



U.S. AIR FORCE

Headquarters U.S. Air Force

Air Force Cyber Vision 2025



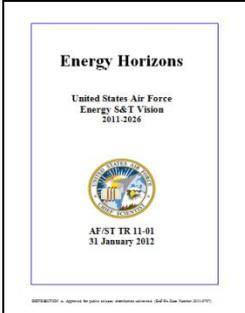
**Dr. Mark T. Maybury
Chief Scientist**

15 August 2012

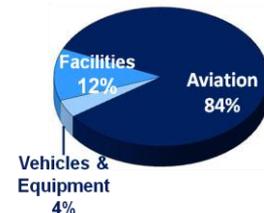
***5th International Symposium on
Resilient Control Systems (ISRCS)
Salt Lake City, Utah***

Distribution A. Approved for public release; distribution is unlimited. Public Release Case No 2012-0438

Integrity - Service - Excellence



Energy Horizons: Air Force Energy S&T Vision



Energy Horizons Vision

Assured energy advantage across air, space, cyberspace and infrastructure

Findings

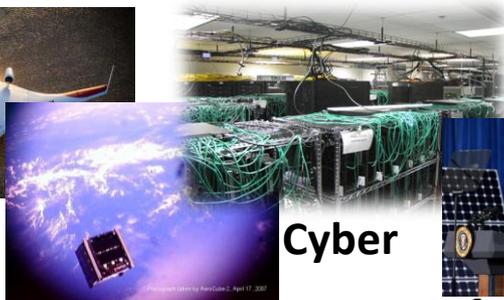
- Energy S&T advances can revolutionize cost, readiness, and resiliency
- Air fuels and facilities/data centers primary cost drivers
- Benefits from systems, operations, supply, and culture
- Partnership and S&T leverage essential

Recommendations

- Mission-focused S&T roles (lead, follow, watch) in near-, mid-, far-term
- **Air:** Efficient engines and structures, distributed virtual training, flight formation
- **Space:** Efficient photovoltaics, efficient ground stations, fractionated constellations
- **Cyber:** Efficient cloud and HPC
- **Infrastructure:** Secure microgrids, Expeditionary energy, small modular nuclear reactors, solar to petrol
- **Enabling:** nanomaterials, biomimicry, autonomy



Air



Space



Cyber



Infrastructure



1. AFCyber

National Cyber Security



“We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control... But ... we've failed to invest in the security of our digital infrastructure.”

President Barack Obama, 29 May 2009

“The most menacing foreign intelligence threats in the next two to three years will involve cyber-enabled espionage ... insider threats ... and espionage by China, Russia, and Iran.” Lt. Gen James Clapper, Jr. USAF (Ret), DNI, 31 Jan 2012

“Our military depends on resilient, reliable, and effective cyberspace assets to respond to crises, conduct operations, project power abroad and keep forces safe.”

Michael Donley, Secretary of the Air Force, 26 Mar 2012

“In cyberspace, we must continue our ongoing development of dynamic defenses for our vital networks so that they are protected. And to counter aggressors that are able to intrude and to root through our networks, we must increase our ability to find and disable any malware, to discern and interpret any forensic evidence, and to attribute threats and track them to their source.”

Gen Norton Schwartz, Chief of Staff, USAF 20 Sep 2011

“Cyberspace superiority describes our mission to gain advantage in, from, and through cyberspace at the times and places of our choosing, even when faced with opposition.”

Gen William Shelton, AFSPC/CC, 7 Feb 2012



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)

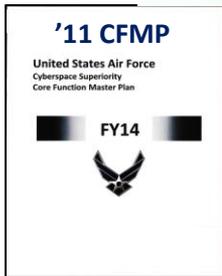
Education and Training

- Cyber Operator Career Field (17D), AFA CyberPatriot
- 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

UCT = Undergraduate Cyber Training
 CFMP = Core Function Master Plan
 WIC = Cyber Weapons Instructor Course

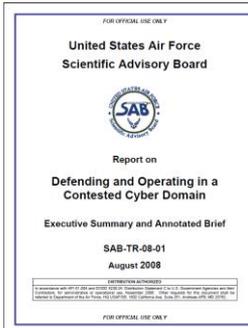
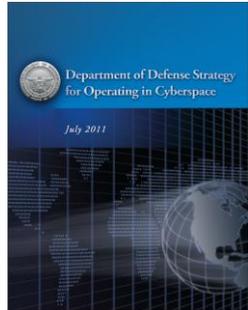




Cyber Vision 2025

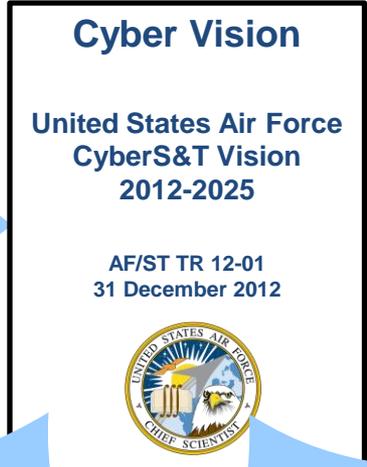
Study Methodology

STRATEGY



REQUIREMENTS AND PLANS

COCOM and MAJCOM Requirements



Independent Senior Expert Review

MISSION FOCUS

- Threat
- Cyber
- Air Cyber
- Space Cyber
- C2ISR Cyber
- Mission Support (Education & Training, Acquisition, T&E)
- Cross Cutting Enabling S&T

RFIs, EXPERT SUMMITS

CFMPs



Current Environment

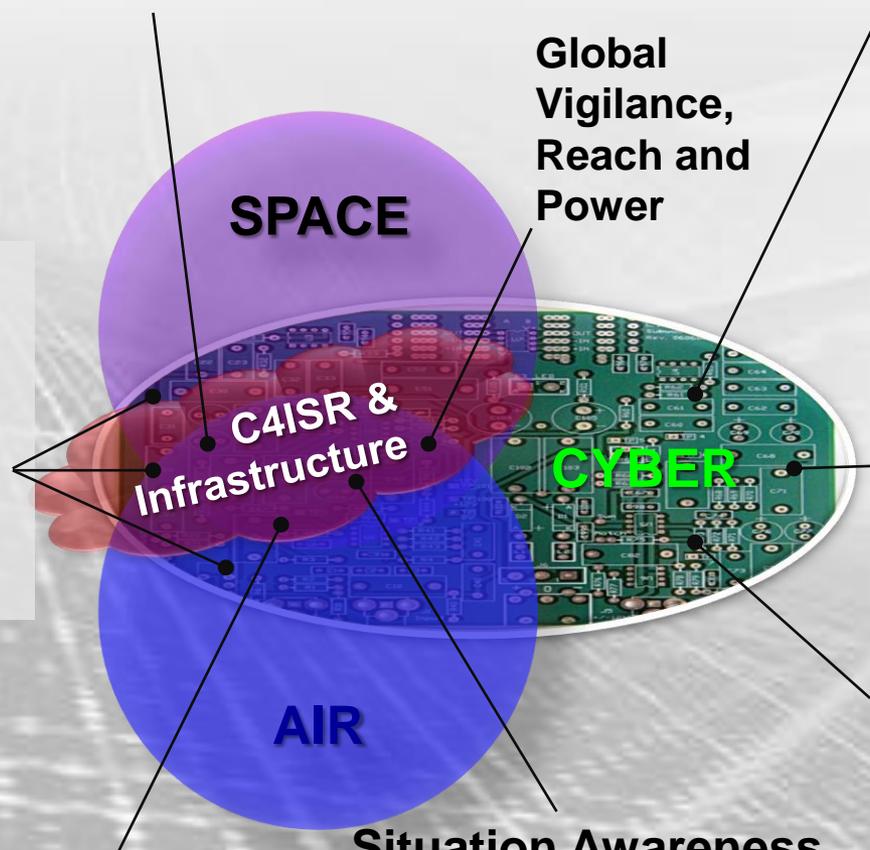
Assured Air, Space, C4ISR and Cyber Operations

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

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

Global
Vigilance,
Reach and
Power



C4ISR &
Infrastructure

SPACE

AIR

CYBER

Situation Awareness,
Common Operational
Picture (COP)

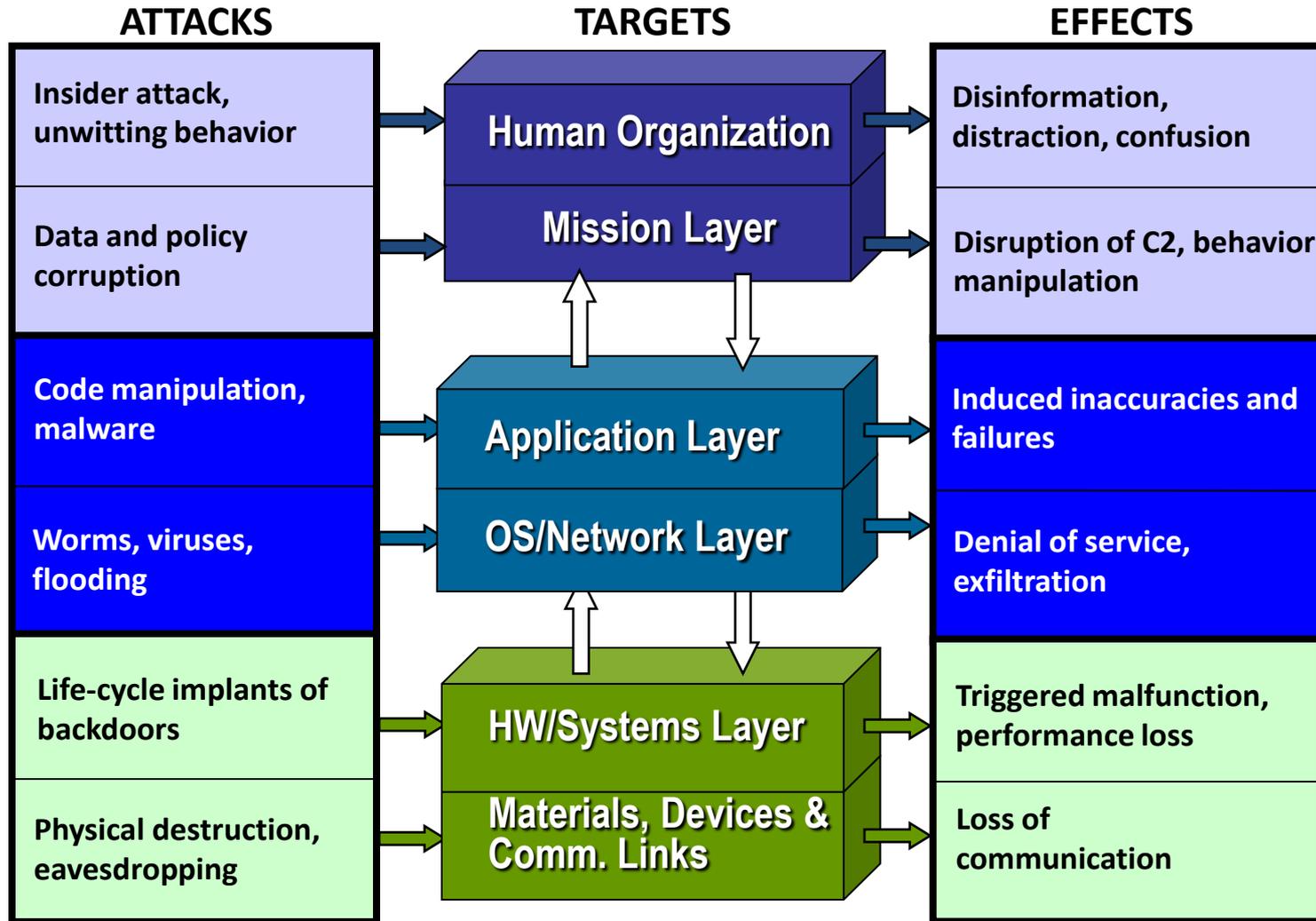
- Networks
- Sensors
- Data Links
- Embedded Systems
- Command & Control
- Supply Chain
- Databases
- Operators

Integrated Air, Space, ISR
and Cyber Operations

Cyber is Inextricably Entwined with the Air and Space Missions



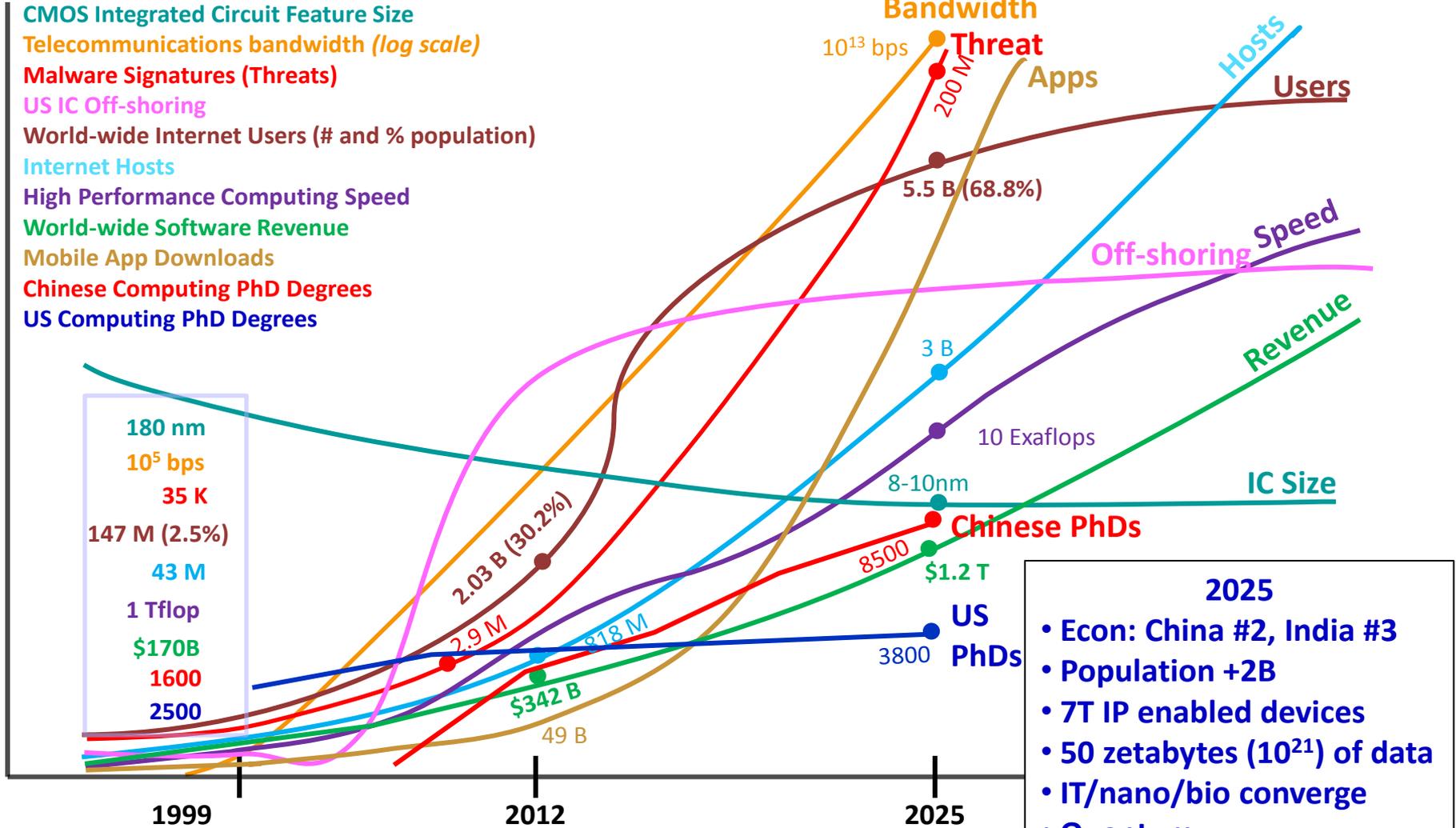
Missions are Contested at Multiple Levels





Future Trends

1999-2025

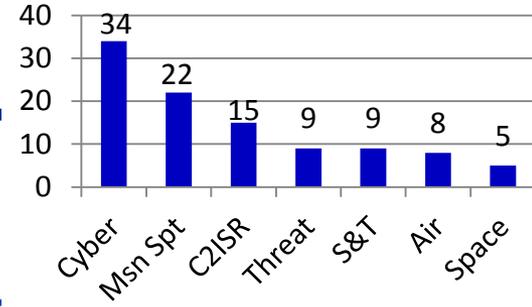


CMOS – Complimentary Metal-Oxide Semiconductor; IC – Integrated Circuit
 PhD Degrees in Computer Science/Computer Engineering/Computational Mathematics



External Experience

RFI Responses
(Total 102)



HP IBM Apple Oracle Google GE at&t Sandia National Laboratories Lawrence Livermore National Laboratory OAK RIDGE National Laboratory Argonne NATIONAL LABORATORY Los Alamos NATIONAL LABORATORY EST. 1943 Pacific Northwest NATIONAL LABORATORY BERKELEY LAB Lawrence Berkeley National Laboratory Idaho National Laboratory INL symantec BOEING HARRIS NORTHROP GRUMMAN Telcordia ManTech International Corporation CACI EVER VIGILANT EVERIS The Cornerstone of Network Security ViaSat OPNET Agi SOLERA NETWORKS SAGE Solutions AIS Assured Information Security, Inc. Carahsoft technology corp. ManTech International Corporation CACI EVER VIGILANT EVERIS The Cornerstone of Network Security

Accenture Priority Carahsoft AIS ManTech International Corporation CACI EVER VIGILANT EVERIS The Cornerstone of Network Security

ViaSat OPNET Agi SOLERA NETWORKS SAGE Solutions AIS Assured Information Security, Inc. Carahsoft technology corp. ManTech International Corporation CACI EVER VIGILANT EVERIS The Cornerstone of Network Security

MITRE RAND CORPORATION Adventium ENTERPRISE TerraEchos DesignKnowledge TERADATA THE BEST DECISION POSSIBLE wyle

APL Software Engineering Institute Carnegie Mellon MIT THAYER SCHOOL OF ENGINEERING AT DARTMOUTH STANFORD UNIVERSITY PURDUE UNIVERSITY GEORGE MASON UNIVERSITY UNIVERSITY OF VIRGINIA ZELTECH Zel Technologies, LLC NARUS serco BCSI SPYRUS SECURITY TO THE EDGE



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., hardening, 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



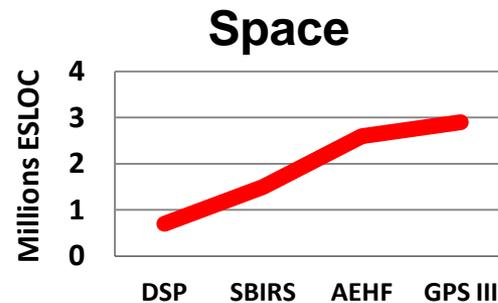
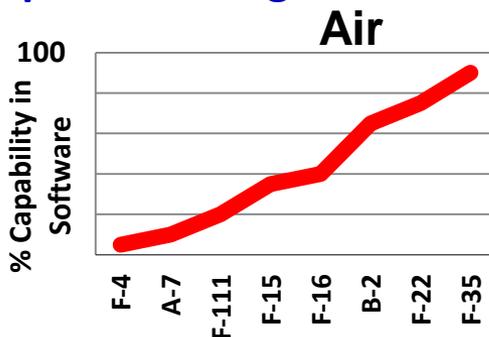
2. MedEvac

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





AF Cyber S&T Vision

***“Assured cyber advantage
across air, space, cyber, C2, ISR, 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, resiliency, and effectiveness edge over our adversaries
- ***Across*** – we require advantage within and across
- ***Air, space, cyber, C2, ISR, 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 (AFPSC, 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 & resiliency
 - Optimize human/machine systems
 - Establish foundations of trust

UNCLASSIFIED//FOUO Cyber S&T Roadmap Technology Leader (L), Follower (F), Watcher (W)				
Area	Focus	Near (FY12-FY15)	Mid (FY16-20)	Far (FY21-25)
Assure and Empower the Mission	Assure	<ul style="list-style-type: none"> • Mission Mapping for Selected Missions (L) • To Do Mission aware Routing (L) • Access and Co Effects (L) • System Resilience (L) 	<ul style="list-style-type: none"> • New Role CS for AFNET (L) • High-Dyn. mission awareness (L) • Access and Co Effects (L) • Access and Co Effects (L) 	<ul style="list-style-type: none"> • Assure national operations in a cloud environment (F) • Self-protecting information (L) • Access and Co Effects (L)

UNCLASSIFIED//FOUO Air Cyber S&T Technology Leader (L), Follower (F), Watcher (W)				
Area	Sub-Areas	Near (FY12-15)	Mid (FY16-20)	Long (FY21-25)
Assure and Empower the Mission		<ul style="list-style-type: none"> • Space-environmental sensors for anomaly attribution (L) • Enable and report cloud computing (W) 	<ul style="list-style-type: none"> • Space-environmental sensors for anomaly attribution (L) • Generate, detect single photons/radiation (W) 	<ul style="list-style-type: none"> • Real-time, assured real-time C2 in theater (Software Defined Radio) (L) • Real-time, assured real-time C2 in theater (Software Defined Radio) (L) • Real-time, assured real-time C2 in theater (Software Defined Radio) (L)

UNCLASSIFIED//FOUO C2ISR Cyber S&T Technology Leader (L), Follower (F), Watcher (W)				
Area	Near (FY12-FY15)	Mid (FY16-20)	Long (FY21-25)	
Foundations	<ul style="list-style-type: none"> • System Risk Quantification and Resilience (L) • Online validation and verification analysis of aerospace systems (F) • Frameworks for Cyber Resilience (F) 	<ul style="list-style-type: none"> • Online verification and verification analysis and repair (F) • Software fault analysis (F) 	<ul style="list-style-type: none"> • Autonomous Physical Security Systems (L) • Autonomous cyber management & dynamic control (F) • Autonomous cyber management & dynamic control (F) 	

UNCLASSIFIED//FOUO Enabling Cyber S&T Technology Leader (L), Follower (F), Watcher (W)				
Area	Near (FY12-FY15)	Mid (FY16-20)	Long (FY21-25)	
Foundations	<ul style="list-style-type: none"> • Measurement, Analysis & Verification (L) • Measurement Based Probabilistic Verification (F) • Analytic Verification (F) 	<ul style="list-style-type: none"> • Dynamic Telemetry & Repair of Vulnerability (L) • Telemetry & dynamic Repair of Cyber Vulnerability (L) • Software prediction and anti-tamper (F) • Automated code repair (F) 	<ul style="list-style-type: none"> • Physical Verification (L) • Quantum Verification and Validation Methods (F) • Genetic quantum computing platforms (F) • Autonomous code repair (F) 	
Human/Social Machine Systems	<ul style="list-style-type: none"> • Situation Awareness (L) • Objective measures of operator performance and situation awareness (F) • Social network analysis of blue and red behavior (F) 	<ul style="list-style-type: none"> • Real Time Assessment of Operator Performance (L) • Real time assessment of cyber operator performance and optimal situation awareness (L) • Real time analysis of social networks for red intent (F) 	<ul style="list-style-type: none"> • Human Performance Augmentation (L) • Complex human and system integration real time human performance augmentation (F) • Autonomy enhancement through social networks (F) 	

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

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



CV25 S&T Themes



Mission Assurance and Empowerment



Agility and Resilience



Optimized Human-Machine Systems



Software and Hardware Foundations of Trust



Agility and Resilience

- **Agility.** Nimbleness and adaptability. (e.g., dynamic, reconfigurable architectures such as IP hopping at the network layer)
- **Resilience.** The ability to avoid, survive, and recover from disruption. Disruption can be either a sudden or a sustained event and may be natural or manmade (e.g., internal failure or external attack). Can be enhanced by
 - Redundancy, diversity, and fractionation (distributed functionality) enabling systems to repel, absorb, and/or recover from attacks.
 - Hardening, reduction of attack surfaces, critical mission segregation, and attack containment.
 - Autonomous compromise detection and repair (self healing) and adaptation to and evolution from changing environments and threats can enhance survival.



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**

- **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**
- **Active defense requires rapid maneuver enabled by dynamic, reconfigurable architectures (e.g., IP hopping, multilevel polymorphism)**



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**



AF Core Mission and Prioritized S&T Roles

- ***Technology Leader*** – Creates or invents novel technologies through research, development and demonstration. Key S&T for core Air Force Title 10 missions and associated platforms with few or no other investors outside of the Air Force, e.g., IADS
- ***Fast Follower*** – Rapidly adopts, adapts or accelerates technologies originating from external leading organizations, e.g., hardening DoE's microgrids
- ***Technology Watcher*** – Uses and leverages others S&T investments for non core missions, e.g., generic IT



Cyber S&T Roadmap

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

Area	Thread	Near (F12-FY15)	Mid (FY16-20)	Far (FY21-25)
Assure and Empower the Mission	Mission awareness from managed information	<ul style="list-style-type: none"> Mission Mapping for Selected Missions (L) 10 Gbit Mission Aware Routing (L) 	<ul style="list-style-type: none"> Real-time C2 for AFNET (L) 100 Gbit dynamic mission awareness (L/F) 	<ul style="list-style-type: none"> Assured mission operations in a cloud environment (F) Self-Protecting Information (L)
	Empower	<ul style="list-style-type: none"> Access and D5 Effects (L/F) Scalable Cyber Ops Framework (L) 	<ul style="list-style-type: none"> Access and D5 Effects (L/F) Cyber/SIGINT & EW (L/F) 	<ul style="list-style-type: none"> Access and D5 Effects (L/F)
Enhance Agility & Resilience	Resilience	<ul style="list-style-type: none"> Real-time encryption at 10Gbits (F) Secure mobile platforms (F) 	<ul style="list-style-type: none"> Embedded anti-tamper pwr (F) Red team automation (F) 	<ul style="list-style-type: none"> Anticipatory defense(L) Autonomic anti-tamper (L) Self Healing Networks (F)
	Agility	<ul style="list-style-type: none"> Morphable architectures (L) 	<ul style="list-style-type: none"> Protected root of trust for cyber C2 (L) 	<ul style="list-style-type: none"> Agile VM replacement (L)
	Cloud	<ul style="list-style-type: none"> Virtualization for the AOC (L) Cloud services (W) 	<ul style="list-style-type: none"> Formal logic (W) Resilient services (F) 	<ul style="list-style-type: none"> Composable architectures (F)
Optimize Human-Machine Systems	Visualize	<ul style="list-style-type: none"> Common operating platform (L) 	<ul style="list-style-type: none"> Augment human performance (L) Automated decision tools (L) 	<ul style="list-style-type: none"> Automated mission view (L)
	Measure	<ul style="list-style-type: none"> Objective measures, sensors, and assessments of operator cognitive state, performance, and trust in automation (L) Cyber operator stress and vigilance analysis (L) 	<ul style="list-style-type: none"> Automated individual performance measurement (L) 	<ul style="list-style-type: none"> Individual and group performance prediction (L)
	Train, Educate	<ul style="list-style-type: none"> Operator selection criteria(F) Adversarial/social reasoning (L) 	<ul style="list-style-type: none"> Human battle damage assessment (L) 	<ul style="list-style-type: none"> Automated cyber refresh (F)
Foundations of Trust & Assurance	Trust	<ul style="list-style-type: none"> System decomposition and trustworthiness modeling tools (F) Reverse engineering and vulnerability analysis tools (L) 	<ul style="list-style-type: none"> Supply chain assurance techniques (F) Threat avoidance metrics (L) 	<ul style="list-style-type: none"> Quantitative risk modeling (F)
	Assure	<ul style="list-style-type: none"> Formal representations of Missions (L) 		<ul style="list-style-type: none"> Formally provable mission assurance in a contested cyber domain (L)

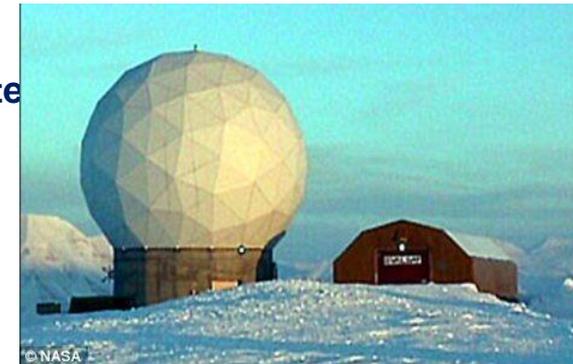
D5 = Deny, Disrupt, Degrade, Deceive, Destroy

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



Space Threat: Malicious Cyber Activities

- **Night Dragon**—since Nov 09, covert attacks on global oil, energy, and petrochemical companies*
 - Used social engineering, spearphishing, Microsoft Windows vulnerabilities, Microsoft Active Directories, and remote administration tools
 - Copied production/financial docs, collected data from SCADA systems
- **Satellite Center in Spitsbergen Norway is common control center for these satellites:**
 - Oct 07— **Landsat 7** (earth observation satellite) experienced 12 or more min of interference (not discovered until Jul 08)**
 - Jun 08—**Terra Earth Observation System AM-1** experienced 2+ min of interference**
 - Party achieved all steps required to command satellite but did not issue commands
 - Jul 08— **Landsat 7** experienced 12+ min of interference**
 - Party did not achieve all steps required to command satellite
 - Oct 08— **Terra EOS AM-1** experienced 9+ min of interference**
 - Party achieved all steps required to command satellite but did not issue commands



Svalbard Satellite Tracking Station in Norway is believed to be the access point

* Reported in McAfee's *Global Energy Cyberattacks: "Night Dragon,"* 10 Feb 2011

** Reported in the *2011 Report to Congress of the US-China Economic and Security Review Commission*



Space Cyber S&T

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

Area	Near (F12-FY15)	Mid (FY16-20)	Far (FY21-25)
Assure and Empower the Mission	<ul style="list-style-type: none"> • 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) 	<ul style="list-style-type: none"> • Survivable, assured real-time C3 in theater (Software Defined Radio) (L) 	<ul style="list-style-type: none"> • Small, networked satellite constellations for communications, GPS, missile warning (L)
Optimize Human-Machine Systems	<ul style="list-style-type: none"> • Restructure cyber acquisition and operations policy - allow for full spectrum (F) 	<ul style="list-style-type: none"> • Detect hidden functions, malware in the integrated space/cyber networks (hypervisors, etc) (F) 	<ul style="list-style-type: none"> • Tools for intent and behavior determination (F)
Enhance Agility and Resilience	<ul style="list-style-type: none"> • Reconfigurable antennas and algorithms (L) 	<ul style="list-style-type: none"> • Autonomous self-healing systems (F) 	<ul style="list-style-type: none"> • Cognitive Communications - agile, reconfigurable, composable comm and sensors (L)
Foundations of Trust and Assurance	<ul style="list-style-type: none"> • Foundations of trust – hardware foundries, trusted software generation (W) 	<ul style="list-style-type: none"> • Trusted satellite-cyber architectures (L) • Strong satellite C2 authentication (L) • Generate, detect single photons/radiation (W) 	<ul style="list-style-type: none"> • Flexible, scalable high-rate encryption (F) • Space Quantum Key Distribution (QKD) (F) • Autocode generator generators that produce software that is correct by construction (W)



Partnership and Focus



Intelligence Community

COCOMs



Army, Navy, Marines
Land and Maritime cyber



**National Labs
FFRDCs**


U.S. AIR FORCE
Air, Space, C2ISR

Federal Research
DARPA, NSF, FAA, OSTP, NASA, NIST



Academia

Industry & Consortia
(e.g., DIB Pilot)

International

Critical Infrastructure
DHS, EPRI, Utilities



Air Force will leverage cyber capabilities and investments of our partners and focus S&T investment on Air Force mission



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



Videos

- **1. AF Cyber Defense**
<http://www.youtube.com/watch?v=t849CYRd2Ak>
- **2. MedEvac**
<http://www.youtube.com/watch?v=2AQ65I9FUPA>
- **3. RPA Reaper C2 Sniper**
<http://www.youtube.com/watch?v=fiB3vrhPDNs&feature=relmfu>
- **4. Space C2 – Collision Avoidance**
<http://www.youtube.com/watch?v=RfAHw1kTpvY&feature=relmfu>
- **5. Combat Search and Rescue**
<http://www.youtube.com/watch?v=PWUw9TMD5f8&feature=relmfu>

