory control.

- **Software and hardware foundations of trust**
  - Operator trust in systems (e.g., sensors, communications, navigation, C2) enabled by trusted foundries, anti-tamper technologies, and supply chain assurance, as well as effective mixes of government, commercial off the shelf, and open source software.
  - Formal verification and validation of complex, large scale interdependent systems.
  - Advanced vulnerability analysis, automated reverse engineering, real-time forensics tools.
  - High speed encryption, quantum communication, and quantum encryption for confidentiality and integrity.
## Cyber S&T Roadmap

Technology Leader (L), Follower (F), Watcher (W)

<table>
<thead>
<tr>
<th>Area</th>
<th>Thread</th>
<th>Near (F12-FY15)</th>
<th>Mid (FY16-20)</th>
<th>Far (FY21-25)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assure and Empower the Mission</strong></td>
<td>Mission awareness from managed information</td>
<td>• Mission Mapping for Selected Missions (L)</td>
<td>• Real-time C2 for AFNET (L)</td>
<td>• Assured mission operations in a contested cyber environment (F)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 10 Gbit Mission Aware Routing (L)</td>
<td>• 100 Gbit dynamic mission awareness (L/F)</td>
<td>• Self-Protecting Information (L)</td>
</tr>
<tr>
<td></td>
<td>Empower</td>
<td>• Access and D5 Effects (L/F)</td>
<td>• Access and D5 Effects (L/F)</td>
<td>• Access and D5 Effects (L/F)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Scalable Cyber Ops Framework (L)</td>
<td>• Cyber/SIGINT &amp; EW (L/F)</td>
<td></td>
</tr>
<tr>
<td><strong>Enhance Agility &amp; Resilience</strong></td>
<td>Resilience</td>
<td>• Real-time encryption at 10Gbits (F)</td>
<td>• Embedded anti-tamper pwr (F)</td>
<td>• Anticipatory defense (L)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Secure mobile platforms (F)</td>
<td>• Red team automation (F)</td>
<td>• Autonomic anti-tamper (L)</td>
</tr>
<tr>
<td></td>
<td>Agility</td>
<td>• Morphable architectures (L)</td>
<td>• Protected root of trust for cyber C2 (L)</td>
<td>• Self Healing Networks (F)</td>
</tr>
<tr>
<td></td>
<td>Cloud</td>
<td>• Virtualization for the AOC (L)</td>
<td>• Formal logic (W)</td>
<td>• Agile VM replacement (L)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cloud services (W)</td>
<td>• Resilient services (F)</td>
<td></td>
</tr>
<tr>
<td><strong>Optimize Human-Machine Systems</strong></td>
<td>Visualize</td>
<td>• Common operating platform (L)</td>
<td>• Augment human performance (L)</td>
<td>• Composable architectures (F)</td>
</tr>
<tr>
<td></td>
<td>Measure</td>
<td>• Objective measures, sensors, and assessments of operator cognitive state,</td>
<td>• Automated individual performance measurement (L)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>performance, and trust in automation (L)</td>
<td>• Automated decision tools (L)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Train, Educate</td>
<td>• Operator selection criteria (F)</td>
<td>• Human battle damage assessment (L)</td>
<td>• Automated cyber refresh (F)</td>
</tr>
<tr>
<td></td>
<td>Trust</td>
<td>• System decomposition and trustworthiness modeling tools (F)</td>
<td>• Supply chain assurance techniques (F)</td>
<td>• Quantitative risk modeling (F)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reverse engineering and vulnerability analysis tools (L)</td>
<td>• Threat avoidance metrics (L)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assure</td>
<td>• Formal representations of Missions (L)</td>
<td></td>
<td>• Formally provable mission assurance in a contested cyber domain (L)</td>
</tr>
</tbody>
</table>

D5 = Deny, Disrupt, Degrade, Deceive, Destroy
## Air Cyber S&T

**Technology Leader (L), Follower (F), Watcher (W)**

<table>
<thead>
<tr>
<th>Area</th>
<th>Sub-Areas</th>
<th>Near (FY12-15)</th>
<th>Mid (FY16-20)</th>
<th>Long (FY21-25)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vehicle Systems</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPUs</td>
<td>Trusted Foundry (F)</td>
<td></td>
<td>Anti-Tamper Root-of-Trust (L)</td>
<td>Composable Msn Sys (L)</td>
</tr>
<tr>
<td>Flight Control</td>
<td>Separation Kernel (F)</td>
<td>Anti-Tamper Root-of-Trust (L)</td>
<td>Model-Driven Arch. (F)</td>
<td></td>
</tr>
<tr>
<td>Buses</td>
<td>Risk Assessment (L)</td>
<td>Cyber Black Box (L)</td>
<td>High Bandwidth Bus (L/W)</td>
<td></td>
</tr>
<tr>
<td>Prognostics &amp; Health</td>
<td>Embedded Cyber Diagnostics (L)</td>
<td>Secure Maintenance Aids (L)</td>
<td>Cyber Dashboard &amp; Dynamic Mission Retasking (L)</td>
<td></td>
</tr>
<tr>
<td><strong>Mission Systems</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sensors</td>
<td>Sensor s/w tamper protection (L)</td>
<td>Ingested Data Integrity (L)</td>
<td>Attack resistant sensor sys (L)</td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>5th to 4th Platform Comm (L)</td>
<td>5th to 5th Platform Comm (L)</td>
<td>Cognitive, Self-Healing Airborne Networks (L)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Frequency Agile Spectrum (L/W)</td>
<td>Agile, Virtual Networks (L)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Navigation</td>
<td>GPS Hardening (L)</td>
<td>GPS Alternatives (L)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Air Traffic Control</td>
<td>TCAS (W)</td>
<td>ADS-B/C (W)</td>
<td>Autonomy (L)</td>
<td></td>
</tr>
<tr>
<td><strong>Ground Systems</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logistics</td>
<td>Supply Chain Security (F)</td>
<td>Active RFID - ITV (W)</td>
<td>Anti-Fragility (L)</td>
<td></td>
</tr>
<tr>
<td>Cryptography</td>
<td>Suite B Applications (F)</td>
<td>Lightweight / Adaptive Encrypt(W)</td>
<td>Quantum Encryption (F)</td>
<td></td>
</tr>
<tr>
<td>Launch &amp; Recovery</td>
<td>Collab/Coop Control (L)</td>
<td>Autonomous Launch / Rec (F)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BLOS C2</td>
<td>Multi Vehicle Control (L)</td>
<td>Advanced Satellite Comms (L)</td>
<td>Massive Data Analytics (L)</td>
<td></td>
</tr>
<tr>
<td><strong>Support Systems</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AOC</td>
<td>Secure CPU (F)</td>
<td>Survivable - C2 (L)</td>
<td>Secure CPU++ (F)</td>
<td></td>
</tr>
<tr>
<td>TACC</td>
<td>Managed Info Objects (L)</td>
<td>Trusted Enterprise Mgmt (L)</td>
<td>Sys of Svcs Assurance (L/F)</td>
<td></td>
</tr>
<tr>
<td>DCGS</td>
<td>Composable Security (L)</td>
<td>Trusted Cloud Computing (L)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GIG</td>
<td>Mission mapping (L)</td>
<td>Quantum Communications (L)</td>
<td>Homomorphic Computing (F)</td>
<td></td>
</tr>
</tbody>
</table>

Distribution A. Approved for public release; distribution is unlimited.
# Space Cyber S&T

Technology Leader (L), Follower (F), Watcher (W)

<table>
<thead>
<tr>
<th>Area</th>
<th>Near (F12-FY15)</th>
<th>Mid (FY16-20)</th>
<th>Far (FY21-25)</th>
</tr>
</thead>
</table>
| **Assure and Empower the Mission** | • Space/cyber test beds (fractionated, fight-through demos, shorter time to need) (L)  
• Space environment sensors for anomaly attribution (L)  
• Enable and exploit cloud computing (W) | • Survivable, assured real-time C3 in theater (Software Defined Radio) (L) | • Small, networked satellite constellations for communications, GPS, missile warning (L) |
| **Optimize Human-Machine Systems** | • Restructure cyber acquisition and operations policy - allow for full spectrum (F) | • Detect hidden functions, malware in the integrated space/cyber networks (hypervisors, etc) (F) | • Tools for intent and behavior determination (F) |
| **Enhance Agility and Resilience** | • Reconfigurable antennas and algorithms (L) | • Autonomous self-healing systems (F) | • Cognitive Communications - agile, reconfigurable, composable comm and sensors (L) |
| **Foundations of Trust**           | • Foundations of trust – hardware foundries, trusted software generation (W) | • Trusted satellite-cyber architectures (L)  
• Strong satellite C2 authentication (L)  
• Generate, detect single photons/radiation (W) | • Flexible, scalable high-rate encryption (F)  
• Space Quantum Key Distribution (QKD) (F)  
• Autocode generator generators that produce software that is correct by construction (W) |
<table>
<thead>
<tr>
<th>Area</th>
<th>Near (FY12-FY15)</th>
<th>Mid (FY16-20)</th>
<th>Long (FY21-25)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assure and Empower the Mission</td>
<td>- Semi-automated cyber-mission mapping (L)</td>
<td>- Automated cyber-mission map (F)</td>
<td>- Dynamically generated cyber-mission mapping (L)</td>
</tr>
<tr>
<td></td>
<td>- Integrated physical-space &amp; cyber-space M&amp;S (L)</td>
<td>- Validated physical-cyber space models integrated w/testbeds (L/F)</td>
<td>- Fully integrated capability to predict cyber effects on mission systems (F)</td>
</tr>
<tr>
<td></td>
<td>- Cyber asset characterization (F)</td>
<td>- Large scale cyber quantification and effects estimation (L)</td>
<td></td>
</tr>
<tr>
<td>Human-Machine Systems</td>
<td>- Visualization of cyber impacts on missions (L)</td>
<td>- Mapping human perceptual skills to rep of cyber situations (F)</td>
<td>- Mapping human intuitive reactions to rep of cyber situations (F)</td>
</tr>
<tr>
<td></td>
<td>- Autonomic responses to reliable indicators of adversary activity (F)</td>
<td>- Integration of autonomic “triage” with human decision-making for complex</td>
<td>- Optimization of human-cyber responses to complex cyber sit (L)</td>
</tr>
<tr>
<td></td>
<td>- Validating framework defining a cyber “situation” (L)</td>
<td>cyber situations (L)</td>
<td>- Foundations for projecting adversary trajectories through cyberspace (L)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Foundations for cyber data fusion (L)</td>
<td></td>
</tr>
<tr>
<td>Agility and Resilience</td>
<td>- Secure Clouds (F)</td>
<td>- Identification of the point of compromise (L)</td>
<td>- Automatic compromise detection (F)</td>
</tr>
<tr>
<td></td>
<td>- Cloud-based implementations of AF C2 and ISR functions (L)</td>
<td>- Secure manual rollback to an uncompromised state (F)</td>
<td>- Dynamic rollback (F)</td>
</tr>
<tr>
<td></td>
<td>- Analysis of moving target defense (F)</td>
<td>- Agile integrated ops planning (L)</td>
<td>- Living plan for agile operations (L)</td>
</tr>
<tr>
<td></td>
<td>- Integrated air, space, and cyber plans (L)</td>
<td>- Sequencing kinetic &amp; non-kinetic actions (L)</td>
<td>- Sequencing OCO and DCO actions (L)</td>
</tr>
<tr>
<td>Foundations of Trust</td>
<td>- Commercial HW support for platform attestation (F)</td>
<td>- Trusted foundry or verified HW support for platform attestation (F)</td>
<td>- Contextual verification for information integrity (L)</td>
</tr>
<tr>
<td></td>
<td>- Faster, more secure cryptographic technology (F)</td>
<td>- N-version verification of information integrity (L)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Dynamic keying (F)</td>
<td>- Anti-tamper protection for devices in the field (L)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Anti-tamper protection for SW in adversary territory (L)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

26
## Enabling Cyber S&T

<table>
<thead>
<tr>
<th>Area</th>
<th>Near (FY12-FY15)</th>
<th>Mid (FY16-FY20)</th>
<th>Far (FY21-FY25)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Foundations</strong></td>
<td>Measurement, Analysis, &amp; Verification</td>
<td>Taxonomy of System Vulnerability</td>
<td>Quantum Methods for Vulnerability Assessment and Security</td>
</tr>
<tr>
<td><strong>Agility and Resilience</strong></td>
<td>Secure Virtualization for Critical Infrastructure (e.g. the AOC)</td>
<td>Online Vulnerability Identification, Adaptation and System Repair</td>
<td>Autonomous Physically Secure Cyber Systems</td>
</tr>
<tr>
<td><strong>Human/Social / Machine Systems</strong></td>
<td>Advanced Situational Awareness for Cyber Operators</td>
<td>Online Assessment of Cyber Operator Performance</td>
<td>Cyber Operator Performance Augmentation</td>
</tr>
</tbody>
</table>